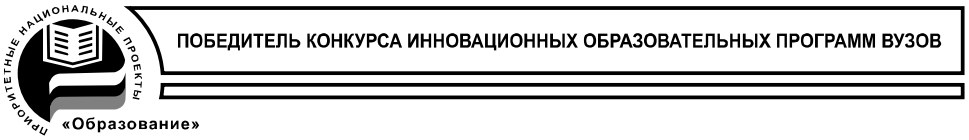
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ



Сборник трудов конференции молодых ученых

Выпуск 6

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

САНКТ-ПЕТЕРБУРГ
2009

В издании «Сборник трудов конференции молодых ученых, Выпуск 6. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ публикуются работы, представленные в рамках VI Всероссийской межвузовской конференции молодых ученых, которая будет проходить 14–17 апреля 2009 года в Санкт-Петербургском государственном университете информационных технологий, механики и оптики.

СПбГУ ИТМО стал победителем конкурса инновационных образовательных программ вузов России на 2007-2008 годы и успешно реализовал инновационную образовательную программу «Инновационная система подготовки специалистов нового поколения в области информационных и оптических технологий», что позволило выйти на качественно новый уровень подготовки выпускников и удовлетворять возрастающий спрос на специалистов в информационной, оптической и других высокотехнологичных отраслях науки. Реализация этой программы создала основу формирования программы дальнейшего развития вуза до 2015 года, включая внедрение современной модели образования.

ISSN 978-5-7577-0335-0
© Санкт-Петербургский государственный университет информационных технологий, механики и оптики, 2009

БЕЗОПАСНОСТЬ И ПРОТИВОДЕЙСТВИЕ ТЕРРОРИЗМУ, ЗАЩИТА ИНФОРМАЦИИ

УДК 681.3.06

ДВУХСТУПЕНЧАТЫЙ АЛГОРИТМ ОБНАРУЖЕНИЯ ДВИЖУЩИХСЯ ОБЪЕКТОВ ПО СИГНАЛАМ СЕНСОРНЫХ МОДУЛЕЙ

Э.В. Козлов
(Объединенный институт проблем информатики НАН Беларуси)
Научный руководитель – к.т.н., с.н.с. Т.В. Левковская
(Объединенный институт проблем информатики НАН Беларуси)

В статье описываются принципы реализации алгоритмов обнаружения движущихся людей и наземной техники в системах пассивной локации. Рассматриваются адаптивные к условиям окружающей среды алгоритмы детектирования полезного сигнала. Описывается разработанный двухступенчатый алгоритм обнаружения движущихся объектов по сигналам сейсмических сенсорных модулей, позволяющий определить местоположение полезных фрагментов без адаптации к уровню шумов и помех, что свидетельствует о его помехоустойчивости. Результаты экспериментов наглядно демонстрируют работоспособность алгоритма обнаружения полезных фрагментов при анализе исходных и очищенных от шума сейсмических сигналов.
Ключевые слова: сенсорный модуль, сейсмический сигнал, детектирование, обнаружение, алгоритм

Введение

В настоящее время при осуществлении охраны часто применяются сейсмические системы пассивной локации (ССПЛ). В этих системах регистрируются и подвергаются обработке сигналы, полученные от размещенных в грунте сейсмических сенсоров. Сигналы возникают при пересечении человеком или транспортным средством зоны обнаружения дачтика(ов). Сейсмические средства удобны для блокировки участков на пересеченной местности и широко применяются при охране периметров объектов [1].

Основные задачи, решаемые ССПЛ – раннее обнаружение вторжения нарушителя на охраняемый объект, идентификация типа нарушителя, а также точное его местоположение.

К главным достоинствам сейсмических сенсоров относятся отсутствие собственного излучения, возможность полного их скрытия вместе с соединительными проводами в грунт. Это сильно снижает вероятность преодоления охраняемой территории даже при осведомленности нарушителя о принципах работы ССПЛ.

К недостаткам ССПЛ относятся низкая помехоустойчивость при заданной вероятности обнаружения ($P_{обн} > 0.9–0.95$) в условиях воздействия разнообразных сейсмических помех природно-климатического и техногенного характера [2].

В табл. 1 приведены основные типы помех, негативно влияющих на работоспособность ССПЛ и способы борьбы с ними [3].

Тип помехи	Стационарность помехи	Примеры	Способы борьбы
I тип	Стационарная во времени и пространстве (не претерпевает заметных изменений более 1 часа)	Снежный покров, промерзание грунта, сейсмический фон	Шумоочистка (например, с помощью вейвлет-преобразования)
II тип	Нестационарная в пространстве и стационарная во времени	ЛЭП, ветер, движение автомобильного и железнодорожного транспорта	Определение частотного диапазона помехи с дальнейшей фильтрацией

III тип	Нестационарная во времени и стационарная в пространстве	Атмосферные осадки, гром	Пространственная и частотная фильтрация
IV тип	Нестационарная во времени и пространстве	Движение человека, животных	Многоканальное обнаружение, метод классификации образов

Таблица 1. Типы сейсмических помех и способы борьбы с ними

Перспективы развития сейсмических систем пассивной локации связаны с созданием информативных средств, способных обнаружить и идентифицировать тип движущихся объектов. Характерные типы нарушителей представлены в табл. 2 [3].

Тип нарушителя	Характеристики	Примеры
Нормальный	Не знаком с принципами работы системы пассивной защиты	Случайные люди, хулиганы, вандалы
Подготовленный (неквалифицированный)	Поверхностно знаком с принципами работы ССПЛ только по внешним признакам (наличие сигнализации и т.д.)	Воры, нарушители государственной границы, наркокурьеры
Подготовленный (квалифицированный)	Осведомлен о принципах работы ССПЛ. Для преодоления используют вспомогательные средства	Террористы, опытные воры, работавшие ранее на объекте люди
Подготовленный (высококвалифицированный)	Полностью разбирается в работе системы. Грамотно используют погодные условия и вспомогательные средства	Разведчики, диверсанты, грабители банков

Таблица 2. Типы нарушителей в зависимости от квалификации

Достоинства и недостатки сейсмического обнаружения обусловливают разработку алгоритма детектирования полезных сигналов, позволяющего увеличить помехоустойчивость при работе в реальных природных условиях и в квазиреальном масштабе времени. Разработка подобного алгоритма, а также усложнение анализа сигналов позволяют значительно улучшить технические характеристики ССПЛ.

Особенности реализации алгоритмов обнаружения движущихся объектов в системах пассивной локации

Постановка задачи

Предлагаемый алгоритм должен обладать высокой помехоустойчивостью и работать в квазиреальном масштабе времени. Входными данными является сейсмический сигнал, полученный от сейсмического сенсора. В результате работы алгоритма проводится анализ сигнала (спектральный, энергетический, классификационный) и выделяется область полезного сигнала.

Простейший блок обработки сигнала – пороговый обнаружитель, осуществляющий детектирование входного сейсмического сигнала по определенным физическим параметрам (амплитуда, длительность, частота) [3].

Анализ в подобной системе базируется на выявлении отличий полезных сигналов и помех. Алгоритмы обработки в самом общем случае схожи, но они подлежат коррек-

тировке в зависимости от возможностей конкретной системы и физических условий ее эксплуатации.

Обработка полученных сейсмических сигналов зачастую затруднена. Поэтому на первом этапе анализа часто применяется фильтрация, позволяющая выделить и исключить нежелательные спектральные составляющие сигналов, тем самым увеличить соотношение «сигнал/помеха» [4].

Большинство детекторов полезного сигнала функционирует следующим образом. Анализируемый сигнал разбивается на кадры (окна анализа). Для каждого кадра рассчитывается вектор параметров, определяющий значение классификационного параметра. В зависимости от алгоритма определяется разница между значениями классификационного параметра для текущего и предыдущего кадров, или разница между значениями классификационного параметра и порога. Сигнал на интервале текущего окна анализа считается полезным, если значение классификационного параметра больше заданного порогового значения. В качестве классификационного параметра чаще всего используются энергия сигнала, кратковременный спектр, кепстр сигнала. Для сглаживания классификационного параметра используется медианная фильтрация, а также размытие полученной последовательности значений классификационного параметра.

Одной из главных проблем является точное определение порогового значения. В условиях нестационарных окружающих шумов более надежно работают адаптивные алгоритмы, в которых характеристики шума и соответственно пороговые значения рассчитываются на интервалах отсутствия полезного сигнала. Порог $\mathrm{Thr(d)}$ может быть определен на основании статистики следующим образом:

$$\mathrm{Thr(d)} = \mathrm{mean(d)} + \lambda \cdot \mathrm{std(d)},$$

где $\mathrm{mean(d)}$ и $\mathrm{std(d)}$ – среднее значение и стандартное отклонение классификационного параметра d соответственно, λ – коэффициент.

Следует отметить, что среднее значение и стандартное отклонение, используемое при вычислении порога, определяется характеристиками окружающего шума. Данный алгоритм работает только на ограниченном интервале стационарности шума. Поэтому для определения порога часто используется метод минимума статистики. Этот метод основан на отслеживании минимума классификационного параметра. Оценка порогового значения определяется с учетом минимального значения из заданного числа последних значений.

Определение местоположения (начальных и конечных границ) полезного сегмента сигнала осуществляется путем анализа классификационного параметра. В современных детекторах для улучшения их характеристик часто используются двухступенчатые алгоритмы. Такой алгоритм предусматривает использование двух пороговых значений: порог по значению классификационного параметра $\mathrm{Thr(d)}$ при определении начала и конца полезного фрагмента сигнала и порог по длительности $\mathrm{Thr\ (n)}$, устанавливающий интервалы подтверждения правильности срабатывания детектора. В общем случае пороги срабатывания детектора полезного сигнала при определении начальной и конечной границ могут принимать разные значения.

Описание двухступенчатого алгоритма обнаружения движущихся объектов по сигналам сенсорных модулей

Анализируемый сигнал разбивается на кадры (окна анализа). Для каждого кадра анализа рассчитываются энергетические (амплитудные) параметры: энергия сигнала в n-ом окне анализа $\mathrm{E(n)}$; средняя энергия сигнала для заданного временного интервала $\mathrm{E_{av}(n)}$; отклонение энергии сигнала от ее среднего значения $\mathrm{D(n)}$; среднее отклонение энергии сигнала для заданного интервала времени $\mathrm{D_{av}(n)}$. Перечисленные выше параметры рассчитываются по формулам (1)–(4):

$$E(n) = \frac{1}{N}\sum_{i=0}^{N} X(i)^2 , \quad (1)$$

$$E_{av}(n) = \frac{1}{2M}\sum_{m=n-M}^{n+M} E(m), \quad (2)$$

$$D(n) = E(n) - E_{av}(n), \quad (3)$$

$$D_{av}(n) = \frac{1}{2K}\sum_{k=n-k}^{n+k} D(k), \quad (4)$$

где N – длительность окна анализа (кадра) в отсчетах; 2*M – интервал усреднения энергии в кадрах; 2*K – интервал усреднения отклонения энергии сигнала от его среднего значения в кадрах.

В качестве классификационного параметра используется значение, рассчитанное в соответствии с выражением (4). Принятие решения о начале полезного фрагмента сигнала осуществляется в два этапа. На первом этапе фиксируется момент времени n, для которого значение классификационного параметра $D_{av}(n)$ больше заданного порогового значения $Thr(d)$. На втором этапе анализируется интервал времени, в течение которого выполняется условие $D_{av}(n) \geq Thr(d)$. Окончательное решение о начале сегмента полезного сигнала принимается, если $D_{av}(n) \geq Thr(d)$ на интервале времени, равном $Thr(n)$ кадрам анализа. Аналогичным образом принимается решение о конце участка полезного сигнала, т.е. условие $D_{av}(n) < Thr(d)$ должно выполняться на интервале времени, равном $Thr(n)$ кадрам.

Результаты экспериментальных исследований алгоритма обнаружения движущихся объектов

Сигналы, полученные от сейсмических сенсоров при движении (ходьбе, беге) человека в зоне обнаружения, представляют собой квазипериодические импульсные последовательности (рис.1). Паузы между импульсами заполнены случайным сигналом (сейсмошумом). Амплитуда огибающей импульсной последовательности увеличивается по мере приближения нарушителя к сейсмоприемнику и убывает при удалении от него примерно по экспоненциальному закону. Скорость нарастания и убывания сейсмического сигнала, возникающего при движении наземной техники, гораздо медленнее, чем при движении человека (группы людей). В большинстве случаев, характерных для охраны объектов, сигнал имеет ширину спектра от 55 до 100 Гц. Наличие отдельных локальных минимумов в спектрах объясняется отражениями сигналов от неоднородностей в грунте и последующим сложением прямого и отраженного сигналов в точке установки сейсмоприемника [5].

Тестирование работы алгоритма обнаружения движущихся объектов было проведено на сигналах 16-ти сейсмических сенсорных модулей. Сейсмокоса, состоящая из 16-ти сенсоров, соединенных электрическим кабелем, была размещена в поверхностном слое грунта, а блок приема и обработки сигналов – в помещении. Сенсоры были проложены в два ряда на расстоянии 5 м. друг от друга и заглублены в грунт на 0,5 м. Расстояние между ними в каждом ряду составляло 10 м. Были записаны сигналы при движении человека и группы людей (2, 3 человека) вдоль сейсмических сенсоров и посередине между ними. Сигналы оцифровывались с частотой дискретизации 1250 Гц, 16 бит на отсчет.

Для проверки алгоритма было разработано программное обеспечение, обеспечивающее ввод сигналов, шумоочистку (вейвлет-преобразование), ДПФ-спектральный анализ, анализ энергетических характеристик сигнала, детектирование полезного сигнала.

Результат анализа исходного сейсмического сигнала двухступенчатым алгоритмом детектирования представлен на рисунке. Вертикальные маркеры соответствуют начальной и конечной границам обнаруженного полезного фрагмента сигнала. Из рисунка видно, что значение классификационного параметра стремится к нулю в отсутствии полезного сигнала.

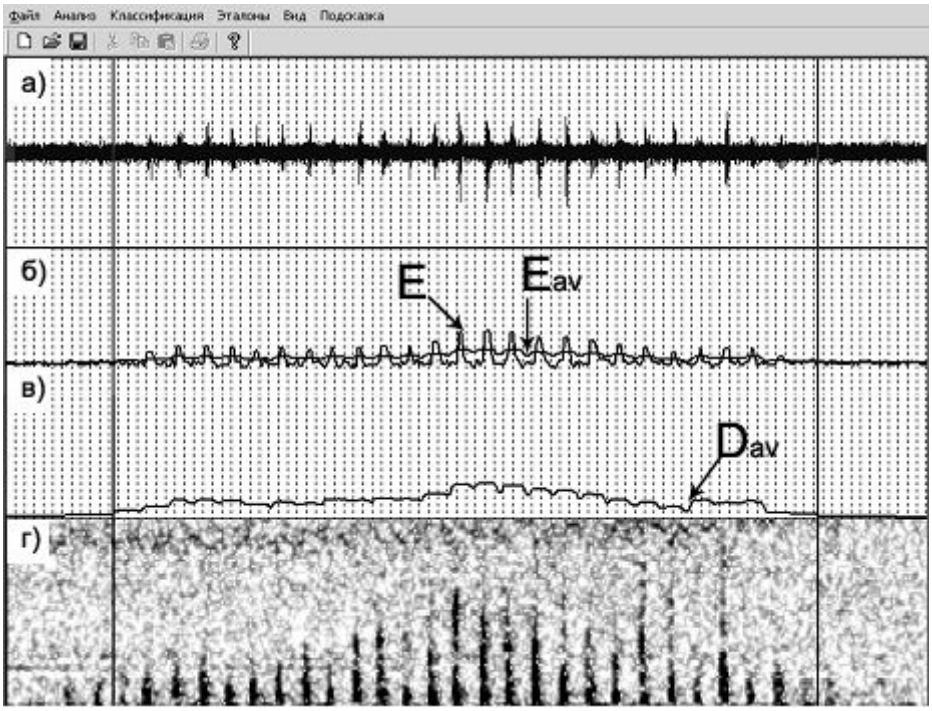


Рисунок. Результат работы алгоритма детектирования полезного сигнала, записанного при пересечении человеком зоны обнаружения сейсмического сенсора а) исходный сигнал; б) энергетические параметры (2), (3); в) классификационный параметр (4); г) ДПФ спектр сигнала

В результате проведенных исследований были определены следующие значения интервалов усреднения: M = 16; K = 16. Таким образом, алгоритм работает с задержкой по времени

$$(M + K) * N = (16 + 16) * 0{,}05 = 1{,}6\,(c),$$

где ΔN – длительность сдвига окна анализа сигнала (64 отсчета при частоте дискретизации Fs = 1250 Гц).

Результаты работы алгоритма при использовании спектральной энергии для расчета классификационного параметра аналогичны результатам, полученным при использовании мгновенных значений энергии сигнала, но при этом время выполнения алгоритма увеличивается. Вместе с тем временной фактор является существенным при функционировании алгоритма в реальном (квазиреальном) масштабе времени.

Заключение

Разработанный алгоритм позволяет определить местоположение полезных фрагментов без адаптации к уровню шумов и помех, что свидетельствует о его помехоустойчивости. Алгоритм функционирует в квазиреальном масштабе времени. Результаты экспериментов наглядно демонстрируют работоспособность алгоритма обнаружения полезных фрагментов при анализе сейсмических сигналов, полученных в условиях реальной фоновой обстановки. При использовании очищенного от шума сигнала, ре-

зультат работы алгоритма практически не меняется, что свидетельствует о его помехоустойчивости. Направления дальнейших исследований связаны с адаптацией алгоритма для обнаружения движущейся наземной техники, а также с разработкой алгоритмов классификации движущихся объектов (людей, наземной техники).

Исследования проводились в рамках задания НИР «Разработка алгоритмов и программного обеспечения обработки информации для решения многопараметрической задачи идентификации воздействия по классам» программы Союзного государства «Функциональная СВЧ электроника-2» (№20071866).

Литература

1. Ларин А.А. Охрана периметра: целесообразность и эффективность //Все о вашей безопасности. – 2004. – №2. – С. 17–20.
2. Звежинский С.С. Повышение функциональной эффективности средств обнаружения //Специальная техника. – 2005. – №5. – С. 11–14.
3. Звежинский С.С. Всепогодная система охраны. Технические особенности построения периметровых вибрационных средств обнаружения //БДИ. – 2005. – №1 (58). – С. 62–66.
4. Уайт Дж. Э. Возбуждение и распространение сейсмических волн. М – «Недра». – 1986. – 261с.
5. Муравьев В.Н. Экспериментальные оценки частотно-временных характеристик сейсмических сигналов и помех для разработки систем охранной сигнализации// Современные проблемы фундаментальных прикладных наук – аэрофизика и космические исследования: Сборник трудов 49-й научной конференции МФТИ, Т.3/ МФТИ. – М.: 2006. – С. 89–92.

УДК 336.71.078.3

БАНК КАК СУБЪЕКТ ДЕЯТЕЛЬНОСТИ ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ

Е.В. Аббясова
(Санкт-Петербургский государственный университет экономики и финансов)
Научный руководитель – д.э.н., д.ю.н., профессор М.Н. Бродский
(Санкт-Петербургский государственный университет экономики и финансов)

В статье представлено описание текущей ситуации по организации деятельности по противодействию легализации доходов, полученных преступным путем, в банке. Приведены основные процедуры механизма противодействия легализации преступных доходов. Проведен анализ правового статуса банка при осуществлении данной деятельности и отраслевой принадлежности возникающих отношений.
Ключевые слова: конференция, банк, легализация, противодействие

Введение

Вопрос о публично-правовом статусе банков как участников отношений по осуществлению контроля за противодействием легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма является одним из самых малоизученных в юридической литературе.

Данное противодействие осуществляется на основании Федерального закона от 7 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма».

Как отмечается в литературе, принятие данного Закона обусловлено ростом правонарушений в сфере финансов и денежного обращения, в особенности с использованием официально действующих организаций (банков, страховых компаний, ломбардов и др.) для легализации (отмывания) доходов, полученных преступным путем, и финансирования терроризма. Указанный Закон выступает основой создания правового механизма во главе с специально созданным уполномоченным органом, призванного противодействовать этому отрицательному явления, негативно влияющему на экономику страны, на реализацию прав и законных интересов граждан, общества и государства [1].

Основная часть

В качестве уполномоченного органа в настоящее время выступает Федеральная служба по финансовому мониторингу. К полномочиям этой Федеральной службы отнесены: контроль и надзор за выполнением юридическими и физическими лицами требований законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма; привлечение к ответственности лиц, допустивших нарушение этого законодательства; сбор, обработка и анализ информации об операциях с денежными средствами или иным имуществом, подлежащих обязательному контролю; осуществление проверок полученной информации о названных операциях, получение необходимых разъяснений; создание единой информационной системы в установленной сфере деятельности; участие в разработке и осуществлении программ международного сотрудничества по данным вопросам и др.

Давая определение основным понятиям, используемым в указанном Федеральном законе, он предусматривает, что *доходы, полученные преступным путем*, – это

денежные средства или иное имущество, полученные в результате совершения преступления. *Легализация (отмывание) доходов*, полученных преступным путем, – это придание правомерного вида владению, пользованию или распоряжению денежными средствами или иным имуществом, полученными в результате совершения преступления.

Финансирование терроризма – это предоставление или сбор средств либо оказание финансовых услуг с осознанием того, что они предназначены для финансирования организации, подготовки и совершения хотя бы одного из преступлений, предусмотренных указанными в Федеральном законе статей УК РФ, либо для обеспечения организованной группы, незаконного вооруженного формирования или преступного сообщества (преступной организации), созданных или создаваемых для совершения хотя бы одного из указанных преступлений.

В качестве мер, направленных на противодействие легализации указанных доходов, данный Федеральный закон устанавливает обязательный контроль и обязательные процедуры внутреннего контроля.

К числу таких организаций относятся, что вполне естественно, и банки. На них лежит обязанность осуществления так называемого «внутреннего контроля».

В данном случае *внутренний банковский контроль* – это деятельность банка по выявлению операций, подлежащих обязательному контролю, и иных операций с денежными средствами, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

Указанному контролю подлежит большинство видов банковских операций: операции с денежными средствами в наличной форме; зачисление или перевод на счет денежных средств; предоставление или получение кредита (займа); операции по банковским счетам (вкладам) и др.

В связи с осуществлением данного контроля на банки возлагаются многочисленные обязанности.

Так, они должны:

1) идентифицировать лицо, находящееся на обслуживании в этом банке;

2) предпринимать обоснованные и доступные в сложившихся обстоятельствах меры по установлению и идентификации выгодоприобретателей;

3) систематически обновлять информацию о клиентах, выгодоприобретателях;

4) документально фиксировать и представлять в уполномоченный орган сведения о денежной операции и лице, ее совершающем;

5) представлять в уполномоченный орган по его письменным запросам информацию о соответствующих денежных операциях.

Закон устанавливает, что банки обязаны документально фиксировать информацию, полученную в результате применения правил внутреннего контроля, и сохранять ее конфиденциальный характер.

Основаниями документального фиксирования информации являются:

запутанный или необычный характер сделки, не имеющей очевидного экономического смысла или очевидной законной цели;

несоответствие сделки целям деятельности организации, установленным учредительными документами этой организации;

выявление неоднократного совершения операций или сделок, характер которых дает основание полагать, что целью их осуществления является уклонение от процедур обязательного контроля;

иные обстоятельства, дающие основания полагать, что сделки осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма.

В случае, если у работников банка возникают подозрения, что какие-либо операции осуществляются в целях легализации (отмывания) доходов, полученных преступным путем, или финансирования терроризма, банк, не позднее рабочего дня, следующего за днем выявления таких операций, обязан направлять в уполномоченный орган сведения о таких операциях.

Банкам запрещается:

открывать счета (вклады) на анонимных владельцев, то есть без предоставления открывающим счет (вклад) физическим или юридическим лицом документов, необходимых для его идентификации;

открывать счета (вклады) физическим лицам без личного присутствия лица, открывающего счет (вклад), либо его представителя;

устанавливать и поддерживать отношения с банками-нерезидентами, не имеющими на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления.

При анализе правового статуса банка как субъекта данной деятельности возникает вопрос об их отраслевой принадлежности отношений, возникающих в процессе осуществления этой деятельности. Ответ на этот вопрос зависит от того, во-первых, какие цели преследует рассматриваемый Закон, во-вторых, каков характер деятельности уполномоченного органа, т. е. Федеральной службы по финансовому мониторингу.

Определяя сферу настоящего Закона, установлено, что он регулирует отношения граждан Российской Федерации, иностранных граждан и лиц без гражданства, организаций, осуществляющих операции с денежными средствами или иным имуществом, а также государственных органов, осуществляющих контроль на территории Российской Федерации за проведением операций с денежными средствами или иным имуществом, в целях предупреждения, выявления и пресечения деяний, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием терроризма.

Таким образом, целями данного Закона выступает:

1) *предупреждение*, *выявление* и *пресечение* деяний, связанных с легализацией (отмыванием) доходов, *полученных преступным путем*;

2) *предупреждение*, *выявление* и *пресечение* деяний, связанных с *финансированием терроризма*.

Отметим, что в первом случае речь идет о распоряжении собственником (владельцем) денежных средств, полученных **преступным** путем, т. е. в результате совершения преступления.

Во втором случае, способ происхождения денег значения не имеет – они могут быть приобретены вполне законным путем. Однако использование их носит **противоправный** характер – финансирование терроризма.

Следовательно, в первом случае определяющим является способ приобретения денежных средств, во втором – способ их использования. В обоих случаях этот способ является преступным.

Что касается второго вопроса – о характере деятельности уполномоченного органа, то прежде всего следует подчеркнуть, что сама Федеральная служба по финансовому мониторингу не относится к категории органов, осуществляющих контроль и надзор за деятельностью кредитных организаций. В равной мере данная Федеральная служба не относится к числу государственных органов, осуществляющих надзор за соблюдением частными лицами правил осуществления финансовых (денежных) операций, уже постольку, поскольку рассматриваемый Закон не устанавливает каких-либо обязанностей для этих лиц в части осуществления ими своих денежных операций. Наконец, следует полагать, что деятельность этого

уполномоченного органа не выражает осуществление финансового контроля, регулируемого нормами финансового права. Хотя – и это надо признать – во многих учениках финансового права деятельность Федеральной службы по финансовому мониторингу освещается в разделе «Финансовый контроль».

В связи с этим отметим, что деятельность по противодействию легализации денежных средств, полученных частными лицами преступным путем, не выражает процессов формирования, распределения и использования государственных денежных фондов, что выступает предметом финансового права. Поэтому деятельность Федеральной службы по финансовому мониторингу и возникающие в связи с этой деятельностью отношения не выступают предметом финансового права.

Следовательно, указанная Федеральная служба не является финансовым органом государства в том смысле, что этот орган обеспечивает осуществление процессов формирования, распределения или использования государственных денежных фондов, либо осуществляет тот или иной государственный контроль за осуществлением этих процессов. Поэтому и сам Федеральный закон «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» нельзя отнести к тем актам, которые содержат нормы финансового права.

Как уже отмечалось выше, данный орган проводит сбор, обработку и анализ информации об операциях с денежными средствами или иным имуществом, подлежащих контролю в соответствии с законодательством РФ, осуществляет проверки полученной информации о названных операциях; при наличии достаточных оснований, свидетельствующих о том, что операция, сделка связаны с легализацией (отмыванием) доходов, полученных преступным путем, или с финансированием терроризма, направляет соответствующие информацию и материалы в правоохранительные органы в соответствии с их компетенцией.

Как правильно, по нашему мнению, отмечается в литературе, анализ положения об этой Федеральной службе позволяет отнести ее к разновидностям *правоохранительных* органов.

Характеризуя данную деятельность, в одной из работ указывается, что «легализация (отмывание) доходов, полученных преступным путем, – относительно новое для России социально-экономическое явление, которое может быть определено как одно из направлений экономической преступности. С деятельностью подобного рода хорошо знакомы правоохранительные органы многих стран»[3]. Это означает, что отношения, возникающие в процессе деятельности Федеральной службы по финансовому мониторингу, относятся к разряду *охранительных* отношений.

В литературе охранительные отношения рассматриваются как отношения, функцией которых состоит в восстановлении нарушенных прав и привлечении нарушителя к юридической ответственности. Охранительные отношения возникают между правоохранительным органом, представляющем государство, и правонарушителем. В данной ситуации в роли правоохранительного органа выступает Федеральная служба по финансовому мониторингу. Вторым субъектом выступает либо лицо, добывшее себе денежные средства преступным путем и пытающее их легализировать, либо лицо, пытающееся или фактически осуществляющее финансирование терроризма.

При этом банки выступают в качестве *поставщика информации* для правоохранительного органа. Поэтому, если быть точным, то данное отношение относится, по нашему мнению, к категории *информационных* правоотношений. Основным назначением этого правоотношения является обеспечение правоохранительных органов сведениями о лицах, которые объективно могут быть субъектами, добывшими денежные средства преступным путем либо осуществляющими финансирование терроризма.

Следует признать, что возложение данной обязанности на банки не вполне укладывается в категорию «банковские операции» в том ее содержании, которое вкладывает в эту категорию Закон «О банках и банковской деятельности». Но это вовсе не ставит под сомнение саму правомерность установления государством для банков обязанности по предоставлению указанной информации. В соответствии со ст. 9 Закона «О банках и банковской деятельности» кредитная организация не может быть обязана к осуществлению деятельности, не предусмотренной ее учредительными документами, за исключением случаев, когда кредитная организация приняла на себя соответствующие обязательства, или случаев, предусмотренных федеральными законами.

Кстати, пп. 7 абзаца 3 ст. 5 Закона «О банках и банковской деятельности» в числе сделок, которые вправе осуществлять банки, называет оказание *информационных* услуг. Понятно, что в данном случае речь идет об информационных услугах, которые банки могут предоставлять своим клиентам. В нашем случае имеется в виду та информация, которую банк обязан предоставлять правоохранительному органу о своих клиентах. Тем не менее, информационная деятельность не является чем-то чуждым для банков. Отметим также, что в соответствии с установленным порядком коммерческий банк предоставляет соответствующие сведения не Федеральной службе по финансовому мониторингу непосредственно, а Центральному банку Российской Федерации. Но это не меняет существа дела, а равно характеристики возникающего при этом общественного отношения – оно по-прежнему остается информационным, которое призвано обслуживать основное правоотношение – охранительное.

Характеризуя рассматриваемое нами информационное отношение, можно отметить следующее:

1) данное правоотношение является *публично-правовым*. Оно является таковым по всем аспектам признания общественного отношения в качестве публично-правового. Так, оно регулируется правовым актом, относящимся в публичной отрасли права. Через это правоотношение реализуется публичный интерес, в первую очередь самого государства, заинтересованного в недопущении приобретения преступным путем денежных средств, их легализации, а также совершения денежных операций, направленных на финансирование терроризма;

2) обязательным субъектом этого правоотношения является само государство, представленное своими уполномоченными органами (Федеральной службой по финансовому мониторингу, а в нашем случае Центральным банком Российской Федерации), которые выступают в качестве *получателей информации*;

3) данное правоотношение, как и любое другое публичное правоотношение, является отношением «*власти* и *подчинения*». Банк в данном правоотношении выступает в роли *обязанного* (подчиненного) субъекта. Причем, обязанность банка не сводится к предоставлению Центральному банку информации об операциях с денежными средствами, подлежащих обязательному контролю. Например, банки обязаны, принимать обоснованные и доступные в сложившихся обстоятельствах меры по определению источников происхождения денежных средств или иного имущества иностранных публичных должностных лиц. Иначе говоря, в определенных ситуациях банки должны проявлять активность в проведении мероприятий, направленных решение задач, поставленных Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма». В равной мере банки обязаны воздержаться от совершения действий, запрет на осуществление которых предусмотрен данным Законом;

4) исполнение банками своих обязанностей, предусмотренных указанным Федеральным законом, обеспечивается мерами юридической ответственности, включая лишение банка лицензии на право осуществления банковской деятельности.

Завершая рассмотрение данного вопроса, отметим, что исполнение обязанностей, возлагаемых на банки Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», порождает у них определенные трудности.

Особого внимания заслуживают так называемые «сомнительные», «подозрительные» или «необычные» операции с денежными средствами. Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» предусмотрено направление в уполномоченный орган сведений об операциях, в отношении которых возникают *подозрения*, что эти операции осуществляются в целях легализации (отмывания) доходов, полученных преступным путем. Данные операции выявляются путем применения разработанных кредитными организациями в соответствии с рекомендациями Банка России Правил внутреннего контроля, которые согласовываются с территориальным управлением Банка России.

В своих рекомендациях Банк России определил критерии выявления и признаки *необычных* сделок. Затем в январе 2005 года выходят письма Банка России, содержащие методические рекомендации об операциях, относительно которых *возникают подозрения*, и операциях *повышенной степени риска*. В конце 2005 года Банком России формируются требования по особому контролю за *сомнительными* операциями, проводимыми в кредитных организациях. Совершенно справедливо отнеся к сомнительным операциям операции, связанные с оптимизацией кредитными организациями налогообложения в интересах клиентов и/или владельцев банков, в дальнейшем Банк России увязывает контроль за проведением подобных сомнительных операций с соблюдением требований федерального закона о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма. Поэтому при отсутствии у кредитной организации первичных документов, являющихся основанием для проведения операции, любое перечисление денежных средств, особенно в крупном размере, можно отнести к сомнительным операциям.

Нормотворческие полномочия Банка России предполагают его исключительные права и обязанности по установлению обязательных для органов государственной власти, всех юридических и физических лиц правил поведения по вопросам, отнесенным к его компетенции и требующим правового регулирования.

В условиях отсутствия однозначного понимания правовых норм по *идентификации* клиентов, выявлению *необычных*, *сомнительных*, *подозрительных* операций, а также учитывая невозможность реализации требований указанного Федерального закона в используемых автоматизированных системах, оказаться в числе злостных нарушителей не трудно.

Заключение

Финансовая система, являясь частью экономических, рыночных взаимоотношений, не может быть отделена от тех процессов, которые происходят в экономике. Невозможна ситуация, когда при наличии проблем в налоговом и таможенном контроле нерешенных вопросов коррупции в государственном аппарате, банковский контроль и банковская деятельность будут идеальны.

Попутно отметим, что активное использование Банком России своего права на отзыв у кредитных организаций лицензии на проведение банковских операций за неисполнение законодательства Российской Федерации в области противодействия легализации доходов и финансирования терроризма соответствует рекомендациям Группы разработки финансовых мер по борьбе с отмыванием денег. В результате за 6 месяцев 2007 г. из 25 отозванных лицензий на осуществление банковской деятельности

в 22 случаях причиной отзыва лицензии явилось несоблюдение требований Федерального закона «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Следовательно, подавляющая часть отзыва лицензий имела место не в силу некачественного осуществления самой банковской деятельности, а в силу неисполнения требований рассматриваемого Федерального закона.

Литература

1. Финансовое право: учебник / отв. ред. Н. И. Химичева. 4-изд., перераб. и доп. М. – 2008. – С. 161.
2. Финансовое право: учеб. – 2-е изд., перераб. и доп. / А. Б. Быля, О. Н. Горбунова, Е. Ю. Грачева [и др.]; отв. ред. Е.Ю. Грачева, Г.П. Толстопятенко. М. – 2007. – С. 44 – 45.
3. Алехин А.П., Кармолицкий А.А. Административное право: Учебник. М. – 2007. – С. 539.
4. Алексеева Д.Г., Пыхтин С.В., Хоменко Е. Г. Банковское право: Учеб. пособие. – 3-е изд., перераб. и доп. М. – 2007. – С. 186.
5. Теория государства и права: Учебник для вузов / Отв. ред. д.ю.н., проф. В.Д. Перевалов. – 3-е изд., перераб. и доп. М., 2007. С. 234; Червонюк В.И. Теория государства и права: Учебник. М. – 2007. – С. 496.

УДК 004.056.5

МОДЕЛЬ СОЗДАНИЯ ПРОФИЛЯ ЗАЩИТЫ ДЛЯ БЕСПРОВОДНОЙ СЕТИ

И.Ю. Иващук
Научный руководитель – к.т.н., доцент А.В. Птицын

В данной работе рассматривается модель построения профиля защиты для беспроводной сети. Приводится система критериев для оценки защищенности беспроводной сети и их противопоставление функциональным требованиями безопасности Общих Критериев для дальнейшего определения оценочного уровня доверия данной сети. Также приводится классификация средств защиты информации, включенных в стандарты семейства 802.11.

Ключевые слова: профиль защиты, функциональные требования безопасности, беспроводная сеть, оценочный уровень доверия

Введение

Общие критерии (ОК) представляют собой хорошо структурированную, универсальную библиотеку требований безопасности, сформулированных в весьма общем виде. Их специализация и конкретизация осуществляется в двух основных конструкциях, определенных в ОК: профилях защиты (ПЗ) и заданиях по безопасности (ЗБ).

ПЗ содержит совокупность требований безопасности, взятых из ОК или сформулированных в явном виде, в которую следует включить оценочные уровни доверия (ОУД). ПЗ позволяет выразить независимые от конкретной реализации требования безопасности для некоторой совокупности объектов оценки (ОО), полностью согласованные с набором целей безопасности. ПЗ предназначен для многократного использования и определения, как функциональных требований, так и требований доверия к ОО, которые полезны и эффективны для достижения установленных целей. ПЗ также содержит логическое обоснование требований и целей безопасности.

Профили защиты являются дальнейшим развитием классов защищенности Оранжевой книги и хорошо известных Руководящих документов (РД) Гостехкомиссии России [1]. Но, в отличие от их жесткой классификационной схемы, число профилей защиты не ограничено. Они содержат более полный, целенаправленный и обоснованный набор требований безопасности, учитывающий назначение, угрозы безопасности и условия применения объекта оценки.

Профиль защиты беспроводной сети

Профиль защиты предназначен для сертификации средств защиты информации продуктов и систем ИТ и получения сопоставимых оценок их безопасности. Профили защиты служат также основой для разработки разделов требований безопасности информации (заданий по безопасности) на конкретные изделия ИТ [2].

Именно официально принятые профили защиты образуют построенную на основе ОК и используемую на практике нормативную базу в области информационной безопасности (ИБ). В России эту работу курирует Государственная техническая комиссия при Президенте РФ (Гостехкомиссия России). Представляется, что анализ разрабатываемых профилей, произведенный на относительно ранней стадии, является вполне своевременным и, более того, весьма важным, поскольку позволяет выявить только намечающиеся тенденции, взять на вооружение положительный опыт и попытаться избежать типичных ошибок. Вообще говоря, профили защиты могут характеризовать отдельные сервисы безопасности, комбинации подобных сервисов,

реализованные, например, в операционной системе, а также прикладные изделия ИТ, для которых обеспечение информационной безопасности критически важно.

В качестве ОО при разработке ПЗ беспроводной сети (БС) рассматривается вся сеть, а не отдельные ее сегменты. Разработка профилей защиты для беспроводных сетей позволит аттестовать их в соответствии с международным стандартом ISO 15408.

Критерии защищенности беспроводной сети

Суммируя знания по существующим ныне стандартам в мире WLAN, я выделила ряд критериев для проведения анализа, а впоследствии и оценки защищенности беспроводной сети.

Было выделено две основные группы критериев, в соответствии с которыми и происходит оценка сети:

- Криптографические критерии
- Критерии аутентификации.

Каждая группа включает в себя ряд компонентов.

Криптографические критерии:

1. Криптографические алгоритмы
2. Длина используемого ключа
3. Использование динамических или статических ключей
4. Длина вектора инициализации
5. Технология проверки целостности сообщений (MIC, CCMP)

Критерии аутентификации

6. Протокол
7. Наличие сервера аутентификации
8. Взаимная аутентификация
9. Использование цифровых сертификатов

Соответствие критериев защищенности ФТБ

Каждому из вышеприведенных критериев противопоставляется либо целое семейство, либо отдельные его компоненты функциональных требований безопасности (ФТБ) 2 части ОК. В ходе предыдущих исследований было выявлено следующее соответствие, результаты которого предоставлены в таблице.

Критерии	ФТБ
1. *Криптографические критерии*	
1.1 Алгоритм	FCS_COP.1.1
1.2 Длина ключа	FCS_CKM.1.1
1.3 Динам./стат. ключ	FCS_CKM.2.1
1.4 Длина вектора	FCS_COP.1.1
1.5 Проверка целостности	FCS_COP.1.1
2. *Критерии аутентификации*	
2.1 Протокол	FIA_UAU
2.2 Сервер аутентификации	FIA_SOS
2.2.1 Взаимная аутентификация	FPT_SSP.2
2.3 Цифровые сертификаты	FDP_DAU

Таблица. Соответствие критериев защищенности беспроводной сети ФТБ

Таким образом, чтобы сформировать семейство ПЗ для БС необходимо выработать определенную модель, так как семейство ПЗ представляет собой

совокупность тесно связанных профилей защиты, которые обычно относятся к одному и тому же типу продукта или системы ИТ. Разработка ПЗ может, таким образом, рассматриваться как часть процесса разработки семейства ПЗ.

Модель профиля защиты

Разработка семейств ПЗ может идти по следующим направлениям:

- разработка совокупности иерархически связанных ПЗ для одного и того же типа ОО (ПЗ можно считать иерархическим по отношению к другому ПЗ семейства, если он включает все требования безопасности ИТ, специфицированные в последнем);
- разработка совокупности ПЗ, каждый из которых относится к различным компонентам системы ИТ [3].

В своей работе я придерживаюсь первого варианта, потому что развитие беспроводных технологий происходило таким образом, что каждый последующий стандарт включал в себя те или иные средства защиты предыдущего, как то алгоритмы шифрования данных либо алгоритмы аутентификации.

Следуя полученным критериям для оценки защищенности БС и их последующим соответствием ФТБ ОК, можно сказать, что основное различие между членами семейства ПЗ будет заключаться именно на уровне этих требований безопасности.

Но при разработке ПЗ особое значение уделяется также среде безопасности ОО. И если при непосредственной оценке защищенности БС мы не учитывали этот критерий, то в моей дальнейшей работе он играет далеко не последнюю роль. В ОК ему соответствует семейство физическая защита функций безопасности ОО (FPT_PHP).

Если семейство ПЗ относится к конкретному типу ОО, важно чтобы было четкое различие между различными членами семейства. Другими словами, должны быть четкие различия в требованиях безопасности ОО. Это связано с тем, что ПЗ должен, по крайней мере, отличаться целями безопасности, которые определяют выбор требований безопасности ИТ. В качестве примера, можно рассмотреть случай, когда два ПЗ специфицируют одну и ту же совокупность ФТБ, но разные требования доверия безопасности (ТДБ). Допускается мотивировать более низкое требование безопасности возрастанием безопасности среды ОО. Такие различия должны быть отражены в целях безопасности.

Таким образом, профиль защиты в семействе ПЗ должны различаться ОУД к ОО. Эти уровни определяются исходя из используемых средств защиты информации при построении беспроводной сети. Классификация существующих ныне средств защиты приведена на рисунке.

Заключение

Профиль защиты является неотъемлемой частью процедуры сертификации средств защиты информации продуктов и систем ИТ и получения сопоставимых оценок их безопасности. При разработке семейства профилей защиты за основу берется базовый пакет доверия к которому, в зависимости от ценности активов, добавляют те или иные дополнительные требования доверия.

В ходе работы был получен набор семейств и компонентов ФТБ, которые должны быть включены во все ПЗ семейства (базовый пакет доверия) и являются основополагающими при их построении. Для определения оценочного уровня доверия к беспроводной сети были получены критерии оценки защищенности для подобной сети. Проведя исследования существующих ныне стандартов семейства 802.11, этим критериям были противопоставлены включенные в стандарты средства защиты информации.

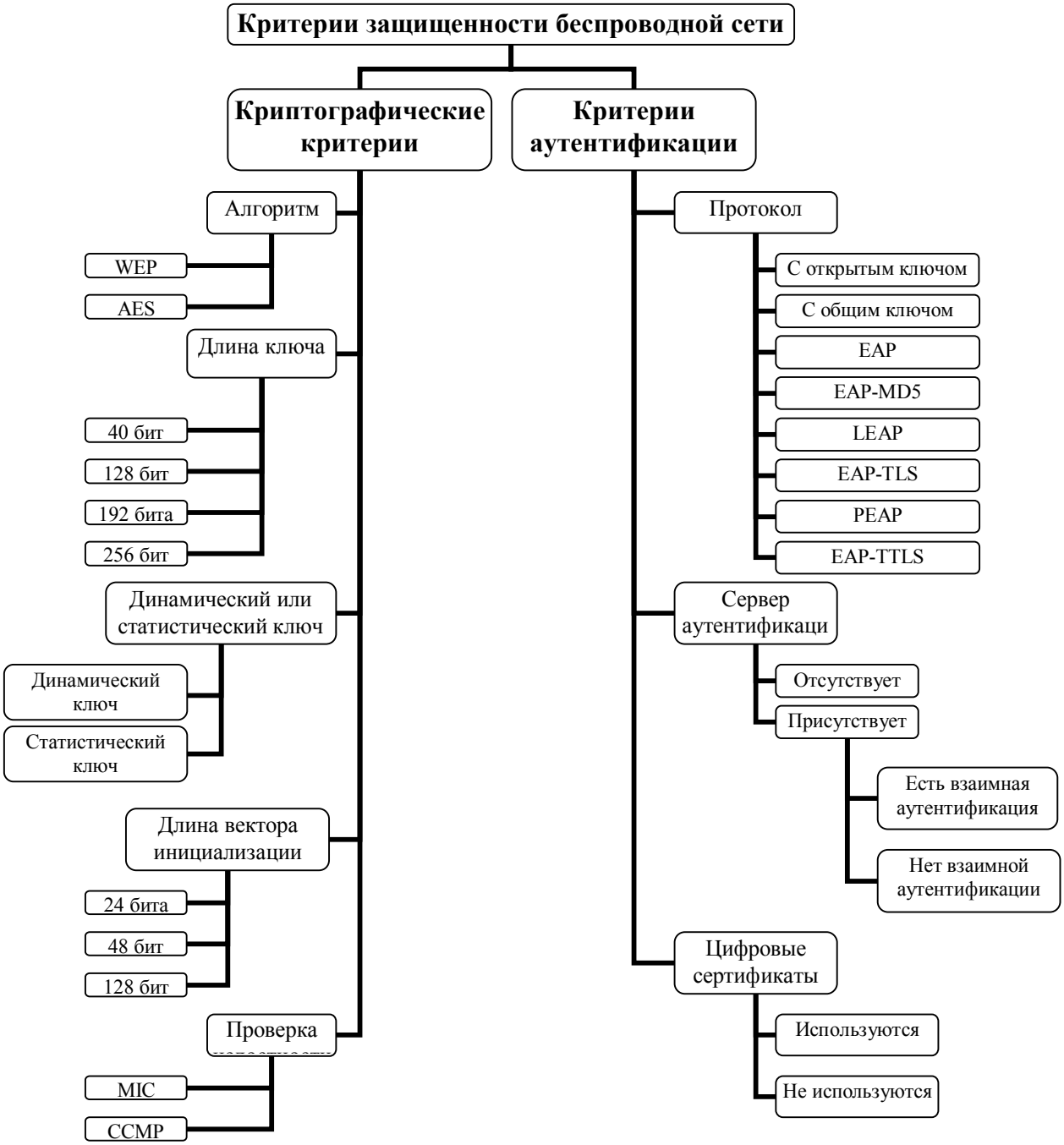


Рисунок. Классификация средств защиты информации беспроводной сети

Литература

1. Руководящий документ ФСТЭК «Безопасность информационных технологий». Федеральная служба по техническому и экспортному контролю, 2002. 1, 2, 3 часть.
2. Руководящий документ ФСТЭК «Руководство по разработке профилей защиты и заданий по безопасности». Федеральная служба по техническому и экспортному контролю, 2003.
3. Руководящий документ ФСТЭК «Руководство по формированию семейств профилей защиты». Федеральная служба по техническому и экспортному контролю. – 2003.

УДК 004.056

ПРОГРАММНО-ИНСТРУМЕНТАЛЬНЫЙ КОМПЛЕКС ПОДДЕРЖКИ И МЕТОДИКА ПРИМЕНЕНИЯ ФУНКЦИОНАЛЬНОЙ МОДЕЛИ «ОБЩИХ КРИТЕРИЕВ»

О.Е. Зайцев
Научный руководитель – к.т.н., доцент А.В. Любимов

Для автоматизации поддержки процесса оценки защищённости ИТ по стандарту «Общие Критерии» (ОК), а также для решения ряда практических задач в данной области необходимо разработать программно-инструментальный комплекс поддержки и методику использования функциональной модели ОК. В данной статье предлагается такая методика и комплекс.

Ключевые слова: функциональная модель, общие критерии, комплекс поддержки, генерация отчёта, выгрузка таблицы

Введение

Национальный стандарт безопасности ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий» («Общие критерии») действует в России с 1 января 2004 года. Опыт использования «Общих Критериев» говорит о том, что применение методологии ОК способствует существенному повышению качества оценки и разработки продуктов и систем ИТ. Таким образом, оценка защищенности ИТ по ОК является перспективным направлением, а проблемы связанные с использованием ОК – очень актуальными.

Решению многих задач способствует представление «Общих Критериев» в виде формальных моделей. Как правило, функциональная модель является основной и наиболее применяемой на практике. Определив базовые параметры функциональной модели ОК [1], она может быть построена с помощью методики структурного анализа и проектирования систем SADT [2], скорректированной с учетом специфики ОК как объекта моделирования.

В настоящей работе представлены результаты разработки программно-инструментального комплекса поддержки построенной функциональной модели деятельности по оценке защищенности ИТ, благодаря которому функциональная модель ОК и общей методологии оценки (ОМО) может использоваться для решения широкого спектра практических задач, возникающих при подготовке и проведении оценки. Также описана и методика применения функциональной модели и комплекса поддержки.

1. Программно-инструментальный комплекс поддержки модели

Функциональная модель деятельности по оценке защищенности ИТ по стандартам ОК и ОМО реализована в виде совокупности таблиц реляционной БД во внутреннем формате программного средства процессного моделирования All Fusion BPwin. На стадиях построения и сопровождения доступ к модели осуществляется через графический интерфейс BPwin, который отображает модель в виде иерархии функциональных диаграмм и предоставляет средства навигации по модели, ее редактирования и расширения. Наряду с BPwin, программно–инструментальный комплекс поддержки модели включает в себя Internet браузер (например Microsoft Internet Explorer) и компоненты Microsoft Office (в частности – Word), которые служат для работы с представлениями модели в пользовательских форматах. Дополнительно могут использоваться и другие средства, входящие в линейку продуктов All Fusion, такие как Data Modeler и Component Modeler. Их включение в программно–

инструментальный комплекс поддержки модели целесообразно в том случае, если модель используется для разработки ПО поддержки оценки. Точный состав программно-инструментального комплекса зависит от конкретного спектра задач, решаемых на данной стадии процесса оценки. Важно отметить, что комплекс позволяет автоматизировать весь процесс поддержки документации процесса оценки, за счет того, что исходные документы – ОК и ОМО изначально представлены в структурированной электронной форме.

Таким образом, в распоряжении пользователя (оценщика, разработчика, заявителя) имеется визуальное структурированное представление процессов и действий по оцениванию ИТ, предусмотренных ОК и ОМО, а также основных документов, используемых в процессе оценки (профиль защиты, задание по безопасности, технический объект оценки), их разделов и подразделов. С одной стороны, это представление обеспечивает максимальную компактность и наглядность, а с другой – имеет формализованную форму, гарантирующую достаточную точность и актуальность.

Встроенные в BPwin средства генерации отчетов позволяют получить широкий набор настраиваемых представлений модели, как в формате MS Word, так и в формате HTML, который позволяет: для оценщика – автоматизировать многие действия по оцениванию, в частности – определение состава и последовательности процессов и действий по оцениванию, а также состава необходимой документации, ее содержания и регламента использования в зависимости от конкретного продукта ИТ и согласованного оценочного уровня доверия (ОУД); для разработчика, потребителя и заказчика – упростить и прояснить использование РД, что помогает лучше подготовится к оценке (например – правильно выбрать ОУД), а также способствует лучшему пониманию и более широкому распространению стандарта ОК.

Как сама модель, так и ее представления могут использоваться в качестве электронного справочника по процессам (действиям) и документам оценки. На рис. 1 представлен пример просмотра HTML представлений модели в браузере Internet Explorer.

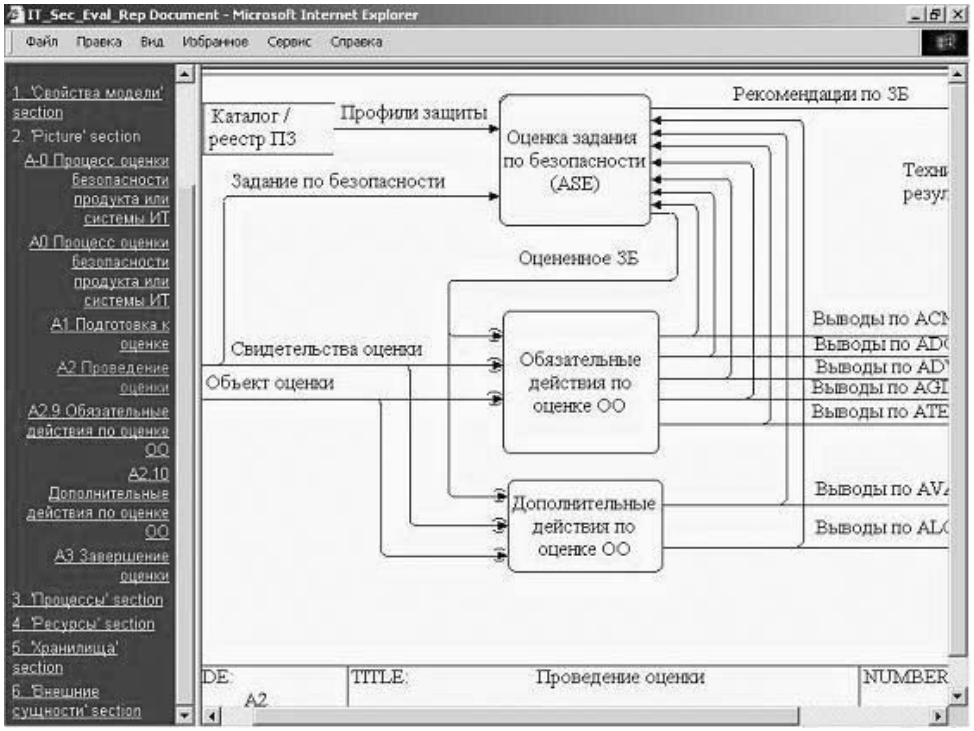


Рис. 1. Просмотр диаграммы детализации процесса «Проведение оценки» в формате HTML

Для каждого документа (раздела, подраздела), используемого в процессе оценки, программные средства поддержки, в частности, позволяют:

– определять, какой процесс (или элемент действий оценщика/разработчика) порождает документ (раздел), в каких процессах (элементах действий) он используется;

– получать описание его содержания со ссылкой на соответствующие разделы (параграфы, пункты) стандарта.

Для каждого процесса (элемента действий оценщика/разработчика) программные средства поддержки, в частности, позволяют:

– определять состав входных и выходных документов (разделов, подразделов);

– получать описание его целей, содержания и условий выполнения со ссылкой на соответствующие разделы (параграфы, пункты) стандарта.

Генерируемые справочники по процессам и документам оценки имеют вид таблиц с варьируемым составом полей изображённой на рис. 2.

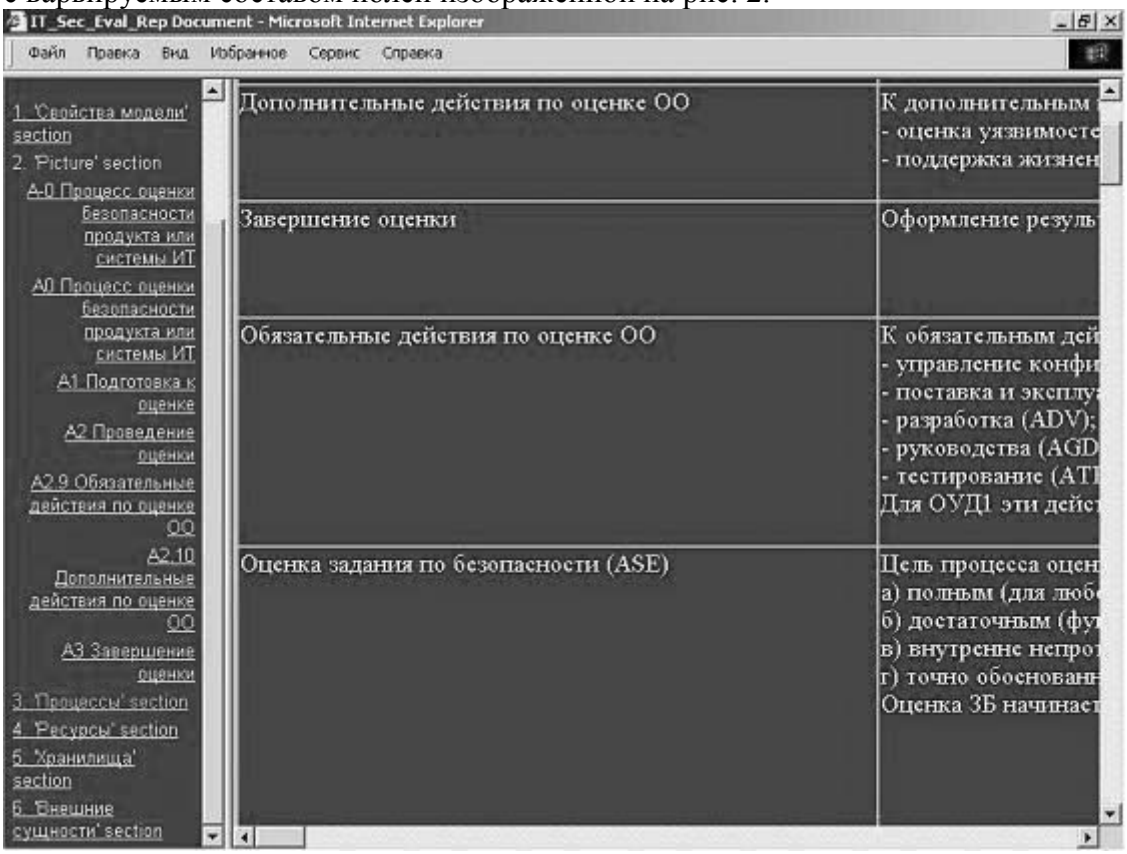


Рис. 2. Представление справочника по процессам оценки в формате HTML

Навигацию по иерархии процессов модели можно осуществлять как средствами Internet Explorer, так и непосредственно средствами BPwin. Последнее более удобно (рис. 3), но требует некоторых навыков работы с этим приложением.

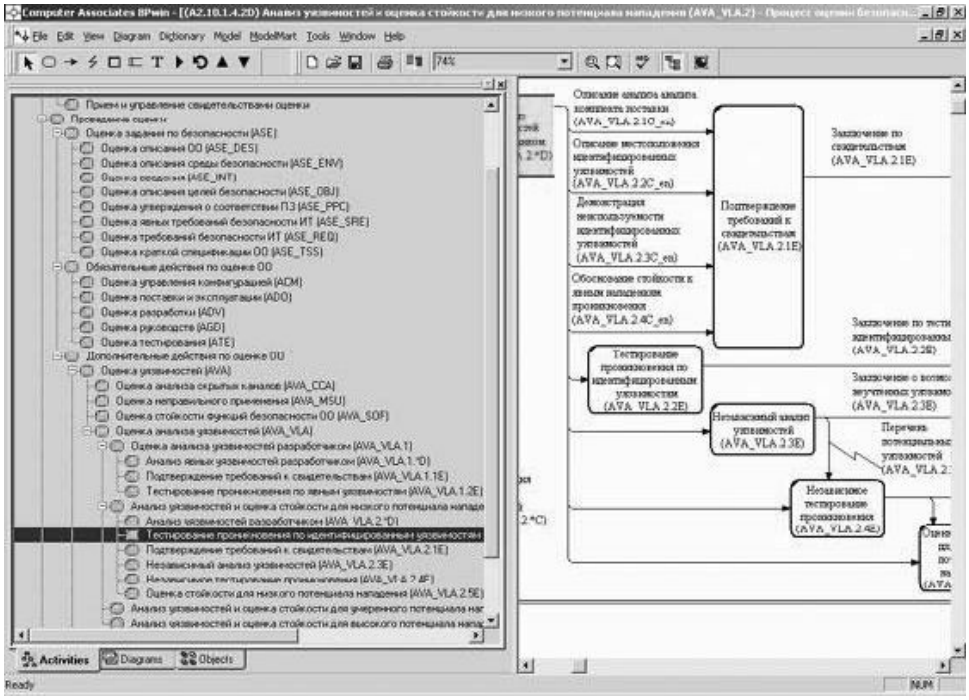


Рис. 3. Навигация по иерархии процессов модели средствами BPwin Model Explorer

2. Методика использования функциональной модели и комплекса поддержки

В соответствии с ОК и ОМО, одним из ключевых этапов подготовки к оценке являются действия по подготовке свидетельств, необходимых при проведении оценки объекта оценки: «Оценщику рекомендуется совместно с заявителем представить список требуемых свидетельств оценки. Этот список может являться совокупностью ссылок на документацию. В нем следует привести достаточную информацию (например, аннотацию каждого документа, или, по меньшей мере, его полное название и перечень разделов, представляющих интерес), позволяющих оценщику легко найти требуемое свидетельство» [3]. Подобного рода совместные действия заявителя и оценщика в методологии ОК не регламентированы, однако именно они во многом предопределяют конечный результат процесса оценки и сертификации. Это в равной мере относится и к другим, не регламентированным этапам процесса оценивания, например – к бизнес планированию работ или к проектированию и согласованию технических результатов оценки. Далее представлены методические рекомендации по использованию функциональной модели при выполнении этих и подобных им действий.

2.1. Подготовка, согласование и контроль конфигурации свидетельств оценки

Все упомянутые в заголовке действия выполняются совместно оценщиком и заявителем при участии разработчика. Заявитель отвечает за обеспечение оценщика свидетельствами оценки, однако начальную версию списка свидетельств оценки обязан предоставить оценщик. Подобный список без труда генерируется по построенной в работе функциональной модели с помощью встроенных средств BPwin и выгружается в файл Microsoft Word в виде табл.1.

Таблица 1. Вид таблицы, генерируемой BPwin при определении списка свидетельств

Имя документа или раздела	Имя объемлющего документа или раздела	Аннотация	Ссылка на стандарт

Аналогично можно получить список свидетельств оценки для любого компонента, семейства и класса ОК, а также для полного процесса оценивания. Настраиваемый шаблон отчета позволяет включать в результирующие таблицы дополнительные столбцы, содержащие практически любую информацию о документе (разделе), которая имеется о нем в модели (например, назначение или порождающий его процесс на стороне разработчика).

Подготовленный таким образом список свидетельств оценки оценщик передает заявителю, как лицу, ответственному за обеспечение свидетельств. Задачей заявителя является дальнейшее согласование списка с разработчиком и оценщиком в ходе подготовки к оценке. Согласованный список свидетельств оценки, представленный в вышеописанной форме, является основным документом, в соответствии с которым выполняется контроль конфигурации свидетельств оценки при реализации предусмотренного стандартом действия «Прием и управление свидетельствами оценки» в ходе процесса «Подготовка к оценке».

2.2. Бизнес планирование работ по оценке и согласование ОУД

При проведении работ по оценке и сертификации продуктов и систем ИТ одной из основных организационных задач является согласование между заявителем, оценщиком и разработчиком состава работ, трудозатрат, сроков и стоимостей, то есть – согласование бизнес плана. Эти параметры, в свою очередь, решающим образом зависят от согласованного ОУД. В задачу оценщика входит разъяснение заявителю финансовых и организационных последствий решения выбора ОУД, в частности – квалифицированное обоснование стоимости. Из опыта зарубежных сертификаций известно, что оценивание продукта или системы корпоративного масштаба по ОУД4 (в настоящее время этот уровень считается оптимальным для корпоративных ИТ) длится не менее года и стоит не менее $500,000. Повышение ОУД ведет к резкому увеличению, как сроков, так и стоимости оценки. Эти соображения иногда заставляют заявителя снижать запланированный (например, из соображений конкурентоспособности) ОУД, и делать это лучше до начала процесса оценки.

Исходным действием для составления бизнес плана является получение перечня работ по оценке для согласованного ОУД, их краткого содержания и планируемого результата каждой работы. Такой перечень может быть достаточно просто извлечен из функциональной модели стандартными средствами генерации отчетов, встроенными в BPwin. Если в UDP (User-Defined Properties) функциональных блоков модели завести числовые значения таких характеристик как «трудозатраты» и «стоимость», они также будут присутствовать в перечне, и для получения полноценного бизнес плана необходимо будет только привязать начало работ к конкретным датам. В итоге, получаем таблицу (табл. 2), выгруженную в файл Word.

Таблица 2. Вид таблицы, генерируемой BPwin при определении перечня работ по оценке для согласованного ОУД

Вид работ	Содержание работ	Ссылка на стандарт	Результат	Трудозатраты (чел.-мес.)	Стоимость (у.е.)

Подведение итогов также можно автоматизировать, если при генерации отчета выбрать Microsoft Excel. Совершенно аналогичным образом можно получить полный перечень работ для всего процесса оценивания.

Заключение

Оценка защищенности ИТ по ОК является перспективным направлением, а проблемы связанные с использованием ОК – очень актуальными. Построенная функциональная модель и программно-инструментальный комплекс ее поддержки способствуют решению многих практических задач в области оценки безопасности ИТ. Методика применения функциональной модели и комплекс поддержки в дальнейшем будут расширены.

Литература

1. Зайцев О.Е. Базовые параметры формальных моделей оценки защищенности ИТ по «Общим Критериям» – Научно-технический вестник СПбГУ ИТМО. Выпуск 39 «Исследования в области информационных технологий – труды молодых ученых». ИТМО, Санкт-Петербург. – 2007. – С. 20–26
2. Зайцев О.Е., Любимов А.В., Суханов А.В. Подходы к структурному моделированию основных компонентов безопасности ИТ «Общих Критериев». – Труды 11-й научно-технической конференции «Теория и технология программирования и защиты информации. Применение вычислительной техники» Санкт-Петербург, 18 мая 2007 г. – С. 56–60
3. РД Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий (проект). – ФСТЭК России. – 2005.

УДК 004.056

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ДАННЫХ ПОЛЬЗОВАТЕЛЕЙ СОЦИАЛЬНЫХ СЕТЕЙ

А.С. Ермилова
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Данная статья посвящена исследованию актуальных проблем безопасности данных пользователей социальных сетей. Исследование проведено на основе самой популярной социальной сети в России – vkontakte.ru. В результате исследования составлен перечень угроз безопасности данных пользователей, выявлены основные каналы и методы утечки информации, проведен анализ используемых методов и средств защиты. Так же рассмотрены основные проблемы правового регулирования отношений в области обеспечения конституционных прав и свобод граждан в информационной среде.

Ключевые слова: социальные сети, персональные данные, угрозы безопасности, каналы и методы утечки информации, средства защиты

Введение

На сегодняшний день в России наиболее успешно развиваются различные социальные сети, направленные на построение сообществ в Интернете людей со схожими интересами и/или деятельностью. Порталы социальных сетей содержат персональные данные миллионов пользователей, тем самым, обеспечивая возможность разнообразного общения между участниками и поиска друг друга на портале и представляя собой огромные on-line директории. Таким образом, возникает ряд вопросов, касающихся обеспечения безопасности персональных данных пользователей данных ресурсов и правого регулирования отношений в области соблюдения Законодательства РФ.

Основная часть

На сегодняшний день достаточно актуален вопрос безопасности данных пользователей социальных сетей. По данным статистики посещаемости сайтов в Интернете [4], первое место занимает социальная сеть vkontakte.ru (средневзвещенное количество обращений за месяц 44 273 718). Данный сайт позиционирует себя как сетевой проект, который помогает поддерживать связь с близкими людьми. На конец февраля 2009 г. на сайте зарегистрировано около 28 000 000 пользователей, 41% из которых занимают жители Москвы, 26% – жители Санкт-Петербурга.

При этом каждая пользовательская страница содержит персональные данные пользователей. Под персональными данными здесь понимается любая информация, касающаяся или могущего быть идентифицированным лица [2]. Как правило, пользователи размещают легитимные данные, такие как: фамилия, имя, дата рождения, контактные данные (номер телефона, icq и прочее), сведения об образовании, место работы, должность, личные фотографии, видео, личные связи (друзья, партнеры, знакомые), заметки, открытая переписка («стена»). Стоит отметить, что информация на сайте актуальна, регулярно обновляется самими пользователями и четко структурирована. Таким образом, подобная социальная сеть представляет собой огромную online директорию.

Теоретически, личные данные пользователей скрыты от посторонних глаз и не доступны для поисковых систем (Yandex, Google, Rambler и других). Но в то же время информация открыта, и методом элементарного поиска можно составить досье на любого зарегистрированного в социальной сети пользователя, даже не нарушая статей закона. Пользователи самостоятельно размещают личную информацию и не

задумываются о возможных последствиях. Стоимость подобной базы данных на рынке составляет свыше 11 млн евро. В то время как обслуживание и поддержка сайта, по данным глобальной сети порядка, по подсчетам 118, 4 млн. рублей ежемесячно.

Рассмотрим этапы взаимодействия пользователя с базой данных веб-вайта.

Первый этап. Допустим пользователь зарегистрирован в социальной сети. Доступ на веб-сайт происходит через интернет-браузер. Как правило, каждый из пользователей заходит на свою страницу с разных IP-адресов, например, с домашнего компьютера, с работы и из интернет-кафе.

Для работы с сайтом предусмотрен механизм аутентификации по email (выступает в качестве логина) и пароль. В качестве пароля непосредственно с сайтом vkontakte используются набор цифр и букв, при вводе пользователем специальных символов как правило возникают проблемы идентификации, связанные с используемой кодировкой браузера. При настройках по умолчанию, в браузер пользователя прописывается значение cookie. При каждом последующем заходе на основе анализа значения cookie из браузера пользователя на странице появляется либо именное приветствие (если есть установленное значение cookie), либо первоначальная форма с запросом имени пользователя (если значение cookie не установлено).

Cookie – это некоторая текстовая информация, которую сервер передает браузеру. Браузер будет хранить эту информацию и передавать ее серверу с каждым запросом как часть HTTP заголовка. Одни значения cookie могут храниться только в течение одной сессии, они удаляются после закрытия браузера. Другие, установленные на некоторый период времени, записываются в файл. Обычно этот файл называется 'cookies.txt' и лежит в рабочей директории установленного на компьютер браузера.

Так как доступ к одному и тому же браузеру может быть осуществлен ни одним пользователем, то любой другой пользователь может получить доступ к данным пользователя подняв из нужной директории cookie, которые в данном случае позволяют получить доступ к email и хэшу паролю. Хэш пароля – это некоторая строчка, вычесленная по паролю. По ней без применения дополнительных средств невозможно вычислить пароль, но это и не нужно, так как можно копировать его значение в браузер и получить доступ к «вашему» аккаунту (только не возможно его поменять без последствий для пользователя).

На данном этапе так же возможен перехват пароля с помощью программ – KeyLoggers и социальной инженерии.

Следующим этапом происходит взаимодействие пользователя с базой данных сайта. Пользователь может свободно просматривать и копировать открытые данные на других аккаунтах. Кроме того, предусмотрена форма поиска по всем возможным параметрам. Каждый пользователь может ограничить доступ к персональным данным в настройках (параметрах) страницы.

На этом этапе непосредственной работы с сайтом возможны следующие методы утечки информации: фишинг, фишинг в приложениях, кража личной информации.

По результатам анализа каналов и методов утечки данных пользователей, можно выделить следующие угрозы: уничтожение, изменение, блокирование, копирование, распространение персональных данных и другие несанкционированные действия.

При исследовании используемых методов и средств защиты, можно сделать вывод о том, что администрация сайта использует передовые технологии защиты от вирусов, фишинга и др. вредоносного программного обеспечения. Но используемые методы не доказывают своей эффективности перед пассивными методами сбора информации по отдельным пользователям. Более того, на основании полученной информации из данной социальной сети, можно расширить сбор дальнейшей информации, которая при определенном варианте ее использования может стать критической. Например, можно построить топологию сети отдельной организации. На веб-ресурсе данной компании в

разделе контактных лиц, как правило, есть контактные данные первых лиц организации. С помощью поиска в социальной сети есть возможность собрать данные по первым лицам и менеджерам компании. С помощью любой другой аналогичной социальной сети, например, мой мир, можно получить email-ы и продолжить сбор необходимой информации для последующей атаки. Для «вскрытия» email можно применить различные программы по восстановлению паролей различными методами. Например, предварительная атака, атака полным перебором, атака по маски, простая и комбинированная атака по словарю, атака по предварительно рассчитанным Rainbow – таблицам и т.д. Так же на рынке программного обеспечения представлено достаточно много программного обеспечения, предназначенного для пассивного сбора информации.

Стоит отметить, что социальная сеть не несет ответственности за персональные данные пользователя, что указано в пользовательском соглашении. Соответственно, действие Федерального Закона «О персональных данных» не распространяется на неё. На примере запуска «новой» оболочки социальной сети vkontakte.ru – ресурса durov.ru, использующей в качестве своей базы данных копию БД первоначального ресурса без информирования пользователей и получения с их стороны разрешения на использование их персональных данных, можно сделать вывод о том, что администрация ресурса не заинтересована даже в косвенном выполнении конституционных прав и свобод граждан в информационной среде.

Заключение

В результате исследования безопасности данных пользователей социальных сетей, можно сделать вывод о том, что пользователи социальных сетей в первую очередь должны самостоятельно контролировать вопросы безопасности их персональных данных в открытых ресурсах. Здесь особенное внимание стоит уделять персональным данным, которые публикуются на веб-ресурсах. Для предотвращения фишинг атак эффективно использовать программы-файрволы, межсетевые экраны и антивирусное программное обеспечение. Для предотвращения доступа к персональных данным другого пользователя с той же машины, необходимо изменить первоначальные настройки используемого браузера.

Стоит отметить, что администрация ресурса не несет ответственности за дальнейшее распространение персональных данных пользователей и их безопасность, что прописано в пользовательском соглашении. При исследовании проблем правого регулирования отношений в области обеспечения конституционных прав и свобод граждан в информационной среде, то стоит отметить их не соблюдение в данной социальной сети.

Литература

1. Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
2. Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».
3. Постановления Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
4. Материалы статистики в Интернете сайта www.liveinternet.ru
5. Материалы сайта www.vkontakte.ru

УДК 004.056:001.57:004.82

ВЫБОР МЕТОДОВ И СРЕДСТВ ОНТОЛОГИЧЕСКОГО АНАЛИЗА СТАНДАРТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.В. Андреева
Научный руководитель – к.т.н., доцент А.В. Любимов

В данной работе проводится выбор методов и средств для онтологического анализа стандартов информационной безопасности. Рассмотрены разные подходы к построению онтологий и представлен краткий обзор их преимуществ и недостатков.

Ключевые слова: информационная безопасность, моделирование, онтология, стандарты

Введение

В настоящее время одним из перспективных направлений в моделировании бизнес-процессов является использование онтологий как спецификаций некоторой предметной области. Онтологии позволяют концептуализировать предметную область, то есть теоретически организовать накопленные знания – определить понятия, отношения и механизмы управления, необходимые для описания процессов решения задач в избранной предметной области. Кроме того, преимуществом использования онтологий является возможность анализа, накопления и повторного использования знаний в предметной области, полученных из разных источников.

В представленной работе проводится выбор методов и средств онтологического анализа стандартов информационной безопасности. Онтологическая модель данной предметной области позволит стандартизировать терминологию различных документов по информационной безопасности, а также представить структуру их текста в стандартизированном виде, читаемом машиной. Общая постановка задачи онтологического анализа стандартов информационной безопасности и ее актуальность для решения широкого спектра практических задач, в первую очередь – для построения гибридных стандартов и систем защиты информации приведена в [1, 2].

Обзор литературы не выявил попыток моделирования онтологий в области информационной безопасности в России. Среди зарубежных разработок самой объёмной из найденных является австрийская онтология Security Ontology [3], разработанная с использованием стандарта OWL-DL. Средства управления для данной онтологии были взяты из различных стандартов по информационной безопасности, в том числе - ISO/IEC 27001.

Участниками данного проекта также проводятся исследования в области моделирования онтологии по стандарту ISO/IEC 27001 [4], которые проводятся с использованием стандарта OWL и других разработок консорциума W3C (RDF, SPARQL, SWRL). Для работы с онтологией используется архитектура OntoWorks.

При всей своей важности, проект Security Ontology разрабатывается, в первую очередь, в целях обучения. Поэтому его результаты имеют в значительной степени эклектичный характер и, безусловно, не представляют в полной мере методологии стандартов информационной безопасности, которые использовались при построении онтологий. По этим причинами ни методики, ни результаты проекта не могут быть существенным образом использованы при решении значимых практических задач информационной безопасности.

Помимо названных были найдены и другие работы в области построения онтологий, связанных с информационной безопасностью [5, 6], однако ни одна из них не связана с организацией данных, представленных в соответствующих стандартах.

На данный момент осуществляется разработка системы моделей, представляющих методологию стандартов информационной безопасности [7–9], поэтому при выбо-

ре метода, языка и инструментального средства поддержки для построения онтологических моделей необходимо основываться на обеспечении возможности их согласования с другими видами моделей (структурными, объектными) – в частности, возможности импорта-экспорта результатов моделирования.

Подходы к построению онтологий можно условно разделить на классический и современный.

Классический подход к построению онтологий

Под классическим подходом понимается построение онтологий в соответствии со стандартом онтологического анализа IDEF5 [10], входящего в известное семейство стандартов, используемых при моделировании бизнес-процессов.

Стандарт IDEF5 подразумевает использование двух языков моделирования - IDEF5 Schematic Language (схематический язык) и IDEF5 Elaboration Language (язык доработок и уточнений). SL в IDEF5 представляет собой наглядный графический язык, специально предназначенным для изложения экспертами в рассматриваемой области системы основных данных в форме онтологической информации. Язык SL используется только н первом этапе моделирования, структурирование информации с использованием этого языка сложно механизировать, предполагается, что схематические диаграммы в данном случае создаются людьми.

Анализ данных и исследование полноты данных, полученных в результате построения онтологической структуры предметной области являются задачей текстового языка EL.

IDEF5 Elaboration Language теоретически похож на язык ограничений OCL (Object Constraint Language), дополняющим язык UML, который, в свою очередь, использовался при построении структурной модели методологии информационной безопасности. И тот, и другой являются формальными текстовыми языками для описания правил: использующихся при построении онтологии или задающих ограничения в UML-моделях.

Хотя стандарт IDEF5 и создавался специально для графического моделирования онтологий, однако, он имеет очень мало инструментальных средств поддержки и, соответственно, существующих способов взаимодействия с другими методологиями. Для создания моделей предметной области в соответствии со стандартом IDEF5 Александром Мокровым и Александром Хохловым было создано специальное инструментальное средство – OnToIDEF5, однако, его не удалось найти в свободном доступе.

Также разработкой программных средств поддержки моделирования с помощью стандартов семейства IDEF занимается компания Knowledge Based Systems, Inc., однако, предложенное ею решение для IDEF5 – SBONT – пока ещё находится в стадии разработки.

Помимо перечисленных для моделирования можно использовать непрофильные (неспециализированные) средства, такие как MS VISIO, но они не подойдут для сравнения различных моделей методологии информационной безопасности.

Так как некоторые символы языка SL IDEF5 можно представить с помощью графических примитивов UML (см. табл. 1), то моделирование онтологий в соответствии с IDEF5 можно было бы проводить с помощью одного из инструментальных средств, предназначенных для создания UML-моделей. Анализ данных на уровне языка EL в этом случае проводился бы с использованием OCL.

Данный вариант также имеет недостатки, так как не все элементы, использующиеся в SL IDEF5, имеют прямой аналог в UML, при этом некоторые элементы могут иметь несколько аналогов в разных ситуациях (например, состояние на схематике переходов в IDEF5 изображено символом типа (класса), в UML же для описания состояния на диаграмме состояний используется отдельный символ).

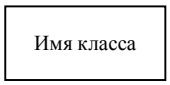
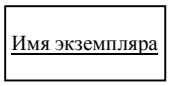
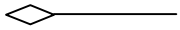
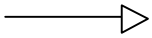
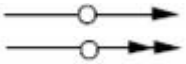
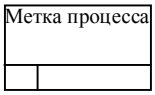
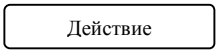
IDEF5		UML	
Название элемента	**Изображение**	**Название элемента**	**Изображение**
Тип (класс)		Класс	
Индивид[1]		Экземпляр	
Двуместные отношения первого порядка, **part-of**		Агрегатная ассоциация	
Двуместные отношения первого порядка, **subkind-of**		Отношение обобщения, **is-a**	
Переход между состояниями		Переход между состояниями	
Процесс		Состояние действия	
Маркер мгновенного перехода		Нетриггерные переходы	

Таблица 1. Соответствие между графическими элементами UML и IDEF5

Современный подход к построению онтологий

Современный подход к онтологическому анализу подразумевает, в основном, построение web-онтологий – онтологий в контексте семантической паутины (web 3.0) и сводится к разработкам консорциума W3C (The World Wide Web Consortium) – поставщика web-стандартов.

Одной из таких разработок является Web Ontology Language (OWL) [11] – язык для представления онтологий и связанной информации в виде семантической сети. OWL использует язык разметки Resource Description Framework (RDF) на основе XML и, соответственно, имеет точки соприкосновения с другими web-ориентированными языками, а также возможность импорта-экспорта моделей между приложениями, работающими с UML и OWL.

Элементами онтологий OWL являются классы, их представители (индивиды), свойства и отношения между классами и/или их представителями.

RDF Schema (RDFS) – семантическое расширение RDF, язык описания словарей RDF-терминов. RDFS позволяет определить уникальные классы ресурсов, представляющие модель предметной области, включая их атрибуты и отношения между классами. Кроме того, RDF Schema включает возможность определения подклассов, а также представляет некоторое количество базовых классов и возможность определения некоторого количества ограничений. Таким образом, RDFS аналогична диаграмме классов в

[1] Может быть как отдельным индивидом, так и экземпляром класса

UML (для описания диаграмм RDFS используется направленный граф ресурсов (Direct Labeled Graph, DLG), в виде которого также могут просматриваться диаграммы классов UML).

OWL-тэг	Название элемента в UML
<owl:Class rdf:ID="…">	Класс
<owl:Thing rdf:ID="…">	Экземпляр
<owl:ObjectProperty rdf:ID="…">	Отношение
<owl:DatatypeProperty rdf:ID="…">	Атрибут

Таблица 2. Соответствие между OWL-тэгами и конструкциями UML

Для построения современных онтологий на базе OWL существует множество средств моделирования, таких как: Protégé, OntoEdit, OilEd, WebOnto и др, среди которых можно выделить Protégé, упоминания о котором встречаются наиболее часто и для которого разработано достаточно большое количество плагинов. Важным преимуществом этой программы, влияющим на возможность согласования онтологической и структурной моделей, также является то, что для неё существует плагин «UML backend», с помощью которого можно осуществлять импорт-экспорт моделей, созданных в Protégé и диаграмм, созданных на основе UML 1.4. Позволяет осуществлять экспорт проекта в виде .xmi-файла, а также импорт .xml-файлов (импорт .xmi не обнаружен).

Пример экспорта онтологии, созданной в Protégé в программу, предназначенную для создания и редактирования UML-моделей представлен на рисунке ниже.

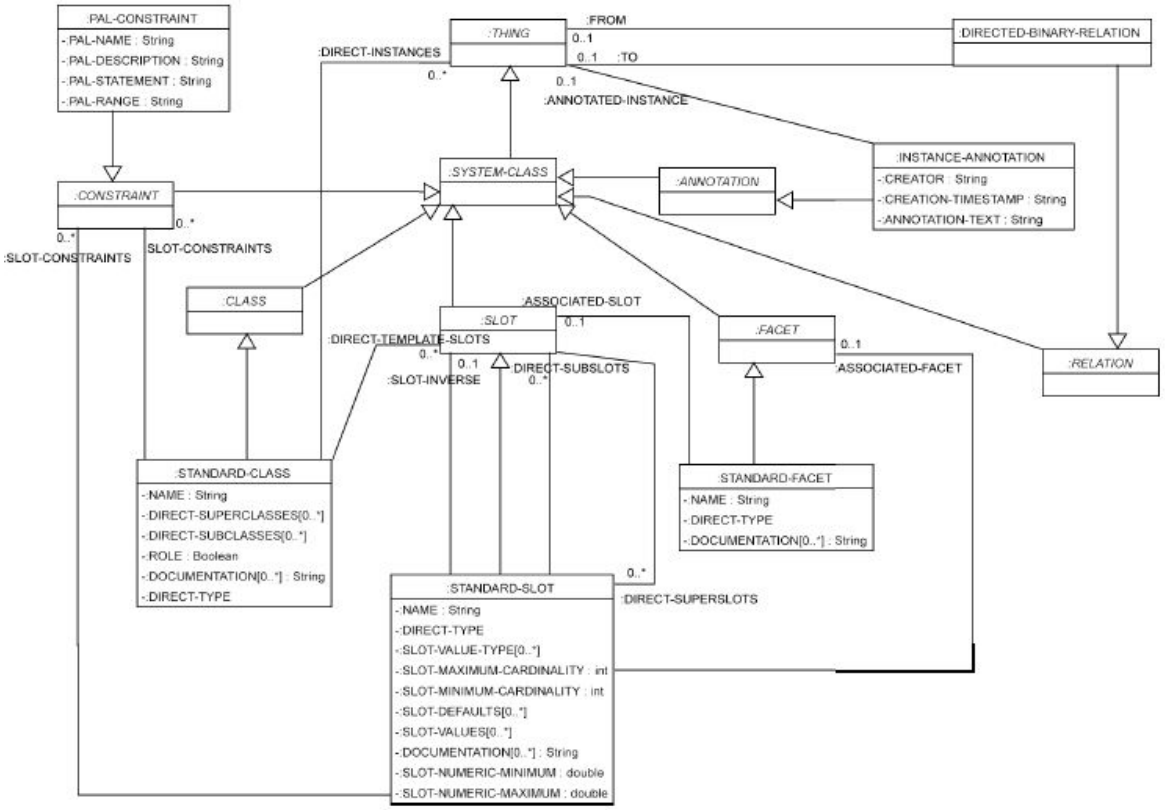


Рисунок. Результат экспорта онтологии из Protégé в Poseidon UML

Заключение

Онтологический анализ стандартов информационной безопасности, являясь одним из уровней интегрального инжиниринга данной предметной области, предназначается для стандартизации терминологии различных документов в области информаци-

онной безопасности, а также согласования и возможной модификации других моделей. В представленной работе был описан выбор методов и средств онтологического анализа стандартов информационной безопасности на основе рассмотрения классического и современного подходов к построению онтологий.

Учитывая большой выбор и гибкость инструментальных средств поддержки моделирования онтологий в контексте семантической паутины на фоне практического осутствия таковых для разработки онтологий по стандарту IDEF5, предполагается использование современного подхода к построению онтологических моделей информационной безопасности. Преимуществом данного подхода также является распространённость онтологий на основе OWL и возможность применения их совместно с большим количеством других технологий, благодаря использованию XML. Однако, при этом возможны заимствования из классического онтологического анализа, если они окажутся полезны и применимы.

Литература

1. Любимов А.В. Инжиниринг стандартов информационной безопасности // Региональная информатика-2008 (РИ-2008). XI Санкт-Петербургская международная конференция. Санкт-Петербург, 22–24 октября 2008 г.: Материалы конференции \ СПОИСУ. – СПб, 2008. – С. 103–104.
2. Андреева Н.В., Любимов А.В. Онтологический анализ стандартов информационной безопасности // Региональная информатика-2008 (РИ-2008). XI Санкт-Петербургская международная конференция. Санкт-Петербург, 22-24 октября 2008 г.: Материалы конференции \ СПОИСУ. – СПб, 2008. – С. 91–92.
3. Security Ontology [http://securityontology.securityresearch.at/]
4. Fenz S., Goluch, G. Ekelhart, A. Riedl, B. and Weippl, E. Information Security Fortification by Ontological Mapping of the ISO/IEC 27001 Standard. Proceedings of the 13th Pacific Rim International Symposium on Dependable Computing, PRDC2007', IEEE Computer Society, Los Alamitos, CA, USA, 0-7695-3054-0, 2007. – PP. 381–388.
5. Raskin V., Hempelmann, C.F., Triezenberg, K.E., Nirenburg, S. Ontology in information security: A useful theoretical foundation and methodology tool //New Security Paradigms Workshop. – 2001. – С. 53–59.
6. Vladimir Jotsov. Dynamic ontologies in information security systems //International Journal «Information Theories & Applications». – 2008. – Vol.15. – С. 319–329.
7. Любимов А.В. Структурное моделирование стандартов информационной безопасности // V Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23–25 октября 2007г. – Труды конференции – Санкт-Петербург, 2008. – С. 123 – 127.
8. Любимов А.В., Черемушкин Д.В. Объектное моделирование как средство описания системы управления информационной безопасностью // Труды 12-й международной конференции «Теория и технология программирования и защиты информации». Санкт-Петербург, 15–16 мая 2008г. – С. 85–89.
9. Любимов А.В., Суханов А.В. Полуформальные модели стандартов информационной безопасности // Вопросы защиты информации. – 2008. – №2 (81) – С. 52–57.
10. [IDEF5, 1994] Information Integration for Concurrent Engineering (IICE). IDEF5 Method Report. – Knowledge Based Systems, Inc., 1408 University Drive East College Station, Texas, USA. – September 21. – 1994.
11. [OWL, 2004] OWL Web Ontology Language. Overview. – W3C Recommendation. – February 10. – 2004. – http://www.w3.org/TR/owl-features/

УДК 004.056.4

МЕТОД ОБНАРУЖЕНИЯ «МЁРТВОГО КОДА» В ПРОДУКТАХ ТЕХНОЛОГИИ ПРОМЫШЛЕННОГО ПРОЕКТИРОВАНИЯ

Ю.А. Торшенко

В статье предложен метод обнаружения предпосылок к возникновению «мертвого кода» на стадиях проектирования, предшествующих формированию программного кода.

Ключевые слова: «мертвый код», быстрая разработка приложений

Метод обнаружения предпосылок к возникновению «мертвого кода» на стадиях проектирования, предшествующих формированию программного кода основывается на детальном анализе UML-диаграмм действий бизнес-процессов организации-заказчика программного продукта (как поставщика основных функциональных требований) и бизнес-логики артефакта RUP посредством построения комплексных кубических покрытий. Суть метода заключается в последовательном выполнение нескольких аналитических задач:

- выделения логической структуры артефакта RUP;
- исследования его логических связей;
- преобразования артефакта в графо-аналитическую модель;
- формирования комплексного кубического покрытия;
- выявления основных показателей наличия «мертвого кода».

В качестве основного объекта для дальнейшего анализа из общей UML-модели бизнес-процесса или бизнес-логики приложения (в зависимости от этапа разработки) выделяется диаграмма деятельности (Activity diagram), как основной инструмент преобразования информационных потоков.

Для общего анализа проводится дальнейшие исследование диаграммы деятельности, а для более детального – подробно изучается каждая линейная задача на диаграмме, так как она может содержать в себе вложенные структурные элементы.

Изучение структурных элементов производится до момента определения наибольшей глубины вложенных задач.

При необходимости для каждой из задач строится собственная логическая структура, состоящая из набора элементарных действий и условий.

Затем для небольших моделей строится общая структура бизнес-процесса. Сложные модели остаются разбитыми на элементы, которые объединяются уже на этапе анализа комплексного кубического покрытия.

Преобразование логической структуры артефакта RUP в ГАМ

Теоретико-графовый подход используется… в быстроразвивающихся разделах линейного программирования и исследования операций при изучении потоков в сетях [1].

В графосимволическом языке операции представляются вершинами некоторого графа. Отношение управления задается в виде дуг этого графа. Отношение информационной зависимости задается путем перечисления имен переменных, являющихся входными и выходными для данной операции [2].

Элементы диаграммы деятельности представляются в форме графо-аналитической модели: задачи (task) преобразуются в линейные вершины, точки принятия решений (decision) – в условные, а переходы между ними и точки слияния (merge) обозначаются дугами (рис. 1).

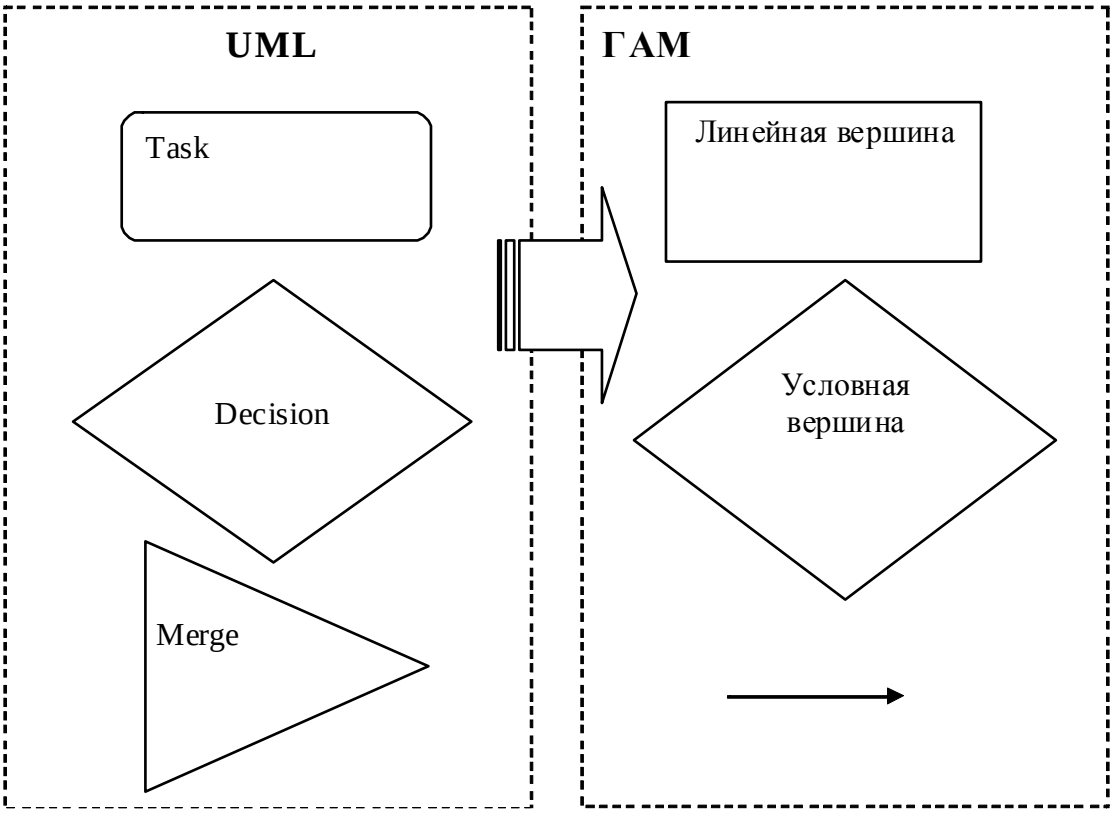


Рис. 1. Преобразование UML диаграммы действий в ГАМ

Соответствие структурных элементов диаграммы деятельности элементам графо-аналитической модели показаны в табл. 1.

Диаграмма деятельности UML			**Графо-аналитическая модель**	
Элемент	**Описание**	**Обозначение**	**Элемент**	**Обозначение**
Start node	Начало программы или процесса		Начало	
Task	Отдельная задача		Линейная вершина	
Decision	Ветвление		Условна вершина	
Fork	Разделение информационных потоков		Виртуальная вершина	•
Merge	Объединение		Виртуальная вершина	•

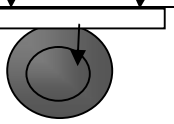
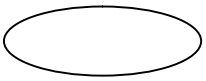
Join	Слияние информационных потоков		Виртуальная вершина	•
Stop node	Завершение программы или процесса		Конец	
Line	Переход от одного элемента к другому		Дуга	

Таблица 1. Преобразование из UML в ГАМ

Для упрощения общей графо-аналитической модели несколько последовательных простых задач обозначим за одну линейную вершину.

После формирования графо-аналитической модели на ее основе строится упрощенное комплексное кубическое покрытие (без учета функций передачи управления) с построением кубов для всех вариантов прохождения условных вершин.

Выявление основных показателей наличия «мертвого кода» в проектируемом программном продукте

Наличие предпосылок к дальнейшему формированию «мертвого кода» определяется по значениям выходных переменных: если все булевы переменные на выходе дают значение false, то в логической структуре исследуемого артефакта присутствуют несогласованные условия, а значит и возникают неисполняемые пути.

Заключение

Применение данного метода возможно для улучшения качества программного обеспечения, разрабатываемого промышленным способом: повышения таких качеств, как надежность и безопасность, а также уменьшения объем кода, что, в свою очередь, поможет ускорить работу программы и снизить риск возникновения уязвимостей.

Литература

1. Харари Ф. Теория графов М.: Мир. – 1973. – 300 с.
2. Игнатьев М.Б., Фильчаков В.В., Осовецкий Л.Г. Активные методы обеспечения надежности алгоритмов и программ – СПб: Политехника. – 1992. – 288 с.

УДК 004

ВЫЯВЛЕНИЕ И УСТРАНЕНИЕ «МЕРТВОГО КОДА» С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ПРОГРАММИРОВАНИЯ IBM RATIONAL APPLICATION DEVELOPER

М.С. Сакулина
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В статье поднимается вопрос о повышении уязвимости компьютерных систем за счет разработки приложений с использованием технологии программирования. Ее использование приводит к появлению большого количества участков «мертвого кода», в котором могут располагаться вредоносные программы. Рассмотрен один из путей устранения данного недостатка.
Ключевые слова: информационная безопасность, технология программирования, программный продукт, «мертвый код», вредоносный, избыточный код, надежность

Введение

Идея о том, что информация является основным ресурсом предприятия, зачастую превосходящим по стоимости финансовые ресурсы, давно не вызывает удивления и споров. Скорее страсти разгораются вокруг вопросов ее сохранения и преумножения. Актуальность этой темы исчезнет не скоро. Поэтому необходимо уделять особое внимание вопросам защиты информации.

В данный момент есть два основных источника угроз: внешний и внутренний. Доступ к данным можно получить либо извне (по сети), либо изнутри, т.е. через непосредственный контакт с носителем (воровство, «инсайдеры» и т.п.).

Данная работа направлена на предотвращение внешних угроз и снижение внутренних. Дело в том, что для проникновения в систему снаружи злоумышленнику (опасной программе) нужна лазейка, открытая изнутри. Поэтому нужно особое внимание обращать на создание и хранение информации (в нашем случае программных продуктов). Халатное отношение в процессе производства может привести к плачевным последствиям. Контроль каждого этапа разработки, анализ продукта в целом и применение современных, отвечающих всем требованиям безопасности средств – вот решение проблемы.

Постановка задачи

Необходимо определить следующие аспекты:

- что является основной угрозой;
- что служит посредником возможных рисков;
- как с этим бороться.

Основная угроза – это не один конкретный фактор, а совокупность многих условий. Как, например, можно отделить угрозу вирусной атаки от вопросов системного администрирования? Поэтому направление данного исследования нужно рассматривать поэтапно, детально разбирая каждую составляющую. Начнем с привычного и наиболее распространенного источника рисков.

Вирусы и вредоносные программы

Как упоминалось раньше, есть два основных источника возможных ущербов: внешний и внутренний. Логично будет начать с менее контролируемого вида угроз для защитника информации, а затем уже перейти к тем факторам, на которые можно влиять напрямую. Поэтому рассмотрим опасные программные модули и их классификацию.

Вредоносные программы отличаются условиями существования, применяемыми технологиями на различных этапах жизненного цикла, собственно вредоносным воздействием - все это и является основой для классификации. В результате по основному (с исторической точки зрения) признаку - размножению, вредоносные программы делятся на три типа: вирусы, черви и Трояны. Они различаются жизненным циклом, а обобщенная схема представлена в таблице.

	Вирусы	Черви	Трояны
Способ проникновения	Вместе с зараженными файлами или другими объектами	Сетевые черви; почтовые черви; IRC черви; P2P черви; IM черви	Маскировка; Вместе с вирусами или червями
Активация	Загрузочные вирусы; Файловые вирусы;	Активное участие пользователя; пассивное участие пользователя	Активное участие пользователя; пассивное участие пользователя
Выполняемые действия	Поиск жертв; Подготовка вирусных копий; Внедрение.	Поиск жертв; Подготовка вирусных копий; внедрение.	Выполнение заложенных функций

Таблица. Общая схема различий жизненных циклов вредоносных программ

Наиболее распространенной на сегодняшний день проблемой являются два первых. Такие программы внедряются в компьютерную систему и копируют себя, распространяясь дальше. Действие они производят различное: «забивают» канал, тем самым, закрывая доступ к сети, изменяют стандартные функции приложений, удаляют или изменяют данные. Борьба с ними ведется постоянно, существует множество антивирусных программ, которые выявляют зараженный объект по сигнатуре вируса, затем лечат либо удаляют его. База сигнатур обновляется постоянно, так что на этом фланге удается держать равновесие.

Троян, пожалуй, является самой опасной вредоносной программой, т.к. может иметь любой вид и вызывать неожиданные последствия. Из-за этого крайне сложно выявить его. К счастью, в наши планы не входит разработка новой антивирусной программы, по крайней мере, сейчас. Проект направлен на то, чтобы обезопасить себя с другой стороны. А именно – не дать возможности подобным программам обосноваться в ОС, т.е. максимально сократить места, в которые они могли бы быть записаны. Нам известно, что зачастую Трояны сохраняются в участках, так называемого, «мертвого кода. Чтобы понять как бороться с этим, нужно знать откуда же появляются такие куски программы. И тут мы переходим ко второму аспекту: посреднику возможных рисков, т.е. от активных опасностей переходим к пассивным. Вместе с этим получаем возможность менять ситуацию в свою пользу и повышать надежность программных продуктов.

Технология программирования и «мертвый код»

В соответствии с обычным значением слова "технология" под технологией программирования будем понимать совокупность производственных процессов, приводящую к созданию требуемого программного средства (ПС), а также описание этой совокупности процессов[1]. Другими словами, технологию программирования мы будем

понимать здесь в широком смысле как технологию разработки программных средств, включая в нее все процессы, начиная с момента зарождения идеи этого средства, и, в частности, связанные с созданием необходимой программной документации[1]. Каждый процесс этой совокупности базируется на использовании каких-либо методов и средств[1].

Естественно, что фирмы, выпускающие различные среды разработки приложений учитывают это и стараются максимально упростить процесс создания и компоновки программного продукта. Проще говоря, появляется определенный порядок действий и набор средств, которые позволяют создавать полноценные коммерческие программы. Современные средства разработки предоставляют возможность создавать программы и приложения «по шаблону». Схематически процесс создания приложения представлен на рисунке.

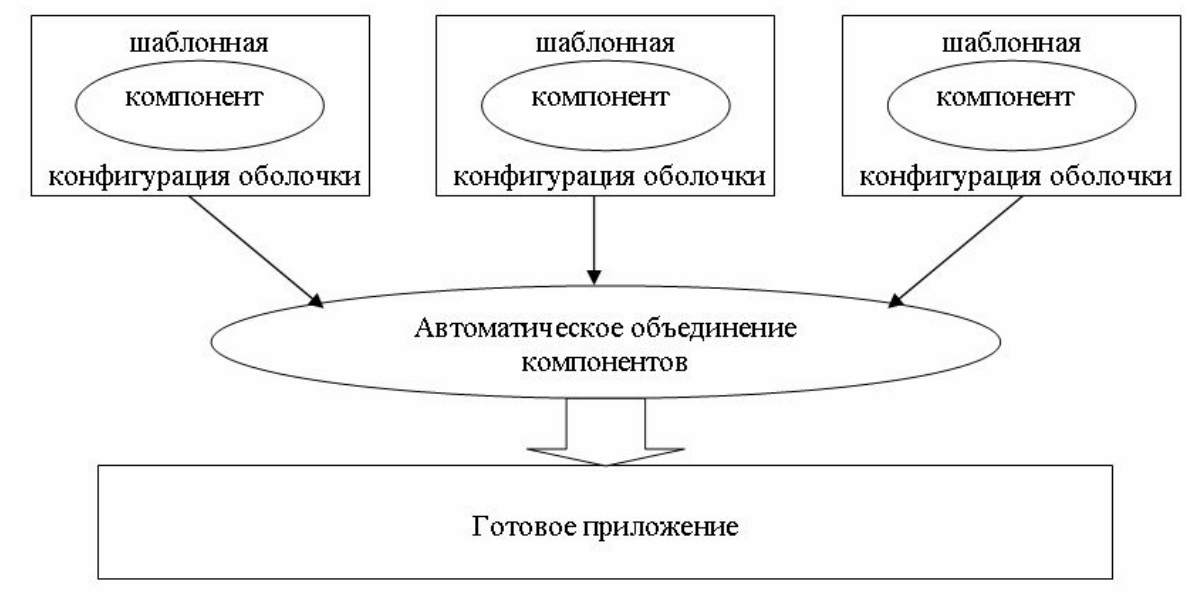


Рисунок. Схема создания приложения с помощью технологии программирования

Основная часть кода генерируется самой средой, программисту остается лишь добавить пару строк для придания проекту индивидуальности. Объединение компонент также упрощено. Даже если все части были созданы разными людьми, соединить их в единый продукт не так сложно, т.к. все создавалось по одной схеме и «оболочка» каждого сегмента практически идентична и предусматривает множество способов объединения. Все это позволяет создавать качественные коммерческие приложения, а подготовка сотрудников не требует высоких затрат. При всех явных плюсах такого подхода существуют и минусы, такие как избыточный и «мертвый код», получаемые при автоматической конфигурации компонентов.

Дать определение таким участкам программы нелегко. Поэтому просто приведем описание свойств «мертвого кода» - это такая часть программы, которая выполняется, но ее выполнение никак не влияет на результат работы. Это практически значит, что «мёртвый код» не может иметь побочного эффекта, даже в виде модификации глобальных переменных, не может изменять окружение работающей программы, не может выполнять никаких операций, которые могут вызвать исключение в работе программы. Мертвый код может занимать до 30% программы, особенно его много получается при развитии приложений, ведь в них вносятся все новые и новые куски.

В теории компиляторов удалением мертвого кода называется оптимизация, удаляющая бесполезные операции, то есть операции, результат которых нигде не используется, и операции, которые в силу различных условий никогда не будут выполнены. Дело в

том, что любой компилятор производит анализ входного кода и синтез нового, понятного машине текста. В ходе этих действий происходит постоянная проверка ошибок, т.к. входные данные зачастую бывают некорректны.

Для работы над проблемами «мертвого кода», размещения вредоносных программ и безопасности информации нужна среда разработки, которая удовлетворяла бы всем описанным выше требованиям. Она должна представлять собой полноценную систему создания приложений, которая воплощала бы в жизнь технологию программирования. Поэтому была выбрана IBM Rational Application Developer.

Методы исследований

IBM Rational Application Developer – это такая среда разработки, которая повышает производительность труда, сводит к минимуму длительность кривой обучения и сокращает время на разработку и тестирование. Application Developer включает в себя интегрированные средства разработки порталов, визуального редактирования UML, анализа кода, автоматизированного тестирования и развертывания - все, что необходимо разработчикам для производительной работы и для того, чтобы полученный код был хорошо спроектирован, масштабируем и готов к работе в производственной среде. Встроенные инструменты контроля версий и поддержки групповой работы позволяют разработчикам сложных проектов и большим командам координировать контроль версий и обеспечить защиту ресурсов группы. Помогает разработчикам, использующим язык Java, быстро проектировать, разрабатывать, собирать, тестировать, настраивать и внедрять качественные портальные приложения, Web-приложения, Web-службы, а также приложения Java/J2EE и SOA[2].

Опции и возможности данного продукта максимально отвечают требованиям современной технологии программирования, а значит позволяют изучить всевозможные пути внедрения инородной программы (вирус, Троян). Требования информационной безопасности при разработке программных средств должны обеспечиваться на следующих этапах их проектирования:

- разработка структуры программного средства, внутренних информационных потоков и протоколов взаимодействия;
- разработка алгоритмического обеспечения программного средства (алгоритмов автономных модулей);
- программная реализация опытного образца;
- комплексные испытания.[3]

Эти исследования - основа для борьбы с мертвым и избыточным кодом. Следовательно, и с распространением вирусов и Троянов, что в значительной степени повышает безопасность компьютерных систем.

Результаты и их обсуждение

Итак, определив угрозы и их источники, самое время приступить к описанию методов борьбы с ними. Принцип работы такой же, как и у компилятора: анализ и синтез. Сначала нужно определить где и как в конкретных условиях появляется «мертвый код» и на сколько он опасен. Затем создать оптимизатор, который будет удалять избыточные куски и повышать безопасность.

Подробное описание проекта начнем с раздела анализа: в работе необходимо сымитировать создание стандартного программного продукта, состоящего из нескольких компонентов.

Можно выделить следующие этапы:

1. Постановка задачи, т.е. описание будущего продукта (предположительно, обучающая программа для студентов).
2. Непосредственно его создание, т.е. написание отдельных компонентов дальнейшее их объединение. Имитация создания продукта несколькими программистами, как обычно и происходит.
3. Контроль безопасности на каждом этапе разработки приложения.
4. Анализ созданного программного продукта и выявление участков мертвого и избыточного кода. Сравнение ручного и программного объединения компонентов.
5. Анализ трансляции кода и работа с компилятором. Пошагово рассмотреть работу приложения, чтобы знать на каком этапе вырабатывается основная часть избыточного кода.
6. Внедрение в продукт (а точнее в обе его версии: созданную вручную и программно) вредоносного кода.
7. Анализ результатов.

По итогам данного исследования начинается создание оптимизатора кода. Под оптимизацией понимают последовательность эквивалентных преобразований исходной программы, уменьшающих ее стоимость. Как набор, так и порядок выполнения этих преобразований зависят от того, что считается стоимостью программы. В нашем случае основной критерий – это качество и безопасность кода. Существует множество способов и методов оптимизирующих преобразований. Наиболее интересны те, которые направлены на устранение избыточных кусков кода. Они основаны на том, что у любого оператора программы есть входные и выходные данные. Преобразование заключается в удалении такого оператора, у которого не используются его выходы. Оно повторно по отношению к самому себе, поскольку удаление одного оператора приводит к тому, что операторы, вырабатывающие для него данные, также могут оказаться неиспользуемыми. На основании этого принципа и данных, полученных при анализе программы и будет строиться оптимизатор.

Заключение

Были рассмотрены основные моменты, влияющие на данную проблему безопасности. Технология программирования – перспективная область развития современных информационных технологий. Из нее в свою очередь вытекает проблема мертвого кода, который возникает при модификации и объединении компонентов. В пресловутые участки загадочного неисполнимого кода становится возможным помещать Трояны и другие вредоносные программы. Изучение среды IBM Rational Application Developer, выявление недостатков и источников мертвого кода, а также их устранение автоматически повысит антивирусную защиту, т.к. объем пространства для размещения вирусов значительно сокращается. Соответственно, первостепенной задачей ученых, занимающихся безопасностью информационных технологий, становится устранение «мертвого кода», оптимизация приложений. Технология программирования также должна тянуться в сторону более тонкой организации. Необходимо решать проблему в ее корне.

Безопасность данных – залог успеха для многих областей деятельности. Создание коммерческих приложений, не требующее высоких затрат также повышает ликвидность предприятия. Ну, а объединение первого и второго – является целью данной работы.

Литература

1. 42 Lessons about Software engineering», taken from IIT Kharagpur's Course Materials, July 29. – 2008.
2. www.ibm.com
3. Алексеев В.М. Обеспечение информационной безопасности при разработке программных средств. Учебное пособие. – Москва. – 1999.
4. Соловьев В.П. Методы предотвращения и обнаружения вторжений. Учебное пособие для студентов. – Москва. – 2007.
5. Касьянов В.Н. Оптимизирующие преобразования программ. – М.: Наука. – 1988. – 336 с.

УДК 004.056(083.74)

КОРРЕКТИРОВКА СТАНДАРТОВ СЕМЕЙСТВА ISO/IEC 27000 НА ОСНОВЕ ОБЪЕКТНОЙ МОДЕЛИ СЛОВАРЯ

Д.В. Черемушкин
Научный руководитель – к.т.н., доцент А.В. Любимов

В работе демонстрируется эффективность методов интегрального инжиниринга на примере использования объектной модели словаря методологии семейства стандартов ISO/IEC 27000 для коррекции стандартов этого семейства. Статья описывает базовые свойства объектной модели словаря, основные этапы ее разработки, иллюстрирует контекстную диаграмму, отражающую текущее состояние понятийного аппарата принятых стандартов. На основе анализа полученной модели выявлено несколько недочетов в описании и использовании ключевых концептов методологии стандартов, сформулированы конкретные рекомендации по их устранению. Одна из рекомендаций описана подробно и пояснена при помощи диаграмм классов.

Ключевые слова: корректировка стандартов, интегральный инжиниринг, объектное моделирование, словарь семейства стандартов, СУИБ, ISO/IEC 27000, UML

Введение

В работах [1, 2] была представлена методика инжиниринга стандартов информационной безопасности (ИБ) и очерчены методы ее применения для решения широкого спектра практических задач в области защиты информации. Одной из таких задач является анализ и коррекция международных, национальных, отраслевых и ведомственных стандартов ИБ.

Каждый международный стандарт является обобщением разнообразного опыта многих организаций, полученного в разное время, в разных странах и с использованием различных подходов и методов. Несмотря на тщательную подготовку и последующую регулярную ревизию он неизбежно содержит недочеты, выражающиеся, в частности, в неполноте или несогласованности отдельных положений и рекомендаций. Выявление подобных недочетов, выработка рекомендаций по их устранению, подготовка новых редакций стандарта является основной работой многочисленных подкомитетов ISO. Использование для этих целей различных полуформальных моделей, получаемых в рамках методики инжиниринга стандартов ИБ, позволяет подвести под эту работу надежную методологическую базу, систематизировать ее и существенно повысить ее эффективность.

В настоящей работе демонстрируется эффективность методов интегрального инжиниринга на примере использования объектной модели словаря методологии семейства стандартов ISO/IEC 27000 (СУИБ) для анализа и коррекции корневых стандартов семейства.

Объектная модель словаря семейства стандартов ISO/IEC 27000

В рамках методики интегрального инжиниринга семейства стандартов ISO/IEC 27000, параллельно с построением полной интегральной модели семейства [3, 4], была разработана частичная модель стандартов, а именно – объектная модель словаря методологии со следующими базовыми свойствами:

- Назначение: полуформальное описание концептов методологии семейства стандартов, выявление и корректировка недочетов в их описании и употреблении.
- Точка зрения: системный аналитик.
- Границы моделирования: концепты, входящие в словари официально принятых (на момент разработки модели) англоязычных стандартах семейства:

ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005:2008, ISO/IEC 27006:2007.

- Глубина моделирования: контекстная модель, отражающая содержание и связь основных понятий методологии семейства.

Объектная модель словаря является ключевой частью модели общего контекста безопасности организации и содержит 39 классов и 63 отношений между ними, представленных на 10 диаграммах. С учетом цели исследования – анализа и коррекции стандартов – в модели представлены объекты двух типов. Во-первых, это описание терминов, определений и их связей, которые присутствуют в опубликованных стандартах линейки на момент анализа. Они представляются классами, не содержащими в именах дополнительного классификатора, и диаграммами, содержащими в названии классификатор "[as-is]". Во-вторых, это дополнительные элементы, рекомендуемые для включения в понятийный аппарат стандартов с целью его улучшения. Диаграммы, представляющие улучшения, в названии содержат классификатор "[to-be]", а соответствующие классы – классификатор "[add]" (если класс описывает новый термин), классификатор "[mod]" (если класс описывает изменения содержания существующего термина) или классификатор "[del]" (если класс описывает термин для исключения). Для наглядности классы и отношения, выражающие модификации разного характера, выделены разным цветом. Для иллюстрации объема и связности модели ее общий вид (полная диаграмма as-is) приведен на рис. 1.

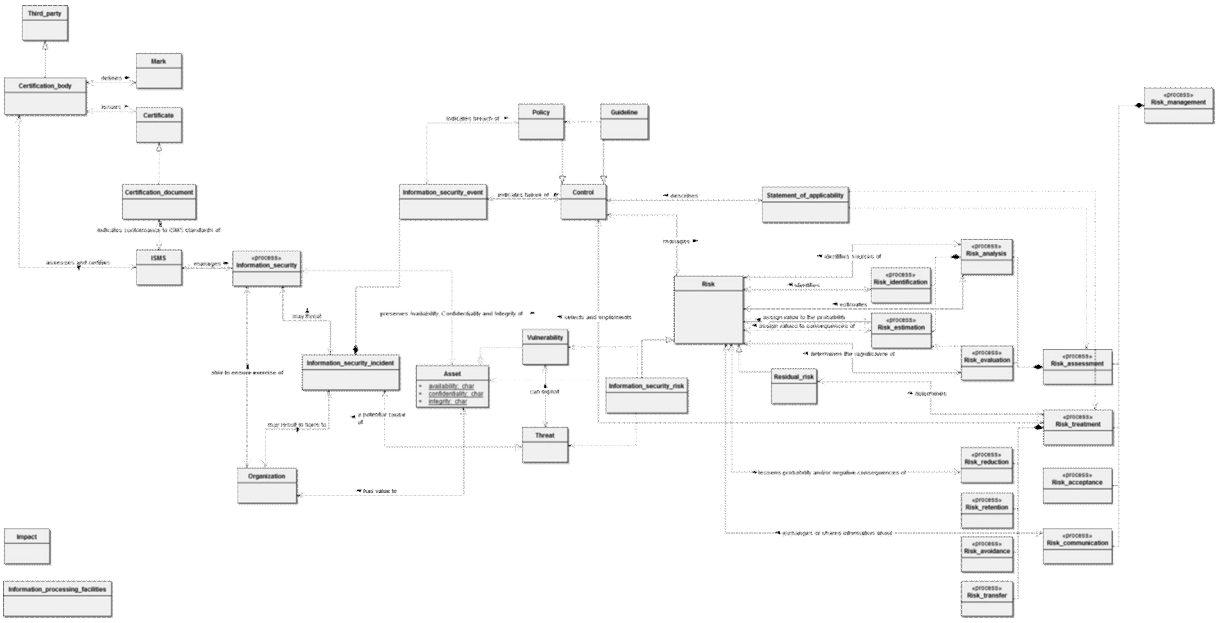


Рис. 1. Контекстная диаграмма as-is

При анализе текста стандартов и представлении результатов в виде объектной модели использовалась следующая последовательность действий:

(1) Создание классов, имена которых соответствуют терминам стандарта, а примечания содержат соответствующие определения.

(2) Анализ определений на предмет наличия в них отношений между терминами стандарта, представление результатов на диаграмме в виде связей.

(3) Детальная проверка классов и связей. Выявление неявных связей между терминами, согласование терминов рассматриваемого в данный момент стандарта с уже описанными на диаграмме, контроль наличия определений и обоснований для всех заведенных классов и связей.

(4) Осуществление перечисленных этапов для следующего рассматриваемого стандарта.

Анализ объектной модели и его результаты

Проведенный объектный анализ выявил недостаточную проработанность понятийного аппарата исследуемого семейства стандартов, проявляющуюся в:

(а) неполноте словаря;
(б) некорректности некоторых определений;
(в) противоречиях между определениями терминов и другими положениями стандартов.

В частности, на неполноту словаря указывает отсутствие определений ряда ключевых понятий, необходимых для представления методологии семейства, таких как "Audit", "Control objective", "Document", "Information asset", "Interested party", "ISMS policy", "ISMS objectives", "Information security policy", "Information security objectives", "Management system", "Record", "Objective", "Procedure" и др. Кроме того, отмечены некорректности с определениями понятий "Certificate" и "Certification body", несоответствие между определением процесса "Risk management" в стандарте ISO/IEC 27002 и его более расширенным описанием в стандарте ISO/IEC 27005 и так далее.

Для устранения этих и им подобных недостатков понятийного аппарата семейства, выявленных в процессе построения и анализа моделей, были выработаны конкретные рекомендации по улучшению стандартов. Некоторые примеры таких рекомендаций приведены ниже. Курсивом в тексте выделены изменения и дополнения положений стандартов.

Рекомендации, направленные на корректировку концепта «Asset» и его контекста

По существующему в семействе определению понятие "Asset" ("Актив") – это "Business asset" ("Бизнес-актив"), синоним – "Organization's asset" ("Актив организации"). В то время как почти везде в стандарте термин "Asset" в чистом виде (т.е. без указаний "business", "organization's" и т. д.) употребляется в смысле "Information asset" ("Информационный актив"), т. е. как частный случай "Asset".

Кроме того, несоответствия возникают и со свойствами (в модели – атрибутами) концепта "Asset". В частности, понятие "Integrity" ("Целостность") в стандарте однозначно трактуется как свойство "Asset". Понятие Confidentiality (Конфиденциальность) трактуется как свойство концепта "Information" ("Информация"), описание и представление которого в принятой парадигме отсутствует. Для понятия "Availability" ("Доступность") вообще не указано, свойством чего она является с точки зрения разработчиков семейства.

Для устранения указанных несоответствий предлагается:

(1) Строго разделить в методологии концепт "Asset" (как актив организации в общем смысле) и концепт "Information asset" (информационный актив организации) как его частный случай.
(2) Дать в словаре стандарта следующее определение новому концепту "Information asset":
Information asset – information and assets associated with information processing facilities [ISO/IEC 27001:2005, A.7.1.2; ISO/IEC 27001:2005, A.7.1.3; ISO/IEC 27002:2005, 7.1.2; ISO/IEC 27002:2005, 7.1.3],
сопроводив его ссылкой на фрагмент стандарта, раскрывающий содержание концепта:
There are many types of *information* assets, including:

a) information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;
b) software assets: application software, system software, development tools, and utilities;
c) physical assets: computer equipment, communications equipment, removable media, and other equipment;
d) services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;
e) people, and their qualifications, skills, and experience;
f) intangibles, such as reputation and image of the organization [ISO/IEC 27002:2005, 7.1.1].

(3) Переформулировать определения понятий "Availability", "Confidentiality", "Integrity", как свойств концепта "Information asset":
Availability – the property *of information asset* being accessible and usable upon demand by an authorized entity [ISO/IEC 27001:2005, 3.2];
Confidentiality – the property that information *asset* is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 27001:2005, 3.3];
Integrity – the property of safeguarding the accuracy and completeness of *information* assets [ISO/IEC 27001:2005, 3.8].

(4) Включить в раздел "Introduction" ("Введение"), "Scope" ("Область действия") стандарта ISO/IEC 27001:2005 или в примечание к определению понятия "Asset" фразу с явным указанием на то, что везде в тексте под "Asset" подразумевается "Information asset", если явно не оговорено другое (например, "Business asset" или "Organization's asset").

Фрагмент объектной модели, из которого вытекают вышеприведенные рекомендации, представлен на рис. 2 (диаграмма as-is).

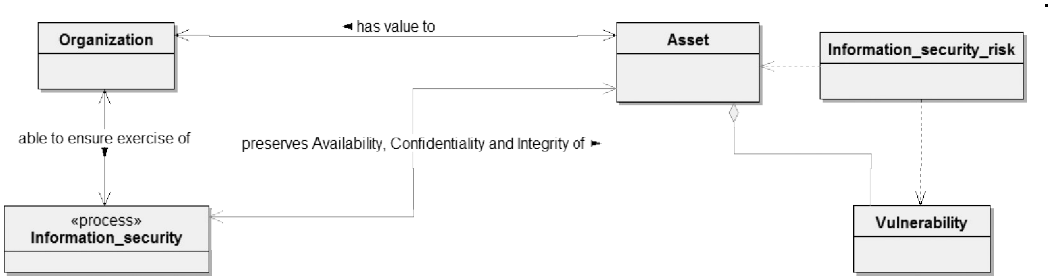


Рис. 2. Диаграмма as-is, описывающая текущий контекст концепта "Asset"

Фрагмент объектной модели, на котором указанные недостатки устранены, представлен на рис. 3 (диаграмма to-be).

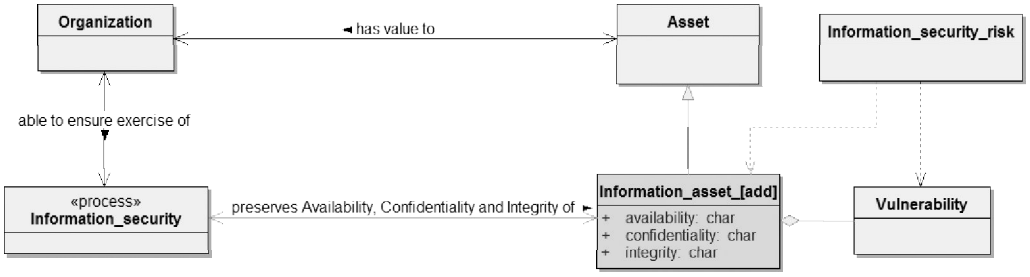


Рис. 3. Диаграмма to-be, отражающая корректировки контекста концепта "Asset"

Рекомендации, описывающие корректировку других концептов

Аналогично тому, как это делалось для группы концептов, связанных с "Asset", при построении и анализе объектной модели словаря были выявлены недочеты в описании и использовании других базовых концептов методологии семейства, в частности – связанных с концептами "Risk management", "Information security event", "Certification body". Формат статьи не позволяет рассмотреть эти недочеты подробно. Поэтому ниже приводятся лишь рекомендации с краткими обоснованиями.

В семействе имеет место следующее противоречие между определением процесса "Risk management" в одном стандарте и его описанием в другом: Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication [ISO/IEC 27002:2005, 2.13]; The information security risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication, and risk monitoring and review [ISO/IEC 27005:2008, 6]. Указанный недостаток предлагается устранить за счет включения в состав процесса "Risk management" концептов "Risk management context establishment" и "Risk monitoring and review" и дать им следующие определения в словаре: Risk management context establishment – *process that* involves setting the basic criteria necessary for information security risk management, defining the scope and boundaries, and establishing an appropriate organization operating the information security risk management [ISO/IEC 27005:2008, 7.1]; Risk monitoring and review – *process* to identify any changes in the context of the organization at an early stage, and to maintain an overview of the complete risk picture [ISO/IEC 27005:2008, 12.1].

В определении "Information security event" присутствует связь с "Information security policy": Information security event – an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [ISO/IEC 27001:2005, 3.5; ISO/IEC 27002:2005, 2.6]. Однако в принятых стандартах понятию "Information security policy" не дано определение (определен лишь термин "Policy"). В связи с чем предлагается ввести это понятие в словарь. Предлагаемое определение: Information security policy – *a policy that provides* management direction and support for information security in accordance with business requirements and relevant laws and regulations. *NOTE:* An information security policy document shall be approved by management, and published and communicated to all employees and relevant external parties [ISO/IEC 27001:2005, A.5.1; ISO/IEC 27002:2005, 5.1]

Термин "Certification body" в семействе стандартов трактуется не как сертифицирующий орган в общем смысле, а как сертифицирующая сторона СУИБ: Certification body – third party that assesses and certifies the ISMS of a client organization with respect to published ISMS standards, and any supplementary documentation required under the system [ISO/IEC 27006:2007, 3.2]. Понятие "Certificate", напротив, имеет широкое значение. Но оно определено с использованием "Certification body", вследствие чего является неверным: Certificate – certificate issued by a certification body in accordance with the conditions of its accreditation and bearing an accreditation symbol or statement [ISO/IEC 27006:2007, 3.1]. Кроме того, определение понятия "Certificate" тавтологично. Устранить эти недостатки предлагается путем исключения из словаря стандартов термина "Certificate", а его определение использовать для модификации определения понятия "Certification document": Certification document – document issued by a certification body *and* indicating that a client organization’s ISMS conforms to specified ISMS standards and any supplementary documentation required under the system [ISO/IEC 27006:2007, 3.1; ISO/IEC 27006:2007, 3.3].

Перечисленные рекомендации после текстологической доработки планируется направить в национальный подкомитет ISO/IEC JTC 1/SC 27 "IT Security techniques", для представления в международный подкомитет от Российской Федерации.

Заключение

На примере объектной модели словаря семейства стандартов ISO/IEC 27000 продемонстрированы преимущества использования методов полуформального моделирования для представления и анализа методологии стандартов ИБ и, что более ценно, эффективного выявления и устранения имеющихся в ней недостатков. При этом важно, что в статье рассмотрено только одно из возможных применений объектных моделей. Более того, в настоящий момент не изучен весь спектр использования подобных моделей и есть основания считать, что он значительно шире круга перечисленных практических задач. Все это указывает на перспективность использования объектных моделей в области информационной безопасности.

Описанное в статье объектное моделирование словаря является частью более содержательной работы по разработке объектной модели общего контекста безопасности, которая была поддержана грантом Правительства Санкт-Петербурга № 3.11/30-04/39 [5].

Литература

1. Любимов А.В. Инжиниринг стандартов информационной безопасности // Региональная информатика-2008 (РИ-2008). XI Санкт-Петербургская международная конференция. Санкт-Петербург, 22–24 октября 2008 г.: Материалы конференции \ СПОИСУ. – СПб, 2008. – С. 103–104.
2. Любимов А.В. Инжиниринг стандартов информационной безопасности: практические аспекты // Региональная информатика-2008 (РИ-2008). XI Санкт-Петербургская международная конференция. Санкт-Петербург, 22–24 октября 2008 г.: Материалы конференции \ СПОИСУ. – СПб, 2008. – С. 104.
3. Черемушкин Д.В. Полуформальное моделирование методологии стандарта ISO/IEC 27001 // Региональная информатика-2008 (РИ-2008). XI Санкт-Петербургская международная конференция. Санкт-Петербург, 22–24 октября 2008 г.: Материалы конференции \ СПОИСУ. – СПб, 2008. – С. 115.
4. Черемушкин Д.В. Задача объектного моделирования системы управления информационной безопасностью // Научно-технический вестник СПбГУ ИТМО. Выпуск 52. Прикладные информационные технологии. / Главный редактор д.т.н., проф. В.О. Никифоров. – СПб: СПбГУ ИТМО, 2008. – С. 237–241.
5. Черемушкин Д.В. Объектная модель общего контекста безопасности организации по семейству стандартов ISO/IEC 2700x // Тринадцатая Санкт-Петербургская ассамблея молодых ученых и специалистов. Аннотации научных работ победителей конкурса грантов Санкт-Петербурга 2008 года для студентов, аспирантов, молодых ученых и молодых кандидатов наук. – СПб: Фонд «ГАУДЕАМУС», 2008. – С. 114.

УДК 004.056(083.74)

ПРИНЦИПЫ ПРОЦЕССНОГО МОДЕЛИРОВАНИЯ СУИБ ПО СТАНДАРТУ ISO/IEC 27001:2005(E)

А.В. Захаров
Научный руководитель – к.т.н., доцент А.В. Любимов

В работе представлены принципы процессного моделирования системы управления информационной безопасностью (СУИБ), обоснован механизм реализации, правила декомпозиции процессов и сборки ресурсов. Приведены практические результаты моделирования на примере нескольких процессов, обосновывается необходимость согласования между процессной и объектной моделями, предлагаются положения по улучшению существующего стандарта.
Ключевые слова: СУИБ, модель, процесс, ресурс

Введение

Система управления информационной безопасностью, регламентируемая серией стандартов ISO/IEC 2700x, основывается на процессном подходе, который определяет действия для проектирования, внедрения, эксплуатации, мониторинга, анализа, поддержки и улучшения информационной безопасности организации.

Спецификой структурного моделирования линейки стандартов ISO/IEC является параллельное создание взаимосвязанных моделей – объектной и процессной. Процессная модель позволяет построить формализованное представление структуры процессов СУИБ. В результате сравнительного анализа существующих в данное время методик была выбрана методика UML, которая поддерживает объектное и процессное моделирование, при формальном следовании методике DFD. Обоснование выбора методики и инструментария приводится в статье автора «Задача процессного моделирования системы управления информационной безопасностью» [3].

Общие принципы построения процессной модели

Согласно стандарту ISO 9000:2005(E) под процессом можно понимать любую деятельность, использующую определенные ресурсы (финансовые, материальные, человеческие, информационные) для преобразования входных элементов в выходные.
Ресурсы, используемые процессами, представляют собой классы объектной модели. Объектная модель рассматривает понятийный аппарат стандарта, выявляя отношения между понятиями и их определениями путем построения модели структурного словаря. Общим принципом построения процессной модели является построение формализованной структуры процессов, связанной с ресурсами-классами, построенных в объектной модели. Реализация задачи проектирования процессной модели в UML решается путем использования диаграмм деятельностей (Activity diagrams) для создания моделей процессов СУИБ. Объектная модель использует диаграммы классов (Class diagram) – для проектирования ресурсов.

Принципы построения и отображения процессов и сборки ресурсов

Процессная модель контекста безопасности организации по семейству стандартов ISO/IEC 2700x тесно связана с объектной, поскольку использует данные объектной модели в качестве ресурсов для процессов. При моделировании контекстного уровня СУИБ организации были сформулированы следующие принципы:

- Построение процессов начинается на верхнем уровне модели, в дальнейшем эти процессы детализируются на нижних уровнях. Терминологически можно гово-

рить о построении процессов «сверху вниз», об использовании дедуктивного метода построения процессов или о декомпозиции процессов.

- Сборка ресурсов берет начало на нижних уровнях модели, в дальнейшем эти ресурсы переходят к процессам на более высоких уровнях. В этом случае допустимо говорить о сборке ресурсов «снизу-вверх» или об использовании индуктивного метода сборки ресурсов.

Полученные результаты декомпозиции процессов

Диаграммы процессной модели детализируют процессы диаграмм более высокого уровня. Исходный процесс высокого уровня декомпозируется в соответствии с положениями ISO/IEC 27001:2005(E).

Процесс первого уровня «Establish the ISMS» декомпозируется на процессы, представленные в таблице. Для удобства восприятия определения (definition) процессов приводятся в сокращении.

	Name	**Definition**	**Reference**
1	Define the scope and boundaries of the ISMS	Define the scope and boundaries of the ISMS in terms of the characteristics of the business…	ISO/IEC 27001:2005, 4.2.1a)
2	Define an ISMS policy	Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology that…	ISO/IEC 27001:2005, 4.2.1b)
3	Define the risk assessment approach	Define the risk assessment approach of the organization 1) Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements…	ISO/IEC 27001:2005, 4.2.1 c)
4	Identify the risks	1) Identify the assets within the scope of the ISMS, and the owners2) of these assets…	ISO/IEC 27001:2005, 4.2.1 d)
5	Analyze and evaluate the risks	1) Assess the business impacts upon the organization that…	ISO/IEC 27001:2005, 4.2.1 e)
6	Risk treatment	Possible actions include: 1) applying appropriate controls; 2) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policies and the criteria for accepting risks (see 4.2.1c)2))…	ISO/IEC 27001:2005, 4.2.1 f)
7	Select control objectives and controls for the treatment of risks.	Control objectives and controls shall be selected and implemented to meet the requirements identified by the risk assessment and risk treatment process…	ISO/IEC 27001:2005, 4.2.1 g)
8	Risk acceptance	Obtain management approval of the proposed residual risks…	ISO/IEC 27001:2005, 4.2.1 h)
9	Obtain management authorization to implement and operate the ISMS	Obtain management authorization to implement and operate the ISMS…	ISO/IEC 27001:2005, 4.2.1 i)
10	Prepare a Statement of Applicability	A Statement of Applicability shall be prepared that includes the following: 1) the control objectives and controls selected in 4.2.1g) and the reasons for their selection…	ISO/IEC 27001:2005, 4.2.1 j)

Таблица 1. Декомпозиция процесса «Establish the ISMS»

На рис. 1 представлен общий вид диаграммы процессов, декомпозирующих процесс «Establish the ISMS».

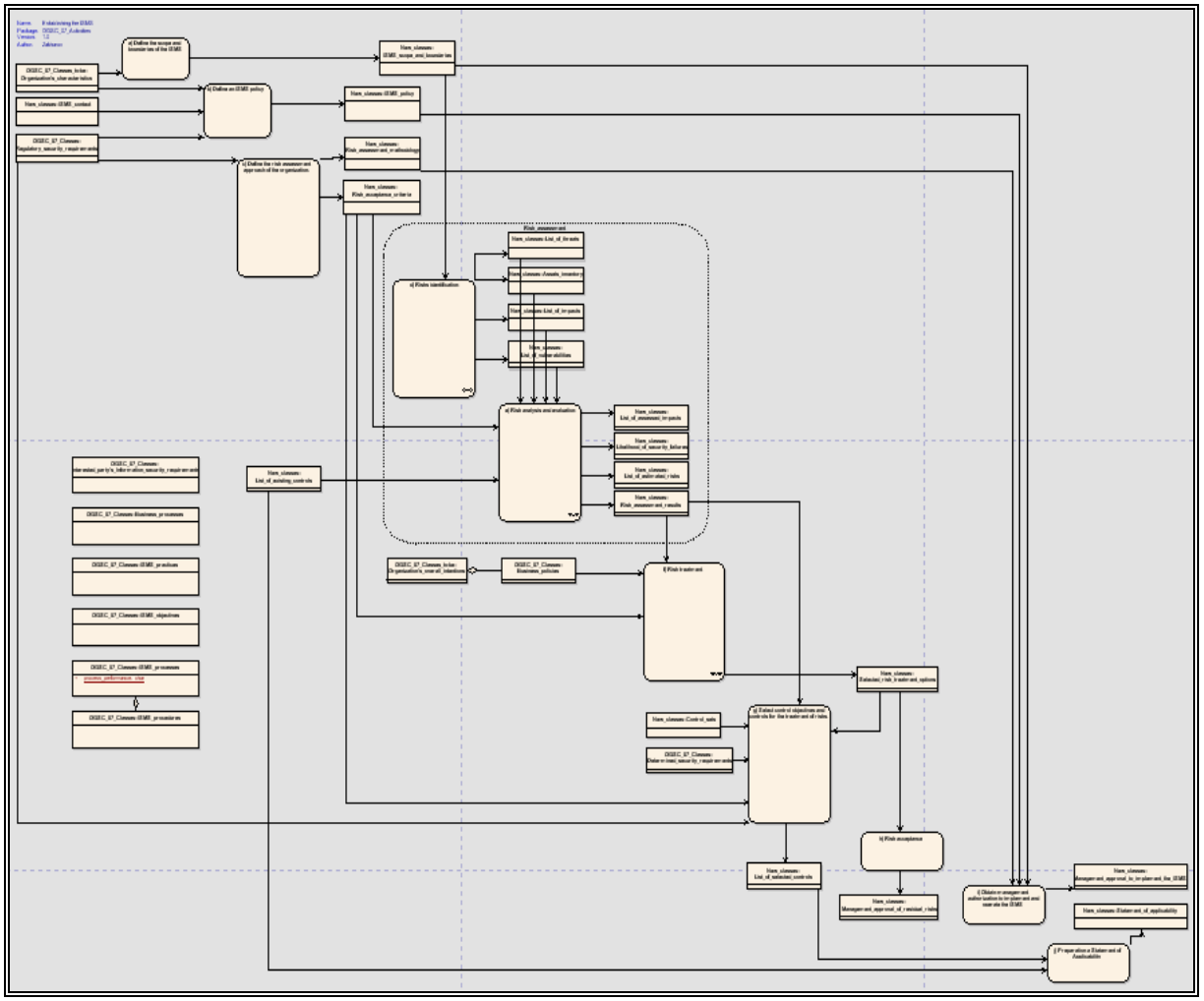


Рис. 1. Детализация процесса «Establish the ISMS»

Полученные результаты по сборке ресурсов

Сборка ресурсов начинается с нижнего уровня. Так, в ходе проведения декомпозиции процесса «Risk analysis and evaluation» были выявлены следующие процессы:

- Assessment of business impact from security failures
- Assessment of realistic likelihood of security failures
- Estimating the levels of risks
- Determining whether the risk is acceptable

На следующем этапе необходимо проанализировать текст стандарта, чтобы определить ресурсы, которые используют выявленные процессы. При сборке ресурсов аналитик опирается на положения стандарта, относящиеся к данному процессу. Так, на диаграмме декомпозиции процесса «Risk analysis and evaluation» были определены процессы и относящиеся к ним ресурсы.

	Name	Definition	Input	Output
1	Assessment of business impact from security failures	Assess the business impacts upon the organization that… [ISO/IEC 27001:2005, 4.2.1e)1)]	1.List_of_impacts	1.List_of_assessed_impacts
2	Assessment of realistic likelihood of security failures	Assess the realistic likelihood of security failures occurring in… [ISO/IEC 27001:2005, 4.2.1e)2)]	1.Assets_inventory 2.List_of_threats 3.List_of_vulnerabilities 4.List_of_assessed_impacts 5.List_of_existing_controls	1.Likelihood_of_security_failures
3	Estimating the levels of risks	Estimate the levels of risks… [ISO/IEC 27001:2005, 4.2.1e)3)]	1.List_of_assessed_impacts 2.Likehood_of_security_failures	1.List_of_estimated_risks
4	Determining whether the risk is acceptable	Determine whether the risks are acceptable or require treatment using the criteria for accepting risks [ISO/IEC 27001:2005, 4.2.1e)4)]	1.List_of_estimated_risks 2.Risk_acceptance_criteria	1.Risk_assessment_results

Таблица 2. Входящие и выходящие ресурсы процессов декомпозиции «Risk analysis and evaluation»

Пример диаграммы, детализирующей процесс «Risk analysis and evaluation» представлен ниже на рис. 2:

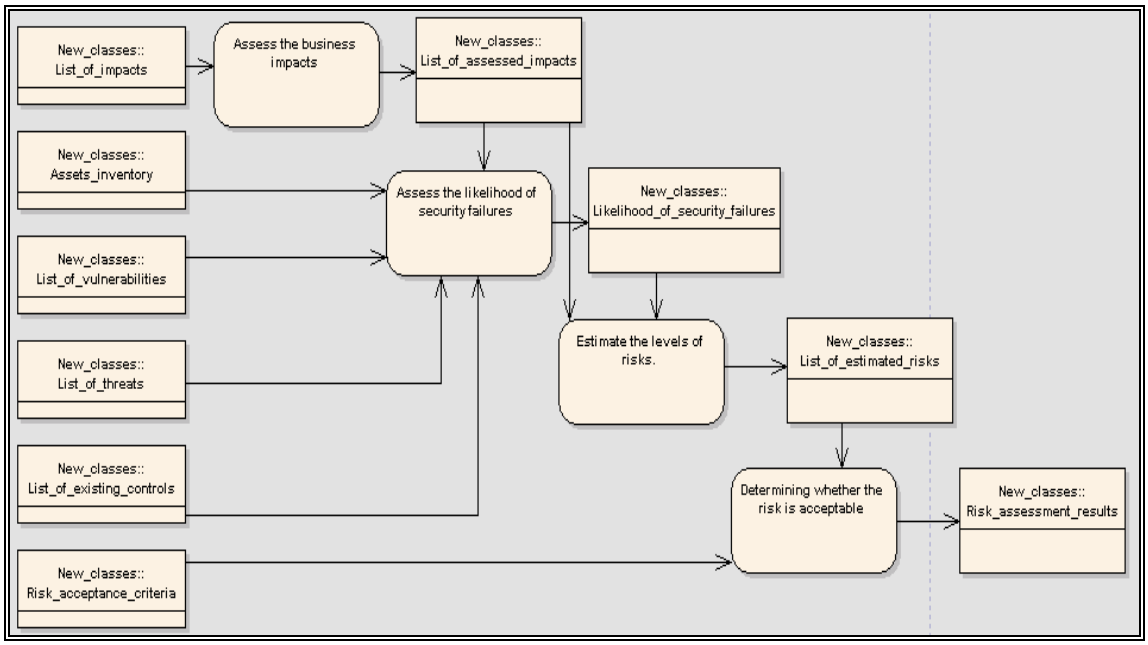


Рис. 2. Декомпозиция процесса «Risk analysis and evaluation»

На более высоком уровне входящие и исходящие ресурсы отображаются как относящиеся к процессу «Risk analysis and evaluation». Причем входящие ресурсы являются исходящими ресурсами предстоящего процесса «Risks identification», а исходящие

ресурсы процесса «Risk analysis and evaluation» являются входящими для последующих процессов.

Входящие ресурсы для процесса «Risk analysis and evaluation»:

1. Assets_inventory
2. List_of_impacts
3. List_of_threats
4. List_of_vulnerabilities
5. Risk_acceptance_criteria
6. List_of_existing_controls

Исходящие ресурсы из процесса «Risk analysis and evaluation»:

1. List_of_assessed_impacts
2. Likelihood_of_security_failures
3. List_of_estimated_risks
4. Risk_assessment_results

На рис. 3 представлены процессы «Risks identification», «Risk analysis and evaluation» и относящиеся к ним ресурсы.

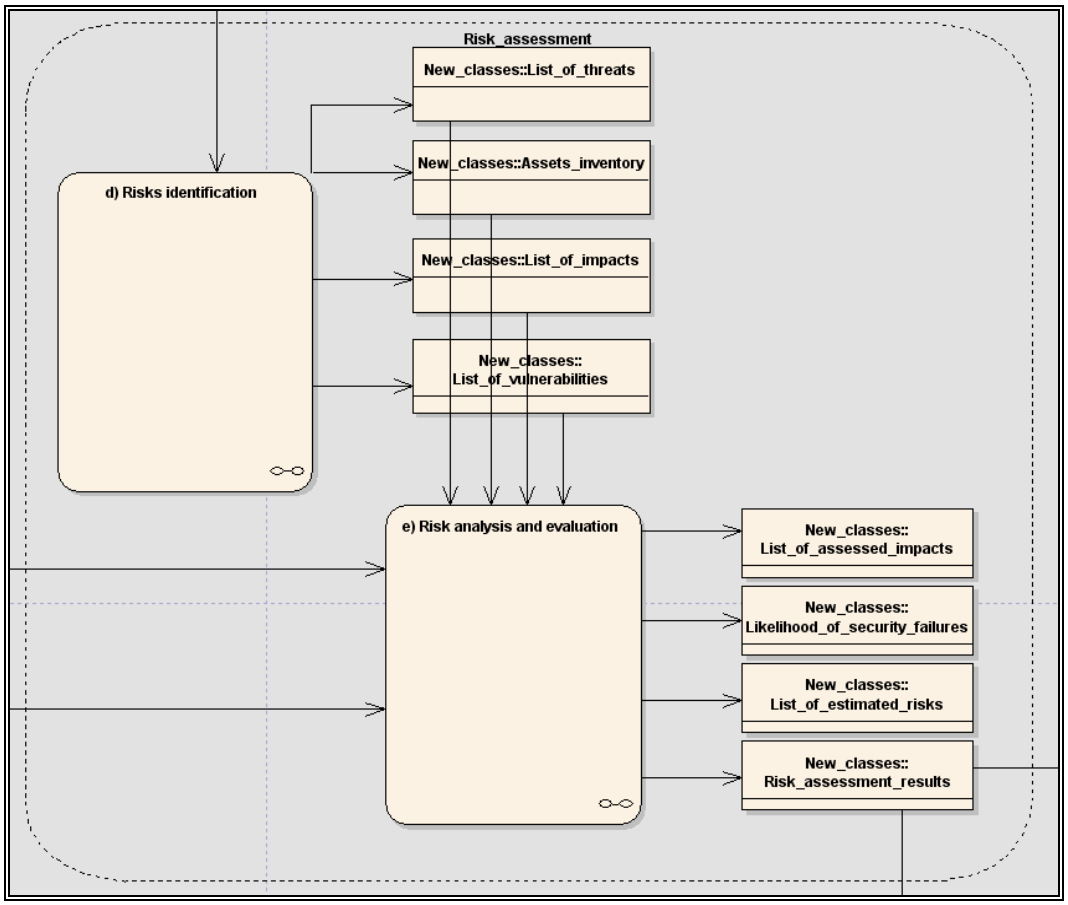


Рис. 3. Процесс «Risk_assessment»

В результате построения процессной модели СУИБ были отмечены следующие трудности:

- Неоднозначная трактовка терминов в стандарте.
- Потери ресурсов при детальной декомпозиции процессов.
- Концентрация большого числа ресурсов на высокоуровневых процессах.

- Несогласованность определений ресурсов на объектной и процессной моделях.

Анализ трудностей процессного моделирования позволяет говорить о существующих недоработках терминологической базы стандарта и о пробелах в организации процессов функционирования СУИБ. Процессная модель позволяет наглядно представить существующие недоработки стандарта ISO/IEC 27001:2005(E) и предложить положения по улучшению стандарта.

Заключение

Процессная модель позволяет построить формализованное представление структуры процессов СУИБ. В результате анализа методик моделирования были сформулированы принципы декомпозиции процессов и сборки ресурсов. Процессы детализируются «сверху вниз», сборка ресурсов происходит «снизу-вверх». В результате моделирования были построены модели процессов по разработке СУИБ, и собраны ресурсы, структура которых определена в объектной модели. В ходе моделирования были выявлены недоработки стандарта и предложены положения, улучшающие содержания стандарта.

Литература

1. ISO/IEC 27001:2005 «Information technology – Security techniques – Information security management systems – Requirements».
2. ISO/IEC 27002:2005 «Information technology – Security techniques – Code of practice for information security management».
3. Захаров А.В. Задача процессного моделирования системы управления информационной безопасностью. Сборник тезисов V Всероссийской межвузовской конференции молодых ученых. – СПб: СПбГУ ИТМО. – 2008. – 330 с.
4. Андреева Н.В. Функциональная модель системы управления информационной безопасностью как средство внедрения стандартов линейки ISO/IEC 2700x (BS 7799). Научно-технический вестник СПбГУ ИТМО. Выпуск 39. – СПб: СПбГУ ИТМО. – 2007.
5. Любимов А.В., Зайцев О.Е., Суханов А.В. Подходы к структурному моделированию основных компонентов безопасности ИТ «Общих критериев» // Труды XI-й международной конференции «Теория и технология программирования и защиты информации», Санкт–Петербург, 18 мая 2007 г. – С. 57–60.
6. Буч Г., Рамбо Д., Якобсон И. Язык UML. Руководство пользователя. 2-е изд.: Пер. с англ. Мухин Н. – М.: ДМК Пресс, 2007. – 496 с.

УДК 004.738.5

АНАЛИЗ ЗАЩИЩЕННОСТИ И ПОИСК УЯЗВИМОСТЕЙ ВЕБ-САЙТОВ

А.О. Бразовский
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В статье приводится содержание и статистика исследований в области анализа защищенности веб-сайтов. Статистика по оценке защищенности содержит результаты работ по ручному и автоматизированному анализу Web-приложений. Как правило, такие работы включают сканирование с предварительными настройками и ручным анализом результатов, ручной поиск уязвимостей недоступных автоматическим сканерам и анализ исходных кодов.
Ключевые слова: веб-сайт, Интернет, оценка защищенности, сканер безопасности, уязвимости

Международная статистика уязвимостей

В 2007 году группой компаний, в которую входили Booz Allen Hamilton, BT, Cenzic с Hailstorm, dblogic.it, HP, Application Security Center с WebInspect, Positive Technologies с MaxPatrol, Veracode, WhiteHat Security с WhiteHat Sentinel, были произведены работы с использованием автоматизированных инструментов по оценке защищенности Web-приложений. В статистику, собранную этими компаниями, вошли два набора данных: результаты автоматического тестирования и результаты работ по оценки защищенности с использованием методов BlackBox (метод черного ящика) и WhiteBox (метод белого ящика).

Данные автоматического сканирования содержат информацию по сканированию без предварительной настройки (со стандартным профилем) сайтов хостинг-провайдера. При анализе этой информации следует учитывать, что далеко не все сайты используют интерактивные элементы. Кроме того, дополнительная экспертная настройка сканера под конкретное приложение позволяет существенно повысить эффективность обнаружения уязвимостей.

Стоит также учитывать ошибки 1-го и 2-го рода при автоматическом сканировании, когда сканер безопасности может пропустить уязвимость или наоборот предположить о наличии уязвимости там, где она на самом деле отсутствует. Экспертная оценка позволяет практически устранить ошибки второго рода и минимизировать ошибки первого рода, но не исключает их.

В результате было получено 3 набора данных:

- суммарная статистика по всем видам работ;
- статистика по автоматическому сканированию;
- статистика по оценке защищенности методом «черного» и «белого» ящика.

Всего в статистику включены данные по 32717 сайтам, в которых было обнаружено 69476 уязвимостей различной степени риска [1].

Анализ данных

Анализ полученных данных показывает, что более 7% всех проанализированных сайтов может быть скомпрометировано полностью автоматически. Около 7,72% приложений содержат уязвимости высокой степени риска, обнаруженные при автоматическом сканировании систем (рис. 1). Однако при детальной ручной и автоматизированной оценке методами черного и белого ящика вероятность обнаружения уязвимости высокой степени риска достигает 96,85%.

В значительной степени это связанно с тем, что при детальном анализе оценка риска более адекватна и учитывает не только тип уязвимости, но и реальные последст-

вия ее использования с учетом архитектуры и реализации приложения. Кроме того, важным фактором является тот факт, что в автоматическом сканировании участвовали сайты хостинг-провайдера, в некоторых случаях не содержащие активного контента, в то время как работы по оценке защищенности, как правило, проводятся для приложений содержащих сложную бизнес-логику. Т.е. результаты автоматизированных сканирований можно интерпретировать как данные для среднего Интернет-сайта, в то время как «BlackBox» и «WhiteBox» больше относятся к интерактивным корпоративным Web-приложениям.

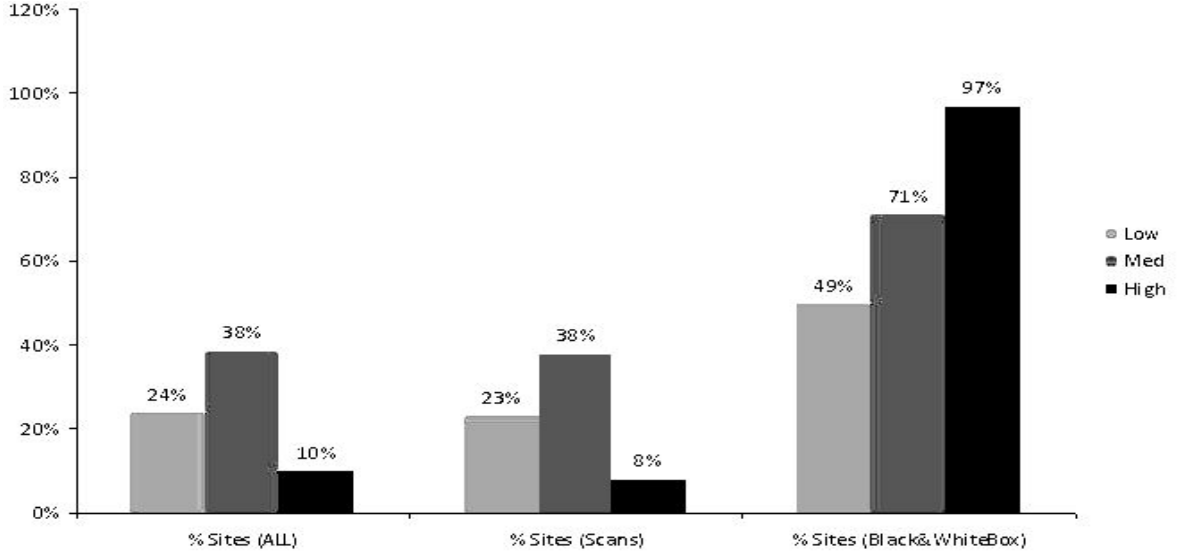


Рис. 1. Вероятность обнаружения уязвимостей различной степени риска.

Наиболее распространенными уязвимостями являются межсайтовый скриптинг (Cross-Site Scripting), утечка информации (Information Leakage), "SQL-вторжение" (SQL Injection) и предсказуемое расположение ресурсов (Predictable Resource Location) (Рис. 2). Уязвимости типа Cross-Site Scripting и SQL Injection возникают по причине ошибок в разработке систем, Information Leakage и Predictable Resource Location связаны с недостаточно эффективным администрированием в системах.

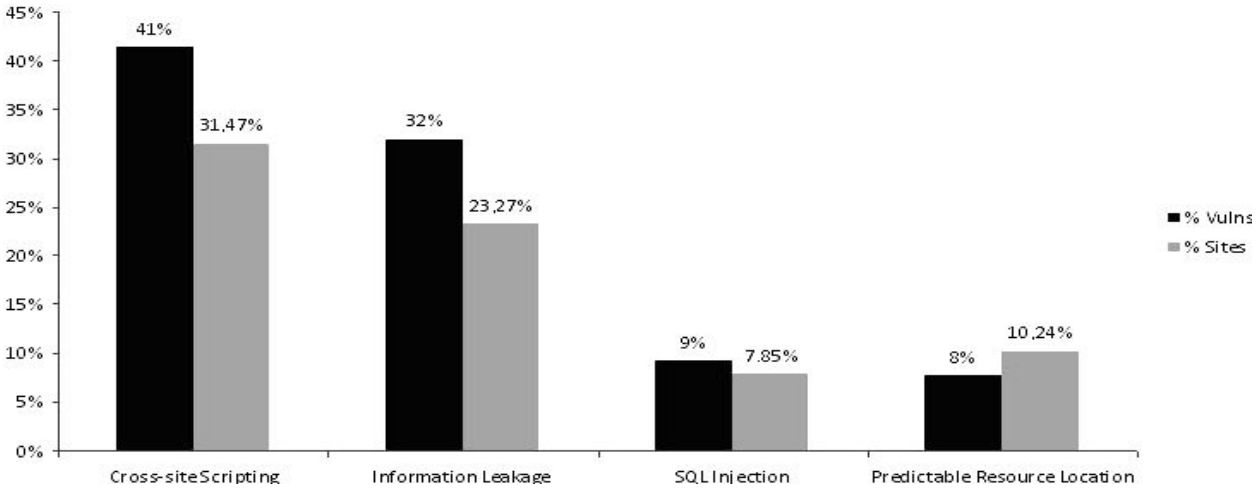


Рис. 2. Наиболее распространенные уязвимости

При детальном анализе систем методами BlackBox и WhiteBox ощутимый процент сайтов оказались уязвимы также для подмены содержания (Content Spoofing), неполного ограничения доступа (Insufficient Authorization) и неполного ограничения полномочий (Insufficient Authentication) (Рис. 3). Вероятность обнаружения уязвимостей типа SQL Injection при таком подходе к анализу защищенности достигает 25%.

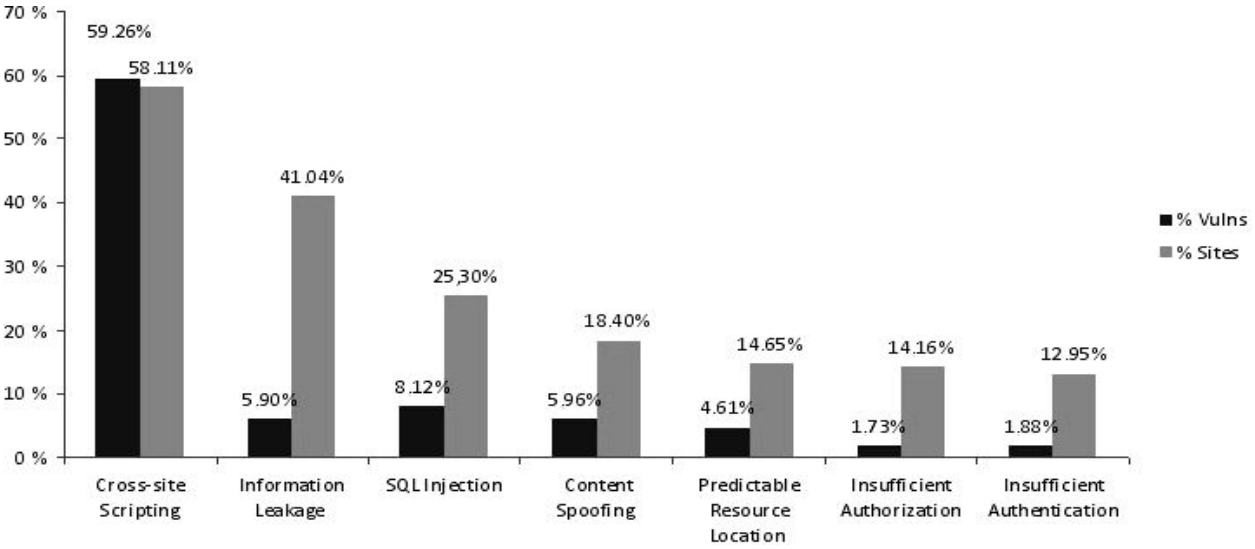


Рис. 3. Наиболее распространенные уязвимости (BlackBox & WhiteBox)

Если рассматривать вероятность обнаружения уязвимости с точки зрения классов Web Application Consortium Threat Classification version 1 (см. табл. 1), то наиболее распространены классы Атаки на клиентов (Client-side Attacks), Недостаточная защита информации (Information Disclosure) и Выполнение кода (Command Execution). Детальный анализ подтверждает распространенность классов Аутентификация (Authentication) и Авторизация (Authorization).

	% ALL	% Scans	% Black & WhiteBox
Authentication	1,17%	0,02%	20,82%
Authorization	1,28%	0,07%	19,01%
Client-side Attacks	33,13%	31,17%	69,37%
Command Execution	8,15%	7,32%	27,85%
Information Disclosure	31,78%	30,42%	56,54%
Logical Attacks	0,90%	0,20%	13,92%

Таблица 1. Распределение вероятности обнаружения уязвимости по классам WASC TCv1

Сравнение методов анализа защищенности

При сравнении автоматического сканирования с детальной оценкой методами BlackBox и WhiteBox заметно отставание автоматического сканирования в поиске уязвимостей Authorization и Authentication, логических ошибок.

Уязвимость	Отношение вероятностей выявления уязвимостей автоматическим сканированием к вероятности, полученной методами Blackbox и Whitebox
Content Spoofing	18,30%
Insufficient Authorization	14,15%
Insufficient Authentication	12,95%
SQL Injection	8,68%
Brute Force	7,98%
Abuse of Functionality	7,97%
HTTP Response Splitting	7,18%

Таблица 2. Разница в вероятности обнаружения уязвимостей различными методами

Как уже говорилось ранее (см. рис. 1), вероятность обнаружения уязвимости высокой степени риска при детальном анализе в 12,5 раз выше, чем при полностью автоматическом сканировании.

Если рассматривать такой показатель, как количество обнаруженных уязвимостей на один сайт (см. табл. 3), то детальный анализ позволяет в среднем идентифицировать до 9 уязвимостей высокой степени риска на одно приложение, в то время как автоматизированное сканирование – только 2, 3.

	All	Scans	Black&WhiteBox
Low	3,15	2,96	1,11
Med	2,35	2,04	2,65
High	4,22	2,33	8,91
All	2,12	1,61	13,11

Таблица 3. Количество уязвимостей на сайт

Дополнительные замечания

В рамках данного исследования использовалась классификация Web Application Security Consortium Threat Classification version 1. В связи с этим, некоторые типы уязвимостей не вошли в суммарные результаты. В будущем планируется применять более современную классификацию WASC TC version 2.

Наиболее широко распространенная уязвимость Cross-Site Request Forgery в рамках данной статистики занимает далеко не первое место. Это связано с двумя моментами: достоверное обнаружение ее автоматическими методами затруднено, в связи с ее распространенностью, ее присутствие воспринимается как должное многими экспертами.

Исследования Positive Technologies

В Российском сегменте Интернета тоже проводятся подобные исследования. Так, например, в 2006 г. компания Positive Technologies представила статистику по уязвимостям Web-приложений [2].

Данные получены в ходе тестирования на проникновение и оценки защищенности Web-приложений и основаны на результатах автоматизированного сканирования узлов публичного хостинг-провайдинга и ручного анализа защищенности Web-приложений.

В приводимой статистике учитываются только уязвимости Web-приложений. Такие распространенные недостатки, как отсутствие актуальных обновлений безопасности операционных систем (ОС) и неверная настройка Web-сервера не рассматриваются.

Безопасность общедоступных Web-серверов

Positive Technologies совместно с хостинг-провайдером masterhost проводит постоянное бесплатное сканирование серверов, размещенных в Интернет. Сканирование проводится с помощью сканера уязвимостей XSpider 7.5 в полностью автоматическом режиме. В среднем в месяц анализируется 10 000 различных Web-серверов. Настройка политики сканирования XSpider под конкретные серверы не производится.

Всего в 2006 г было проведено 111 936 сканирований, обнаружено 129 197 различных уязвимостей высокого и среднего уровня риска. Уязвимыми оказались 31 113 сайтов. Уязвимости низкой степени риска в данный отчет не включены, в связи с низкой достоверностью их обнаружения в ходе полностью автоматического сканирования.

Уязвимость	Процент уязвимостей	Уязвимые сайты
Cross-Site Scripting	72,22%	23,28%
SQL injection	14,67%	7,28%
Information Leakage	8,26%	4,20%
HTTP Response Splitting	3,47%	2,74%
SSI Injection	0,74%	0,27%
Path Traversal	0,32%	0,32%
OS Commanding	0,11%	0,03%
…	…	…

Таблица 4. Распределение обнаруженных уязвимостей по различным классам

Наиболее распространена уязвимость класса "Межсайтовое выполнение сценариев" (Cross-Site Scripting, XSS). Эта уязвимость была обнаружена на 23% из всех сайтов. Количество идентифицированных XSS составляет до 72% всех обнаруженных ошибок. В среднем каждый уязвимый сайт содержит 4 уязвимости данного класса.

Вторая по полярности уязвимость класса "Внедрение операторов SQL" (SQL Injection) содержится в 7% сайтов и на нее приходится 14% общего количества ошибок.

На третьем месте – уязвимости, приводящие к утечке важной информации с сервера (Information Leakage). На них приходится 4% серверов и 8% всех ошибок. В данную статистику включались только те, которые могут быть отнесены к средней степени риска.

Если рассматривать распределение ошибок по степени риска, то на критичные уязвимости приходится всего 15%. Такой невысокий процент вызван ограничениями, связанными с используемым методом сбора данных. Суммарная вероятность обнаружения на сервере уязвимостей различной степени риска: высокая – 7,86%, низкая – 28,67%.

Безопасность корпоративных Web-приложений

Данные получены компанией Positive Technologies в ходе анализа и оценки защищенности Web-приложений в 4-м квартале 2006 г. Работы проводились с использованием как ручных, так и автоматизированных средств. Всего в статистику вошли данные по 35 различным Web-приложениям, таким как системы клиент-банк, электронные торговые площадки, внешние корпоративные сайты и т.д. В общей сложности на серверах было обнаружено 368 различных уязвимостей Web-приложений.

Уязвимость	Процент уязвимостей	Процент сайтов
Cross-Site Scripting	44,8%	83%
Information Leakage	21,2%	80%
Predictable Resource Location	5,4%	34%
SQL injection	10,1%	31%
HTTP Response Splitting	3,5%	29%
Insufficient Authorization	3,3%	20%
Directory Indexing	3,0%	20%
Insufficient Anti-automation	1,6%	17%
Path Traversal	1,4%	11%

Insufficient Authentication	1,1%	11%
Insufficient Process Validation	1,1%	11%
Bruteforce	0,8%	9%
SSI Injection	1,1%	6%
…	….	…

Таблица 5. Распределение обнаруженных уязвимостей корпоративных Web-приложений по различным классам

В отличие от статистики, полученной в ходе только автоматизированного сканирования Web-серверов, ручной анализ позволил выявить гораздо большее количество ошибок. Это связанно как с меньшей эффективностью полностью автоматизированного сканирования, так и с тем фактом, что во втором случае анализу подвергались приложения, заведомо содержащие динамический контент.

Кроме того, в статистике появились новые классы уязвимостей, такие как "Недостаточная аутентификация и авторизация" (Insufficient Authorization, Insufficient Authentication) и др. Это связанно с тем, что данные недочеты относятся к так называемым "логическим ошибкам", обнаружение которых с помощью автоматизированных средств затруднено, т.к. требует понимания бизнес-логики приложения.

Как и в предыдущем случае, наиболее распространенной уязвимостью является "Межсайтовое выполнение сценариев" (83%). Внедрение операторов SQL переместилось на третье место по количеству (10,1%) и на четвертое место по полярности (31%).

Второе и третье место занимают разглашение информации (Information Leakage) и предсказуемое расположение ресурсов (Predictable Resource Location).

Следует отметить, что логические ошибки достаточно распространены. Так, ошибки системы авторизации, были обнаружены на 20% сайтов. Недостатки системы аутентификации встречались в 11% систем. Несмотря на относительно небольшой процент подобных уязвимостей на фоне других (суммарно 4,4%), зачастую достаточно наличия одной ошибки для полной компрометации системы.

Более половины (54%) из всех обнаруженных недочетов – это уязвимости средней степени риска. Серьезное место занимают ошибки "Межсайтовое выполнение сценариев". На уязвимости низкой и высокой степени риска приходится 27% и 18% соответственно.

Суммарная вероятность обнаружения уязвимостей различной степени риска при глубоком анализе Web-приложений: высокая – 65%, средняя – 93%, низкая – 99%. То есть в 65% сайтов были обнаружены критичные уязвимости, в 93 случаев из 100 в программном обеспечении веб-приложения содержатся уязвимости средней степени риска.

Заключение

В заключении чтобы подчеркнуть значимость проблематики и необходимость изучения данной сферы, хотелось бы привести несколько слов ведущих Российских специалистов в области веб-безопасности об уязвленности веб сайтов [3]:

Руководитель отдела сетевых проектов компании «Доктор Веб» **Евгений Кузин**:

«Широкое распространение DDoS-атак произошло благодаря так называемым – ботнетам – логическим сетям внутри Интернета, состоящим из зараженных вирусами (многие современные вирусы имеют в себе функцию удаленного контроля над ПК) компьютеров. Хакеры, контролирующие сеть, могут за несколько минут привести ее в боевую готовность и заставить тысячи компьютеров по всему миру рассылать спам, вирусы или же атаковать сайты. Обычный пользователь при этом останется в неведении, даже не подозревая, для чего именно используется его компьютер»

Старший вирусный аналитик «Лаборатории Касперского» **Виталий Камлюк**:

«Сегодня невозможно сделать так, чтобы сайт не был атакован – возможность допустить атаку существует, пока у легального пользователя существует возможность открыть веб-сайт с этого сервера. Но грамотно выстроенная система защиты позволяет минимизировать последствия нападения, либо перенести его практически без потерь»

Литература

1. «Международная статистика уязвимостей WEB» http://www.webappsec.org/projects/statistics/
2. «Сетевая безопасность: наиболее распространенные уязвимости Web-приложений» http://www.bit.prime-tass.ru/news/show.asp?topicid=17&id=46543
3. «Перед атакой все равны» http://telnews.ru/Dmitrij_Rodin/c49018

УДК: 002:004:056

СОВРЕМЕННЫЕ МЕТОДЫ И СРЕДСТВА СЕТЕВОЙ ЗАЩИТЫ. МЕЖСЕТЕВЫЕ ЭКРАНЫ

М.А. Семенова, В.А. Семенов
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Вопросы информационной безопасности в Internet остаются на сегодняшний момент одним из самых актуальных. Покупая у поставщиков МЭ их продукт, заказчик не решит все эти проблемы, обеспечив надежную защиту всех ресурсов корпоративной сети. И не потому что предлагаемый МЭ не обеспечивает необходимой защиты механизмов, а потому что необходимо сделать правильный выбор МЭ может быть даже комбинируя их. А для этого необходимо разобраться во всех плюсах и минусах различных технологий. На основе приведенной в статье классификации МЭ более отчетливо прослеживаются их достоинства и недостатки.

Ключевые слова: автоматизированные системы, межсетевые экраны, проблемы безопасности, обеспечение информационной безопасности, угрозы ИБ, пакетные фильтры, шлюзы, аутентификация, вирусы и атаки, мобильный код

Введение

Когда речь заходит о защите от атак на автоматизированные системы (АС), то первое, что приходит на ум большинству пользователей, – это межсетевые экраны (МЭ). Говоря общими словами МЭ – это локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС.

МЭ, защищающий сразу множество (не менее двух) узлов (машин), призван решить две задачи: 1) ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам корпоративной сети; 2) разграничение доступа пользователей защищаемой сети к внешним ресурсам. Решение этой задачи позволяет, например, регулировать доступ к серверам, не требуемым для выполнения служебных обязанностей.

МЭ используют в своей работе один из двух принципов:

1. "Разрешено все, что не запрещено в явном виде". Данный принцип облегчает администрирование межсетевого экрана, т.к. от администратора не требуется никакой предварительной настройки.

2. "Запрещено все, не разрешено в явном виде". Этот принцип делает межсетевой экран практически неприступной стеной. Однако, повышая защищенность, мы тем самым нагружаем администратора безопасности дополнительными задачами по предварительной настройке базы правил межсетевого экрана.

Классификация

Функционально МЭ разделяются на три основных категории (типа):

Рис. 1. Классы МЭ

Каждая из этих систем имеет свои преимущества и свои недостатки. Ниже будут описаны принципиальные различия между ними.

Для определения уровня защищенности МЭ, который они обеспечивают при межсетевом взаимодействии, применяются показатели защищенности. Конкретные перечни показателей определяют классы защищенности МЭ. Деление МЭ на соответствующие классы необходимо в целях разработки и применения обоснованных и экономически оправданных мер по достижению требуемого уровня защиты информации при взаимодействии сетей ЭВМ, АС. Устанавливается 5 классов защищенности МЭ[1, 2]. Самый низкий – пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый – для 1Г, третий – 1В, второй – 1Б, самый высокий – первый 1А. [3].

Показатели защищенности	**Классы защищенности**				
	5	**4**	**3**	**2**	**1**
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	=
Тестирование	+	+	+	+	+
Руководство администратора	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

(«+» – присутствует; «-» – частично отсутствует; «=» – полностью отсутствует)

Таблица 1. Требования к защищенности МЭ

Пакетные фильтры

Пакетные фильтры – это одни из первых и самые распространенные МЭ, которые функционируют на третьем, сетевом уровне и принимают решение о разрешении прохождения трафика в сеть на основании информации, находящейся в заголовке пакета. Именно эта технология используется в абсолютном большинстве маршрутизаторов и даже коммутаторах. В качестве параметров, используемых при анализе заголовков сетевых пакетов, могут использоваться: 1)адреса отправителей и получателей; 2)тип протокола (TCP, UDP и т.д.); 3)номера портов отправителей и получателей (для TCP и UDP трафика); 4)другие параметры заголовка пакета (например, флаги TCP-заголовка).

С помощью данных параметров, описанных в специальном наборе правил, можно задавать достаточно гибкую схему разграничения доступа.

Пакетные фильтры, обладая рядом достоинств, не лишены и ряда серьезных недостатков. Во-первых, исходя из того, что они анализируют только заголовок, за пределами рассмотрения остается поле данных, которое может содержать информацию, противоречащую политике безопасности. В целом, недостаток пакетных фильтров заключается в том, что они не умеют анализировать трафик на прикладном уровне, на котором совершается множество атак – проникновение вирусов и т.д.

Другой недостаток пакетных фильтров – сложность настройки и администрирования. Приходится создавать как минимум два правила для каждого типа разрешенного взаимодействия (для входящего и исходящего трафика). Неконтролируемое увеличение числа правил может приводить к появлению брешей в первой линии обороны, создаваемой пакетными фильтрами. И не стоит забывать, что при настройке фильтра может случиться ситуация, когда одно правило противоречит другому. Увеличение числа правил несет с собой и еще одну проблему – снижение производительности межсетевого экрана.

Данные МЭ могут быть реализованы как аппаратно, так и программно. Причем пакетный фильтр может быть установлен не только на устройстве, расположенном на границе между двумя сетями (например, на маршрутизаторе), но и на рабочей станции пользователя, повышая тем самым ее защищенность.

Однако достоинства пакетных фильтров перевешивают указанные недостатки и обуславливает их повсеместное распространение.

Достоинства	Недостатки
1.Высокая скорость работы. 2.Простота реализации. 3.Данная возможность встроена во все маршрутизаторы и многие ОС, что не требует дополнительных финансовых затрат. 4. Низкая стоимость или свободное распространение (в случае приобретения).	1.Отсутствует возможность анализа прикладного уровня. 2. Нет защиты от подмены адреса. 3. Сложность настройки и администрирования. 4.При увеличении числа правил возможно снижение производительности. 5.Требуется детальное знание сетевых услуг и протоколов. 6. Нет контроля состояния соединения. 7.Трудность функционирования в сетях с динамическим распределением адресов.

Таблица 2. Достоинства и недостатки пакетных фильтров

Шлюз на сеансовом уровне

Эта технология практически не встречается в виде единственной технологии, реализованной в межсетевом экране. Они поставляются в рамках прикладных шлюзов или инспекторов состояний.

Смысл технологии фильтрации на сеансовом уровне заключается в том, что шлюз исключает прямое взаимодействие двух узлов, выступая в качестве посредника, который перехватывает все запросы одного узла на доступ к другому и, после проверки допустимости таких запросов, устанавливает соединение. После этого шлюз сеансового уровня просто копирует пакеты, передаваемые в рамках одной сессии, между двумя узлами, не осуществляя дополнительной фильтрации.

Достоинство данной технологии, в том, что она исключает прямой контакт между двумя узлами. Адрес шлюза сеансового уровня является единственным элементом, который связывает внешнюю сеть, с внутренними, защищаемыми ресурсами. Кроме того, поскольку соединение между узлами устанавливается только после проверки его допустимости, то тем самым шлюз предотвращает возможность реализации подмены адреса, присущую пакетным фильтрам.

Несмотря на кажущуюся эффективность этой технологии, у нее есть один очень серьезный недостаток – невозможность проверки содержания поля данных. Т.е. тем самым злоумышленник может передать в защищаемую сеть вирус.

Достоинства	Недостатки
1.Высокая скорость работы. 2. Простота реализации. 3.Исключение прямого взаимодействия между двумя узлами. 4. Контроль состояния соединения.	Отсутствует возможность анализа прикладного уровня.

Таблица 3. Достоинства и недостатки шлюзов сеансового уровня

Шлюз на прикладном уровне

Посредники прикладного уровня практически ничем не отличаются от шлюзов сеансового уровня, за одним исключением. Они также осуществляют посредническую функцию между двумя узлами, исключая их непосредственное взаимодействие, но позволяют проникать в контекст передаваемого трафика, т.к. функционируют на прикладном уровне. МЭ, построенные по этой технологии, содержат т.н. посредников приложений и могут, например, разрешать в исходящем трафике команду GET (получение

файла) протокола FTP и запрещать команду PUT (отправка файла) и наоборот. Еще одно отличие от шлюзов сеансового уровня – возможность фильтрации каждого пакета.

Достоинства	Недостатки
1.Анализ на прикладном уровне и возможность реализации дополнительных механизмов защиты (например, анализ содержимого). 2. Исключение прямого взаимодействия между двумя узлами. 3. Высокий уровень защищенности. 4. Контроль состояния соединения.	1.Невозможность анализа трафика от "неизвестного" приложения. 2. Невысокая производительность. 3.Уязвимость к атакам на уровне ОС и приложений. 4. Требование изменения модификации клиентского ПО. 5. Не всегда есть посредник для приложений на базе протоколов UDP и RPC. 6. Двойной анализ - на уровне приложения и уровне посредника.

Таблица 4. Достоинства и недостатки шлюзов прикладного уровня

Инспекторы состояния

Совмещают в себе все достоинства названных выше типов экранов, начиная анализ трафика с сетевого и заканчивая прикладным уровнями, что позволяет совместить в одном устройстве казалось бы, несовместимые вещи – большую производительность и высокую защищенность. Эти МЭ позволяют контролировать: 1) каждый передаваемый пакет (на основе имеющейся таблицы правил); 2) каждую сессию (на основе таблицы состояний); 3) каждое приложение (на основе разработанных посредников).

Действуя по принципу шлюза сеансового уровня, инспектор состояния, тем не менее, не препятствует установлению соединения между двумя узлами, за счет этого производительность такого межсетевого экрана существенно выше, чем у шлюза сеансового и прикладного уровня, приближаясь к значениям, встречающимся только у пакетных фильтров. Еще одно достоинство межсетевых экранов с контролем состояния – прозрачность для конечного пользователя, не требующая дополнительной настройки или изменения конфигурации клиентского программного обеспечения.

Коммутаторы

Данные устройства, функционирующие на канальном уровне, не принято причислять к классу межсетевых экранов, т.к. они разграничивают доступ в рамках локальной сети и не могут быть применены для ограничения трафика из Internet. Однако, основываясь на том факте, что межсетевой экран разделяет доступ между двумя сетями или узлами, такое причисление вполне закономерно.

Многие производители коммутаторов, позволяют осуществлять фильтрацию трафика на основе MAC-адресов, содержащихся во фреймах, пытающихся получить доступ к определенному порту коммутатора. Однако практически все современные сетевые карты позволяют программно изменять их MAC-адреса, что приводит к неэффективности такого метода фильтрации. Поэтому существуют и другие параметры, которые могут использоваться в качестве признака фильтрации.

Достоинства	Недостатки
1.Высокая скорость работы. 2.Данная возможность встроена в большинство коммутаторов, что не требует дополнительных финансовых затрат.	1.Отсутствует возможность анализа прикладного уровня. 2. Отсутствует возможность анализа заголовков сетевого и сеансового уровней (исключая некоторые коммутаторы). 3. Нет защиты от подмены адреса.

Таблица 5. Достоинства и недостатки коммутаторов

Выбор межсетевого экрана

Нельзя сделать однозначный выбор в пользу какого-либо из названных экранов. Лучше если вы сможете использовать два межсетевых экрана, строя, таким образом, эшелонированную оборону своей сети. Если один из экранов будет выведен из строя, то до тех пор его работоспособность не будет восстановлена, весь удар примет на себя второй экран.

Возможности

Помимо фильтрации трафика МЭ позволяют выполнять и другие, не менее важные функции, такие как:

Трансляция сетевых адресов

Как показано ранее, для реализации многих атак злоумышленнику необходимо знать адрес своей жертвы. Чтобы скрыть эти адреса, а также топологию всей сети, МЭ выполняют очень важную функцию – трансляцию сетевых адресов. Трансляция может осуществлять двумя способами – динамически и статически. В первом случае адрес выделяется узлу в момент обращения к межсетевому экрану. Во втором случае адрес узла всегда привязывается к одному адресу МСЭ.

Аутентификация пользователей

МЭ помимо разрешения или запрещения допуска различных приложений в сеть, также могут выполнять аналогичные действия и для пользователей, которые желают получить доступ к внешним или внутренним ресурсам, разделяемым межсетевым экраном. При этом проверка подлинности (аутентификация) пользователя может осуществляться как при предъявлении обычного идентификатора (имени) и пароля, так и с помощью более надежных методов, например, с помощью цифровых сертификатов.

Регистрация событий

Являясь критическим элементом системы защиты корпоративной сети, межсетевой экран имеет возможность регистрации всех действий, им фиксируемых. Такая регистрация позволяет обращаться к создаваемым журналам по мере необходимости.

Реализация

Существует два варианта реализации МЭ – программный и программно-аппаратный. Второй вариант также может быть реализован двояко – в виде специализированного устройства и в виде модуля в маршрутизаторе или коммутаторе.

Первое решение – наиболее часто используемое в настоящее время. Хотя на практике далеко не всегда в организации находится свободный компьютер, удовлетворяющий достаточно высоким требованиям по системным ресурсам. Поэтому одновременно с приобретением ПО приобретается и компьютер для его установки. И только после этого устанавливается и настраивается ПО системы обнаружения атак.

Именно поэтому в последние годы стали получать распространения специализированные программно-аппаратные решения. Они поставляются, как специальные программно-аппаратные комплексы, использующие специализированные или обычные операционные системы для выполнения только заданных функций.

Недостатки

Выше уже были перечислены некоторые недостатки, присущие межсетевым экранам, а также способы их обхода. Ниже мы укажем еще некоторые из них.

Потенциально опасные возможности

Новые возможности, которые появились недавно, и которые облегчают жизнь пользователям Internet, разрабатывались без учета требований безопасности. Специфика мобильного кода такова, что он может быть использован и как средство для проведения атак, и как объект атаки.

Как средство для проведения атак мобильный код может быть реализован в виде: вируса; агента, перехватывающего пароли, номера кредитных карт и т.п.

Обычный подход, используемые при обнаружении мобильного кода, заключается в том, чтобы сканировать весь входящий трафик на 80-м или 443-м портах, используемых протоколами HHTP и HTTPS, с целью выявить такие элементы. Но этого недостаточно, т.к. файл с одним расширением может выдавать себя за другой файл и тем самым обойти защиту и оказаться в компьютере.

Другой подход заключается в сканировании всего трафика, проходящего в защищаемом сегменте, чтобы выявить наличие конкретных участков кода. Данный подход производителями средств защиты практически не применяется из-за интенсивности трафика.

Вирусы и атаки

Практически ни один межсетевой экран не имеет встроенных механизмов защиты от вирусов и от атак. Как правило, эта возможность реализуется путем присоединения к МЭ дополнительных модулей или программ разработчиков. Как можно защититься от вирусов или атак, если они проходят через МЭ в зашифрованном виде и расшифровываются только на оконечных устройствах клиентов?

В таком случае лучше перестраховаться и запретить прохождение через межсетевой экран данных в неизвестном формате [1].

Персональные МЭ

Сейчас полноправным пользователем защищаемой МЭ сети является сотрудник, находящийся за пределами защищаемого периметра. К таким сотрудникам относятся пользователи, работающие на дому или находящиеся в командировке. Но все традиционные МЭ построены так, что защищаемые пользователи и ресурсы должны находиться с внутренней стороны, что является невозможным для мобильных пользователей. Чтобы устранить эту проблему было предложено два подхода – виртуальные частные сети и распределенные МЭ. Первое решение обладало только одним недостатком – сам удаленный узел был подвержен атакам, хотя доступ в корпоративную сеть был защищен от несанкционированных воздействий. Установленный на удаленное рабочее место троянский конь мог дать возможность проникнуть злоумышленнику через межсетевой экран и по защищенному каналу. Ведь VPN шифрует и обычный, и несанкционированный трафик, не делая между ними различий. Тогда-то и родилась идея распределенного межсетевого экрана, который являлся бы мини-экраном, защищающим не всю сеть, а только отдельный компьютер. Многие функции распределенного МЭ для домашних пользователей были лишними, поэтому был создан новый подход, который получил название «персонального межсетевого экрана».

Главное отличие персонального МЭ от распределенного – это наличие функции централизованного управления. Именно поэтому распределенные МЭ должны обладать эффективным механизмом настройки, администрирования и контроля, позволяющим администратору безопасности без дополнительных усилий получить подробную информацию о зафиксированных попытках проникновения на защищаемые узлы.

Заключение

Правильный выбор персонального или распределенного МЭ позволит повысить защищенность компьютеров, которые при обычных условиях остаются незащищенными и могут служить точкой проникновения в корпоративную сеть.

Литература

1. Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». – Москва. – 1992.
2. Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». – Москва. – 1992.
3. Специальные нормативные документы ФСТЭК России http://www.fstec.ru/_razd/_ispo.htm

УДК 004.056

ИССЛЕДОВАНИЕ КОНКУРИРУЮЩЕГО ВЗАИМОДЕЙСТВИЯ КОРПОРАТИВНЫХ РЕСУРСОВ НА ОСНОВЕ АНАЛИЗА ИСТОРИКО-СОЦИАЛЬНЫХ МОДЕЛЕЙ. ИССЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ И ЯЗЫКОВЫХ СВЯЗЕЙ

М.В. Береговой
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Исторически сложившиеся социальные модели, фактически могут быть применимы для исследования корпоративных структур. Анализ подобных моделей может помочь более широко взглянуть на корпоративную теорию и принципы конкурентной борьбы.

Ключевые слова: конкурирующее взаимодействие, корпорация, корпоративные ресурсы, информационные связи

Введение

В процессе развития информационных технологий наличие конкурирующего взаимодействия между компонентами системы и борьба за установление контроля отдельных компонентов над однородными общесистемными ресурсами привело к обострению вопросов защиты и безопасности информации.

Конкуренция может возникать как за ресурсы индивидуумов не входящих в корпорацию, так и входящих в неё. Естественно, ни одна корпорация не стремиться к одномоментному захвату ресурсов другой корпорации, так как это требует, как правило, слишком значительных затрат. В данной работе предполагается, что корпорации примерно равны, следовательно, приведённый выше силлогизм верен. Конкурирующая корпорация стремиться взять под контроль индивидуумы и их ресурсы, тем самым, ослабляя соперника.

Конкуренция в любой момент времени представляет собой взаимодействие двух индивидуумов. Один индивидуум, при помощи языка и информации, оказывает влияние на другого, например, передавая ложную информацию и/или выдавая себя за члена корпорации. Целью является получение доступа к части корпоративных ресурсов, которыми владеет индивидуум. Также возможна компрометация индивидуума и, как следствие, компрометация корпоративных ресурсов и нарушение нормального информационного взаимодействия в корпорации.

1. Понятие корпорации, ресурсов и системы

Корпоративную систему можно рассматривать как совокупность субъектов, обладающих частью общих характеристик. Между такими субъектами существуют информационные взаимодействия, т.е. взаимный или односторонний обмен данными. Из этого утверждения следует, что корпоративную систему можно представить как информационную систему, обладающую совокупностью субъектов, осуществляющих информационное взаимодействие. Особенность корпоративной системы как информационной системы заключается в корпоративном характере информационных процессов.

Информационное взаимодействие возникает только при наличии других подобных и конкурирующих субъектов, то есть системы субъектов, что является основой для возникновения между субъектами с целью организации совместной и конкурентной борьбы за ресурсы развития и существования как системы в целом, так и субъектов этой системы. Естественно, подразумевается, что субъекты системы находятся в постоянном информационном взаимодействии между собой.

Субъекты такой системы разделяются по уровням сложности и используемые ими ресурсы также можно разделить по уровням комплексности, т.е. чем сложнее субъект, тем большее разнообразие ресурсов он может использовать.

Объединение во временные объединения – корпорации, связано с необходимостью обеспечения «секретности», по Шеннону, от других членов [4]. Поэтому свойства языка корпорации определяются числом возможных объединений в корпорации, при соблюдении определённых правил безопасности. Также имеет смысл учитывать возможность субъектов объединения в корпорацию, так и отсутствие таковой. Здесь имеется в виду территориальная разрозненность субъектов и параметры каналов связи. Логично, что подобное объединение при сильном удалении субъектов друг от друга, потребует значительных затрат на физическое обеспечение взаимодействия.

В определённый момент возникает внутрикорпоративная конкуренция за ресурсы, как материальные, так и информационные. Защита и безопасность информации становятся важнейшей частью как существования и правильного функционирования системы в целом, так и индивидуального, заключающегося в оптимальном изменении и использовании ресурсов [2].

2.Время жизни и возникновение конкуренции

Образование, развитие и функционирование любой системы, аналогично биологическим процессам в природе. Поэтому сравнение возможно, и далее будут использоваться термины «популяция», т.е. совокупность субъектов и «индивидуум», собственно сам субъект. Каждый индивидуум имеет время жизни, в течение которого создает перераспределяет и приобретает информацию, участвует в создании новых индивидуумов и защищенных образований. Время жизни корпорации больше чем у индивида. Время жизни корпорации тратится на приобретение ресурсов и увеличение количества индивидов. Для лучшей конкуренции необходимо большее количество субъектов, соответственно корпорация растет. Как только численность индивидов в корпорации стабилизируется, конкуренция приобретает вид перераспределения и обработки информации.

При наличии информации, как инструмента борьбы за системные ресурсы, возникают объединения, то есть группы индивидуумов, контролирующих общую часть системных ресурсов. Здесь информация выступает в роли характеристики системных ресурсов, а, значит, помогает противостоять остальным индивидуумам популяции. При помощи информации индивидуум в объединении контролирует часть системных ресурсов объединения, которая заведомо больше чем часть ресурсов, которые контролирует отдельный индивидуум.

После того, как образовались несколько объединений, необходим новый элемент для борьбы за ресурсы, которые или еще не распределены по объединениям, или за ресурсы самих объединений, причем между индивидуумами этих объединений. В этот момент и появляется язык, который способствует распределению информации между индивидуумами. Появление языка влечет за собой появление корпораций, в которых индивидуумы объединены для получения большого количества ресурсов и существуют связи для обмена информацией, то есть происходит как само накопление информации, так и ее распределение.

В данной модели изображенной на рисунке, отражен процесс развития популяции, ее составляющие и связи между ними.

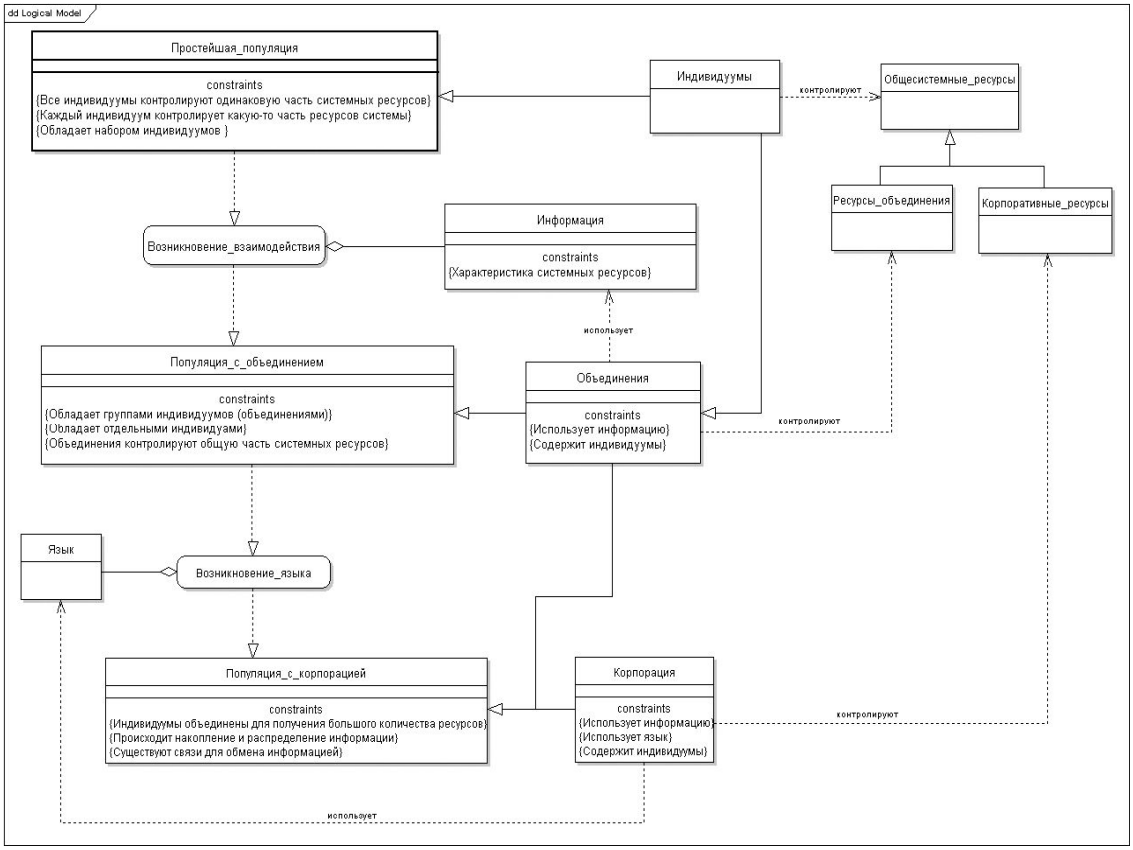


Рисунок. Структурная модель информационно-логических связей в корпорации

В корпорации каждый индивидуум при помощи языка устанавливает различные отношения с другими индивидуумами. В результате таких отношений возникает распределение информации внутри корпорации. Такая деятельность корпорации направлена на накопление корпоративных ресурсов и их сохранение. Так как информация это инструмент для накопления ресурсов, то возникает необходимость в ее защите. Потеря информации, которой располагают индивидуумы, не может привести к большим потерям корпоративных ресурсов.

2.1. Конкуренция в историческом контексте

Исторические процессы, рассмотренные в контексте, как межгосударственных отношений, так и отдельно взятого государства, фактически могут быть применимы для исследования корпоративных структур. Это в полной мере относиться и к религиям, как к неотъемлемой части истории.

Корпорацию можно рассматривать как систему различных индивидуумов, между которыми происходят постоянные взаимодействия по обмену формализованными данными. Для взаимодействия между индивидуумами необходим инструмент, этим инструментом являются информация и язык. Корпорация может изолировать индивидуума, если таковой мешает нормальному функционированию системы в целом или её компонентов. Как пример, тюремное заключение.

Между корпорациями может возникать конкурирующее взаимодействие, более того, как показывает история – это нормальное состояние для корпораций.

Конкуренция может возникать как за ресурсы индивидуумов не входящих в корпорацию, так и входящих в неё. Естественно, ни одна корпорация не стремиться к одномоментному захвату ресурсов другой корпорации, так как это требует, как правило, слишком значительных затрат. Конкурирующая корпорация стремиться взять под кон-

троль индивидуумы и их ресурсы, тем самым, ослабляя соперника. Также возможна компрометация индивидуума и, как следствие, компрометация корпоративных ресурсов и нарушение нормального информационного взаимодействия в корпорации.

Подобное конкурирующее взаимодействие можно рассмотреть на примере любого восстания. Одна из корпораций стремиться избавиться от влияния другой, ослабляя индивидуумов, получая контроль над ресурсами. Это может реализовываться за счёт языка и информации, причём применяя именно свойственные корпорации-противнику. Зачастую, это позволяет получать контроль над ресурсами без применения активных действий, например агитация.

Развитие цивилизаций по своим параметрам схоже с биологическими процессами, в частности с вирусами. Здесь возможно найти достаточно показательный пример в истории нашей цивилизации, а именно противостояние католиков и протестантов. Католическое общество можно рассматривать как корпоративную систему, обладающую определёнными характеристиками, набором индивидуумов и процессами информационного обмена. Появление протестантства можно сравнить с внедрением вируса в систему через одного или несколько индивидуумов. Далее следуют инкубационный период и этап репродуцирования. Во время этих периодов всё большее количество индивидуумов заражаются. В нашем случае – принимают иную веру.

На этапе саморазмножения активизируется иммунная система, пытаясь сдержать рост заражённых индивидуумов. Корпорация пытается защитить свои объекты и ресурсы от поражения. В истории это выражалось в неприятии и отторжении новой идеи.

Одновременно с внедрением или после некоторого промежутка времени определенного числа внедренных копий и т. д. вирус приступает к выполнению специальных функций, именуемых еще логическими бомбами, которые вводятся в программное обеспечение и срабатывают только при выполнении определенных условий, например, по совокупности даты и времени, и частично или полностью выводят из строя компьютерную систему. В биологических системах это проявляется через симптомы болезни, в исторических процессах – через народные волнения и т.п.

На этапе проявления вируса система переходит на режим повышенного воспроизведения антител, за счёт чего пытается нейтрализовать инородные тела, фактически применяя естественный антивирус. Как пример, Варфоломеевская ночь. Подобный метод можно применить к различным историческим, биологическим и информационным процессам.

3. Формирование языковых и информационных связей

Язык всегда являлся важнейшим компонентом развития мировых цивилизаций. На планете насчитывается от 2500 до 7000 языков. Но эти цифры более, чем приблизительны, так как точное количество никому неизвестно из-за отсутствия единого подхода к выделению диалектов одного и того же языка и условности различий между разными языками. Точно так же нет единого подхода к классификации языков. Наиболее популярна генеалогическая классификация, основывающаяся на историческом родстве языков, которые возникли из одного источника – праязыка. Согласно этому подходу языки делятся на языковые семьи, которые, в свою очередь, подразделяются на группы близких друг другу языков.

Сегодня есть семь языков, являющиеся «мировыми языками». Это английский, испанский, арабский, русский, французский, немецкий, португальский. Каждый из этих языков распространён на территориях нескольких государств, что имеет свои исторические причины. В силу этих причин на этих языках говорит достаточно большое количество людей. Такие языки как китайский, хинди и урду тоже входят в число важнейших языков мира, но на международной арене менее популярны.

Носители одного языка стремятся образовывать корпорации. Это может быть, как и территориальное образование, так и информационное. Территориальная формация может находиться в пределах государства, где данный язык является национальным, так и в пределах другой страны. Яркий пример – китайские и арабские кварталы.

Информационная формация наибольшее значение приобрела сравнительно недавно, вследствие глобализации и повышения доступности информационных средств. В этих формация язык и информация являются средствами для установления связей между индивидуумами, посредством чего сохраняется уклад жизни и обычаи, т.е. принципы построения корпорации.

В современных обществах государство не фиксирует национальную принадлежность гражданина в документах, удостоверяющих его личность (например, в паспорте, который, впрочем, во многих странах не обязателен), и не спрашивает человека о его национальности (например, при переписях населения). В ряде полиэтничных стран (Финляндия, Бельгия, Швейцария, Австрия, Испания, Турция, Пакистан, Индия, Канада, Мексика, Гватемала) национально-языковая тема переписи ограничена вопросом о родном языке.

Родной язык относится к тем измерениям человека, которые не выбираются. Природа речевой деятельности человека двойственна: в ней есть и врожденное (генетическое) и приобретенное. Генетически в людях заложена способность в первые годы жизни усвоить язык, причем любой язык. Однако отнюдь не от генетики, а от социальных условий зависит то, какой именно этнический язык (белорусский, немецкий, армянский, эскимосский) усвоит ребенок. Во многих случаях первым языком человека оказывался язык не физических, а приемных родителей; вообще говоря, это язык того окружения, в котором ребенок жил первые годы жизни (например, киргизский или казахский языки тех семей и детских домов, которые в годы войны приняли осиротевших маленьких детей белорусских, украинских или русских родителей). Таким образом, овладение первым языком – это не «природный», а социально-психологический процесс.

В кругу названных измерений человека и социума особое место занимают три признака: язык, этничность (национальность) и конфессионально-вероисповедная принадлежность. Они взаимосвязаны, так что их иногда смешивают (особенно часто определяют этничность, опираясь на признак языка или конфессии). Эти измерения называют в числе главных факторов, создающих своеобразие культуры и ментальности народа, т.е. своеобразие его психического склада, мировосприятия, поведения.

Это один из основополагающих принципов корпорации. Принцип наследственности предполагает, что любой вливающийся в корпорацию индивидуум будет обладать языком и информацией, присущей данной корпорации. Этими инструменты он будет постигать в начале своей жизни и потом передавать по наследству. Если же индивидуум уже обладает информацией и языком другой корпорации, то он будет стремиться передать их корпорации. Однако здесь будет иметь место принцип оссимеляции. Т.е. в корпорации индивидуум приобретёт новые инструменты информационного обмена.

Заключение

Корпоративную систему можно рассматривать как систему различных субъектов, между которыми происходят постоянные взаимодействия по обмену формализованными данными, посредством языка и информации.

Различные по сложности и функциональным особенностям субъекты системы используют различные ресурсы, но некоторые ресурсы могут одновременно использоваться несколькими различными субъектами, в результате происходит борьба за ресурсы. Это фактор наличия конкурирующего взаимодействия между компонентами системы за контроль отдельных компонент над однородными общесистемными ресурсами. В

процессе развития информационных технологий это привело к обострению вопросов защиты и безопасности информации.

Жизненный цикл корпораций, возможно сравнить с развитием государства, ведь оно, собственно, и является корпорацией. Изучение исторических процессов может помочь более широко взглянуть на корпоративную теорию.

Литература

1. Осовецкий Л.Г., Немолочнов О.Ф., Твёрдый Л.В., Беляков Д.А. Основы корпоративной теории информации // СПб: СПбГУ ИТМО. – 2004. – 83 с.
2. Берзин Е.А. Оптимальное распределение ресурсов и теория игр // М.: Радио и связь. – 1983. – 216 с.
3. Буч Г., Рамбо Д., Джекобсон А. Язык UML. Руководство пользователя: Пер. с англ. – М.: ДМК. – 2000. – 275 с.
4. Шеннон К. Математическая теория связи // М.: ИИЛ. – 1963. – 207 с.

УКД 004.056

РАЗРАБОТКА МОДЕЛИ УГРОЗ ИБ СИСТЕМЫ ЭЛЕКТРОННЫХ РАСЧЕТОВ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ РФ

Ю.Б. Борисов

Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В работе представлена постановка задачи разработки модели угроз информационной безопасности системы электронных расчетов (СЭР) организаций Банковской системы Российской Федерации (БС РФ), обоснована ее высокая значимость и актуальность, обозначен подход к ее решению, базирующийся на линейке стандартов Банка России обеспечения информационной безопасностью СТО БР ИББС. На основе анализа угроз СЭР организаций Банковской системы Российской Федерации предложена последовательность разработки модели угроз.

Ключевые слова: система электронных расчетов, информационная безопасность, несанкционированный доступ, модель угроз

Введение

В последнее время высокую актуальность приобретают проблемы надежности и устойчивости функционирования автоматизированной банковской системы (АБС) и особенно проблема обеспечения безопасности циркулирующей в ней информации. Основными причинами нарушения информационной безопасности (ИБ), утраты, хищения или искажения данных, представляющих ценность для их владельца, являются воздействия в результате случайного или преднамеренного несанкционированного доступа (НСД) нарушителя или воздействие на нее различного рода угроз. Особенно широкий размах получили нарушения и преступления в системе электронных расчетов (СЭР), которая является неотъемлемой частью АБС.

Модели угроз и нарушителей (прогноз ИБ) должны быть основным инструментом менеджмента организации при развертывании, поддержании и совершенствовании системы обеспечения ИБ организации.

Модель угроз ИБ СЭР организаций БС РФ

Угрозы информационной безопасности для СЭР организаций БС РФ – это:

(a) нарушение доступности информации и предоставляемых сервисов;

(b) нарушение целостности информации (данных) и программного обеспечения, в том числе несанкционированное изменение состояние счета при совершении расчетных, учетных и кассовых операций;

(c) нарушение конфиденциальности (неправомерное использование) информации, в том числе за счет хищения отчуждаемых машинных носителей с несанкционированно копированной информацией. Нарушение конфиденциальности информации за счет нарушения работы криптографических средств не рассматривается, так как неразрушающее воздействие на такие средства требует профессионального образования (специализированных знаний) в области криптографии, которых нарушитель информационно-телекоммуникационной системы организаций БС РФ, не имеет, что обеспечивается кадровой политикой Банковских систем;

(d) нарушение регламентов технологических процессов совершения банковских операций [1].

Объектами защиты являются:

(1) бизнес-процессы;

(2) платежные и информационные технологические процессы;

(3) информационные активы, в т.ч. различные виды банковской информации

(платежной, финансово-аналитической, служебной, управляющей и пр.) на следующих фазах их жизненного цикла: генерация (создание), обработка, хранение, передача, уничтожение. При этом информация, содержащаяся в платежных и служебно-информационных сообщениях строгой отчетности, не относится к конфиденциальной.

(4) автоматизированные системы, включающие комплексы средств автоматизации и людей – сотрудников Банка России, обеспечивающие реализацию его функций, а также здания и сооружения, где размещены указанные системы.

Уровни информационной инфраструктуры, на которых возможна реализация угроз информационной безопасности в соответствии со стандартом СТО БР ИББС-1.0-2006 представлены в следующей иерархической последовательности:

(I) физический (линии связи, аппаратные средства и пр.);

(II) сетевой (сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);

(III) сетевые приложения и сервисы;

(IV) операционные системы;

(V) системы управления базами данных, хранилищ данных и т.п.;

(VI) банковские технологические процессы и приложения;

(VII) бизнес-процессы [2].

Перечень основных источников угроз для перечисленных объектов защиты имеет следующий вид:

(a) неблагоприятные события природного и техногенного характера;

(b) террористы, криминальные элементы;

(c) компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных кодов и атак;

(d) поставщики программно-технических средств, расходных материалов, услуг и т.п.;

(e) подрядчики, осуществляющие монтаж, пуско-наладочные работы оборудования и его ремонт;

(f) сотрудники БС РФ, являющиеся легальными участниками процессов в ИТС и действующие вне рамок предоставленных полномочий;

(g) сотрудники БС РФ, являющиеся легальными участниками процессов в ИТС и действующие в рамках предоставленных полномочий [3].

Перечень основных возможных уязвимостей для перечисленных объектов защиты можно сгруппировать следующим образом:

(a) потенциальная подверженность района размещения объекта БС РФ воздействию природных и техногенных катаклизмов;

(b) недостаточная отказоустойчивость и катастрофоустойчивость аппаратно-программных и технических комплексов;

(c) физические, моральные, психологические особенности сотрудников, создающие предпосылки террористического или криминального воздействия;

(d) недостатки в организации охраны и технической укрепленности объектов Банка России;

(e) восприимчивость программного обеспечения к вредоносным программным кодам (компьютерным вирусам и т.п.) и другим атакам;

(5) наличие уязвимостей (дыр) программного и аппаратного обеспечения, в том числе наличие в нем недекларированных возможностей;

(6) несоответствующая утвержденной документации настройка конфигурации программного и аппаратного обеспечения, в том числе средств и систем защиты информации, отсутствие контроля их изменения;

(7) некачественная (неполная) регламентация в договорах вопросов взаи-

модействия с поставщиками и подрядчиками (обязанности, ответственность);

(8) ориентация на монопольных поставщиков и подрядчиков;

(9) наличие уязвимостей (слабостей) в системе защиты информации;

(10) несоответствие регламентов деятельности текущему состоянию объекта защиты и неконтролируемость исполнения сотрудниками БС РФ регламентов своей деятельности [4].

Учитывая во внимание выше описанные угрозы информационной безопасности, уровни информационной инфраструктуры, на которых возможна реализация угроз, объекты защиты, а так же перечни основных источников угроз и основных возможных уязвимостей для перечисленных объектов защиты и руководствуясь выполнением требований Стандарта Банка России СТО БР ИББС-1.0-2006 можно представить в виде следующей наглядной таблицы:

№ п./п.	**Основные источники угроз**	**Угроза**	**Уровень реализации угрозы**	**Уязвимость**	**Основные последствия для Банка России и его клиентов и корреспондентов**
1	**2**	**3**	**4**	**5**	**6**
1	Неблагоприятные события природного и техногенного характера	Нарушение доступности, целостности	Физический уровень	Потенциальная подверженность района размещения объектов БС РФ воздействию природных и техногенных катаклизмов	Выход из строя информационно-телекоммуникационной системы, потеря управления, прекращение (отказ) обслуживания, утеря (уничтожение) данных в следствии физического разрушения (порчи) носителей информации
				Недостаточная отказоустойчивость и катастрофоустойчивость аппаратно-программных и технических комплексов	
2	террористы, криминальные элементы	Нарушение доступности, целостности, конфиденциальности	Физический уровень	Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия	Выход из строя информационно-телекоммуникационной системы, потеря управления, прекращение (отказ) обслуживания, утеря (уничтожение) данных в следствии физического разрушения (порчи) носителей информации
		Нарушение доступности, целостности,		Недостатки в организации охраны и технической укрепленности объектов БС РФ	

№ п./п.	Основные источники угроз	Угроза	Уровень реализации угрозы	Уязвимость	Основные последствия для Банка России и его клиентов и корреспондентов
		Нарушение доступности, целостности, конфиденциальности	Сетевой уровень	Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия	Реализация атак (нерегламентированное использование инструментов позволяющих реализовать атаки) на информационно-телекоммуникационные системы Банка России приводящие к прекращению (отказу) обслуживания, модификации настроек сетевого оборудования, неправомерному доступу к оборудованию (сегментам сети)
		Нарушение доступности, целостности, конфиденциальности	Уровень сетевых приложений и сервисов	Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия	Реализация атак (нерегламентированное использование инструментов позволяющих реализовать атаки) на информационно-телекоммуникационные системы Банка России приводящие к прекращению (отказу) обслуживания отдельных сервисов, изменение (модификация) сетевого трафика, перехват информации
		Нарушение доступности, целостности, конфиденциальности	Уровень операционных систем	Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия	Внедрение вредоносного программного кода позволяющего захватить управление операционными системами с целью прекращения (отказа) обслуживания отдельных хостов (групп хостов), изменение (модификация) программного окружения, перехват конфиденциальной информации
		Нарушение доступности, целостности, конфиденциальности	Уровень систем управления базами данных	Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия	Реализация атак (нерегламентированное использование инструментов позволяющих реализовать атаки), внедрение вредоносного программного кода позволяющего захватить управление СУБД с целью прекращения (отказа) обслуживания, модификации информации

№ п./п.	Основные источники угроз	Угроза	Уровень реализации угрозы	Уязвимость	Основные последствия для Банка России и его клиентов и корреспондентов
		Нарушение доступности, целостности, конфиденциальности	Уровень банковских технологических процессов и приложений	Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия	Нарушение непрерывности и правильности функционирования бизнес-процессов Внедрение фиктивных (подложных) платежных документов Угроза деловой репутации
		Нарушение доступности, целостности, конфиденциальности	Уровень бизнес-процессов	Физические, моральные, психологические особенности сотрудников, их незащищенность, создающие предпосылки террористического или криминального воздействия	Нарушение непрерывности и правильности функционирования бизнес-процессов Внедрение фиктивных (подложных) платежных документов Угроза деловой репутации
…	…	…	…	…	…

Таблица. Модель угроз

Заключение

В рамках работы, описанной в данной статье, были решены следующие задачи:

(1) определено понятие угроз информационной безопасности для системы электронных расчетов организаций БС РФ;

(2) определены уровни информационной инфраструктуры, на которых возможна реализация угроз информационной безопасности;

(3) перечислены объекты защиты;

(4) приведен перечень основных источников угроз для перечисленных объектов защиты;

(5) приведен перечень основных возможных уязвимостей для перечисленных объектов защиты;

(6) В соответствии с требованиями Стандарта Банка России СТО БР ИББС-1.0-2006 разработана наглядная модель угроз информационной безопасности системы электронных расчетов организаций Банковской системы Российской Федерации.

Следующим этапом для обеспечения информационной безопасности системы электронных расчетов организаций БС РФ является разработка модели нарушителей информационной безопасности, которая с моделью угроз должна лечь в основу разработки политики ИБ организаций БС РФ.

Литература

1. Староверов Д. Черты характера и стереотипы поведения сотрудника, работающего на конкурента. // Конфидент. Защита информации. – 1999. – № 4–5. – С. 57–62.
2. «Стандарт Банка России. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения СТО БР ИББС-1.0-2006», от 26.01.2006г. – № Р-27.
3. Стрельченко Ю. Информационная безопасность банка. // Банковский журнал. – 2005. – № 1. – С. 37–44.
4. Вихорев С.В., Герасименко В.Г. Борьба с преступлениями в банковских информационно-вычислительных системах. // Системы безопасности связи и телекоммуникаций. – 2007. – ноябрь–декабрь. – С. 54–59.

УДК 681.3.06

КОНТРОЛЬ УЯЗВИМОСТЕЙ В ПРОГРАММАХ С ИСХОДНЫМИ ТЕКСТАМИ (АНАЛИЗ SQC-ФАЙЛОВ)

В.Л. Верещагин
Научный руководитель – д.т.н., профессор А.А. Молдовян

В статье рассматривается способ анализа файлов, которые в процессе компиляции и сборки проекта модифицируются из специального текстового вида в конструкции, соответствующие правилам языка Си. Сформированный в результате файл компилируется и удаляется в случае успешной сборки исполняемого файла. Автор рассматривает такую технологию как потенциальную возможность реализации программной закладки и предлагает подход, позволяющий провести полный статический и динамический анализы.

Ключевые слова: SQL-препроцессор, SQC-файлы, уязвимость, анализ программ, исходные тексты, программная закладка, статический анализ, контроль избыточности

Введение

Вопрос, который поднимается в данной статье, исторически связан с сертификаций программного обеспечения. Несколько лет назад команда исследователей одной из лабораторий министерства обороны испытывала программно-аппаратный комплекс связи, в состав которого входило большое число различных типов исходных файлов. Среди прочих были файлы с непривычным расширением «sqc». В целом название указывало на некоторую связь с языком запросов SQL, но в действительности под этим могло скрываться все что угодно, в том числе и программная закладка.

Одной из первых проверок является «контроль избыточности». Суть её, как видно из названия, заключается в том, чтобы найти те файлы, которые не составляют конечный исполняемый файл, а, следовательно, и не должны подергаться дальнейшим испытаниям. Отступая от главной темы, можно отметить, что часто этой проверке придают излишне строгий смысл: большое число специалистов считают, что такие файлы могут содержать программные закладки и поэтому их необходимо удалить. Но при более детальном рассмотрении оказывается, что удаление такой избыточности не несет никакого функционального значения: если они действительно избыточные, то они и не попадут в исполняемый файл, а если были признаны таковыми ошибочно, то их удаление приведет к ошибкам компиляции. Еще один вариант – это когда файл не компилируется, но используется, допустим, как конфигурационный, или даже дополнительный, откуда считывается специальная строка, активизирующая программную закладку. Взять и удалить его – означает обречь программу на какие-то действия, которые в лучшем случае незаметно пройдут, а в худшем вызовет сбой, чего допускать совсем нежелательно. Такие ошибки необходимо уметь определять на стадии дальнейшего анализа и поэтому удаление избыточности - дело неблагодарное и опасное.

Возвращаясь, к основной теме статьи, приведу пример, когда файлы были определены как подлежащие дальнейшему анализу, а в действительности оказались избыточными. Как уже было сказано выше, в проекте программно-аппаратного комплекса связи наблюдались файлы с расширением «sqc». В них, как и во все остальные файлы, был вставлен уникальный датчик, помогающий определить попадает ли тот или иной исходный файл в исполняемый код. Подробно методика рассматривается в статье [1], здесь же имеет смысл привести её суть: во все файлы проекта вставляются уникальный датчик, который жестко привязан к конкретному файлу. В двух разных файлах вставляются два разных датчика. Специальной поисковой утилитой, в бинарном файле обнаруживаются такой датчик, и это отмечается в базе данных. В ином случае файлы помечаются как избыточные.

Модель обнаружения избыточности настолько проста, что обязательно должны были найтись исключения. К ним целесообразно отнести и данный случай: файлы «sqc» в результате такой проверки были признаны анализатором, как используемые, но в действительности они таковыми не являлись. Оказалось, что данные файлы используются как промежуточные и содержат команды SQL-препроцессора, который не поддерживается стандартом языка Си. Принцип работы с ними как раз и сводится к преобразованию в Си-текст и только после этого компилируется. Интересным еще оказался и тот факт, что в каталоге с исходными файлами присутствовали только sqc-файлы, но не было даже следа от Си-файлов, в которые они должны были быть преобразованы – их разработчики автоматически удаляли после того как компиляция завершалась.

Таким образом, перед исследователями возник интересный пример «призрачного» исходного файла, который вроде и есть, но проконтролировать его существование невозможно так как он живет только в течение процесса компиляции – 5–10 минут.

Описание такой ситуации в научных статьях можно найти только косвенное, например, когда пишут о намеренной модификации файла в процессе компиляции или же по вопросам работы с базой данных. Поэтому решение было необходимо находить исходя из имеющихся данных.

Постановка задачи

К исходным данным целесообразно отнести следующее. Имеется проект для некоего программно-аппаратного комплекса, подлежащего проверке. В состав исходных файлов входят тексты, написанные на языке Си, и вдобавок имеются тексты, содержащие SQL-директивы, обрабатываемые с помощью специального препроцессора. Последовательность компиляции и сборки содержится в make-файлах, где в частности определена схема обработки sqc-файлов (см. рис. 1).

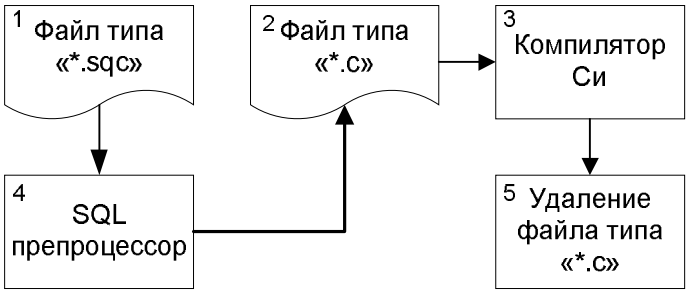


Рис. 1. Последовательность обработки файла типа «sqc»

Файл с расширение «sqc» (см. №1 на рис. 1) обрабатывается с помощью утилиты «sqlpp» (см. №4 на рис. 1) и приводится (транслируется) к виду, понятному для Си-компилятора. Полученный файл компилируется и собирается в исполняемый код.

Задача ставится следующим образом: необходимо определить избыточность файлов и подготовить их к статическому анализу.

Особенностью выполнения является невозможность выполнить статический анализ над sqc-файлами т.к. они не содержат достаточной информации о функциях, переменных и линейных участках. Все эти сведения появляются после того, как файл будет транслирован при помощи SQL-препроцессора. Поэтому целесообразно уточнить задачу: изменить проект таким образом, чтобы вместо sqc-файлов использовались полноценные файлы «*.c».

Другой особенностью является замена проверяемых файлов в процессе статического анализа. Более подробно о статическом анализе написано в статье [2], здесь же можно привести краткое замечание, касающееся особенности его реализации. После

выделения используемых файлов и анализа, реализованных в них языковых конструкций, выполняется вставка специальных датчиков, которые принципиально отличаются от рассмотренных выше. Датчики вставляются в каждый линейный участок программы и сигнализируют об их срабатывании. Когда все датчики вставлены в исходные тексты, необходимо собрать такую измененную версию программы, которую часто называют лабораторной версией. В большинстве случаев достаточно записать исходные файлы в каталог, откуда они попадают на вход компилятора, но если есть такие файлы как «sqc», то может произойти перезапись лабораторных Си-файлов новыми, созданными на этапе препроцессирования. Такое положение дел негативно отразится на результатах анализа и приведет к ошибочным выводам.

Методы исследований

Для того чтобы решить поставленную задачу необходимо произвести предварительную подготовку make-файлов. Во-первых, требуется избавиться от команд удаления Си-файлов, выполняемых после успешной компиляции. Во-вторых, внести такие изменения, чтобы файл был транслирован только один раз, а последующие компиляция производилась только с Си-файлами. Для этих целей удаляются соответствующие строчки из make-файлов и формируется база данных анализатора. В ней необходимо отразить то, чего нет в исходном наборе – файлы, полученные из «sqc» в результате трансляции, иначе анализатор будет «ошибаться», вставляя датчики и собирая сведения о функциональных объектах. Ниже представлена последовательность выполнения этих изменений.

Говоря об анализаторе, стоит сказать несколько слов об особенностях его работы. Как сказано в статье [2] , анализ программы выполняется в несколько этапов (см. рис. 2).

Исходные тексты, составляющие проект программного комплекса (см. №5 на рис. 2), учитываются анализатором (см. №1 на рис. 2) в базе данных (см. №2 на рис. 2) для дальнейшего ведения учета. В базе данных (БД) формируется таблица, предусматривающая поля для сведений об уникальном номере, имени, типе файла, а также о его длине, избыточности и некоторой другой служебной информации. Более подробную структуру БД можно найти в статье [2]. Именно на этом шаге важно учесть, чтобы в БД попали не только sqc-файлы, но и их Си-аналоги. Т.е проект программного комплекса должен включать и те и другие файлы. Для этого необходимо выполнить компиляцию проекта, предварительно проанализировав make-файлы и закомментировав из них команды удаления полученных Си-файлов. Необходимость учитывать сами sqc-файлы вытекает из требований к испытаниям – БД должна отражать действительное положение дел, т.к на основании её будут сформированы отчеты, содержащие контрольные суммы для всех файлов проекта. Если перед занесением в БД удалить sqc-файлы и оставить только их Си-аналоги, то произойдет несогласование между исходным комплектом файлов и полученным в процессе работы.

Таким образом, полный пакет исходных текстов будет получен только после первой компиляции, что весьма необычно.

Вставка датчиков (см. №4 на рис. 2), выполняемая с целью контроля избыточности осуществляется во все файлы, которые были учтены в БД. Соответственно, если в проекте имеются 2 файла, например, «A.sqc» и «A.c», то в оба будут вставлено по уникальному датчику. Наиболее логично было бы предположить, что оба эти файла должны быть отмечены как используемые. Но вот что в этом случае получится: анализатор, работающий по очень простой логике, выбирает для дальнейшего анализа только те файлы, которые помечены, как используемые. Анализ предполагает лексический и синтаксический разборы с последующим семантическим соотнесением найденных конст-

рукций с конструкциями грамматики языка Си. Если отметить, как «используемые» sqc-файлы, то проанализировать их не представится возможным, т.к. для успешного завершения этого процесса придется еще, как минимум, написать грамматику SQL-препроцессора. Если же отметить только их Си-аналоги, то при формировании отчета, окажется, что все sqc-файлы являются избыточными и их будет необходимо удалить из проекта, что приведет к ошибкам компиляции т.к. в исходном наборе файлов имеются только «sqc» и нет их Си-аналогов.

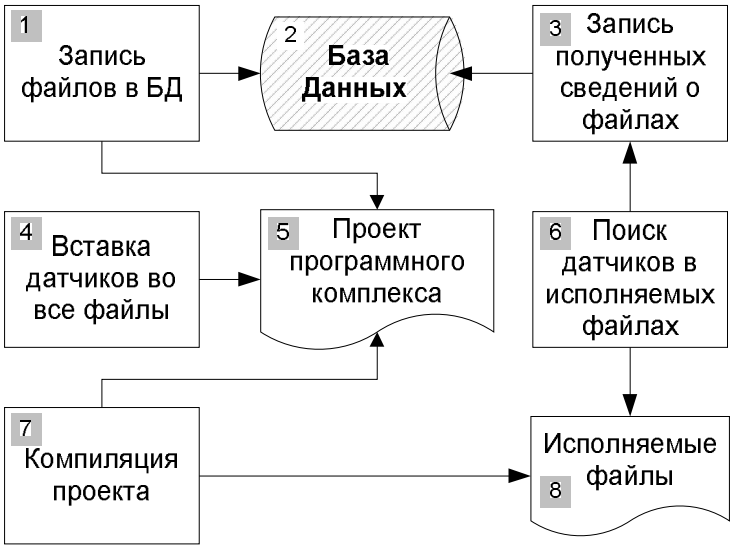


Рис. 2. Общая схема обработки исходных текстов на ранних этапах анализа

В качестве решения предлагается гибкое управление флагом избыточности в БД. На этапе выделения группы файлов для статического анализа необходимо признать Си-файлы «используемыми», а «sqc» – избыточными. На другом этапе – создания отчетов – наоборот.

Общая последовательность действий можно представить в виде следующего алгоритма:

(1) Получение исходных текстов проекта (всех файлов, которые необходимы для успешной компиляции и сборки);
(2) Внесение изменений в make-файлы: комментирование строк с командами удаления Си-файлов, полученных из sqc-файлов.
(3) Компиляция и сборка проекта: получение полной версии исходных файлов.
(4) Создание копии полученной версии файлов с целью возможности обновления лабораторных версий. Это бывает необходимо для получения каких-либо промежуточных данных, например, файлы меняются несколько раз за исследование: один раз в них вставляются датчики контроля избыточности, в другой вставляются другие датчики, контролирующие выполнение линейных участков. И важно, чтобы эти оба варианта датчиков не находились в одном файле. Для этого производится полная замена файлов из сохраненной копии.
(5) Регистрация всех файлов проекта в БД;
(6) Вставка датчиков в зарегистрированные файлы.
(7) Компиляция и сборка проекта: получение исполняемых файлов с датчиками, контролирующими избыточность. В качестве промежуточных результатов получим, что информацию об используемых sqc-файлах. Ведь вполне может оказаться, что часть из них избыточна.
(8) Проведение анализа избыточности файлов. Запись сведений в БД.

(9) Внесение изменений в make-файлы: комментирование строк с командами трансляции sqc-файлов. Если есть избыточные среди sqc-файлов, то это необходимо учесть: закомментировать соответствующие команды компиляции и сборки Си-файлов.
(10) Замена файлов лабораторной версии оригинальными. Это необходимо для того, чтобы можно было вставить датчики контроля избыточности вторично. Теперь необходимо контролировать не столько sqc, сколько полученные из них Си-файлы.
(11) Повторная вставка датчиков во все зарегистрированные файлы.
(12) Компиляция и сборка проекта: получение исполняемых файлов.
(13) Проведение анализа избыточности файлов. Запись сведений в БД. В результате будет получен тот набор файлов, которые можно анализировать по правилам языка Си.
(14) После того, как будет завершен статический анализ создать копию БД и инвертировать флаг избыточности у sqc и соответствующих им Си-файлов. Это позволит сформировать отчет, где будет указано, что sqc-файлы были использованы при компиляции, а Си-файлы учитываться не будут.
(15) Выполнить контрольную проверку: удалить все избыточные файлы, относящиеся к исходным текстам (кроме них существуют еще конфигурационные, объектные, файлы проекта и т.п.) и произвести сборку проекта. Если проект собрался без замечаний, то считаем контроль выполненным верно. В ином случае необходимо определить причину и выполнить коррективу.
(16) Создать отчет об избыточности файлов.

Результаты исследований

Исследования показали, что sqc-файлы, являясь малозаметным компонентом системы и теоретически могут скрывать в своем составе недокументированные возможности. Описанная методика была опробована на нескольких десятках файлов, в различных проектах, работающих под операционной системой реального времени QNX 4.25. На основе полученных результатов были успешно проведены контроль избыточности во всех проектах и сформированы корректные списки файлов, подлежащих статическому и динамическому анализам. К другим результатам исследования стоит отнести невозможность автоматического разбора sqc-файлов без соответствующих на языке Си. Это связано с тем, что даже при наличии грамматики SQL-препроцессора невозможно предугадать каким образом будет сформирован конечный Си-файл т.к. могут различаться версии транслирующих программ. В любом случае необходимо выполнять трансляцию средствами, предоставляемыми разработчиком. В качестве варианта возможно развития следует рассматривать полную автоматизацию процесса обработки сведений в БД, файлов проекта и выдачи результатов.

Заключение

Приведенная выше методика была успешно опробована на 3-х проектах общей численностью исходных текстов более 10 000 шт., из которых объем sqc-файлов составлял 1%. В результате был осуществлен полноценный контроль «невидимых» Си-файлов. К недостаткам метода следует отнести неполную автоматизацию процесса, которая могла быть оправдана небольшим объемом исследуемых файлов. Другим недостатком является большое количество итераций, которые приходится выполнить в процессе получения исходных текстов. К достоинствам следует отнести простоту, эффек-

тивность и структурированность метода, возможность достаточно быстро автоматизировать процесс анализа.

Литература

1. Котенко Д.А. Контроль избыточности исходных файлов программ на основе вставки программных датчиков. V Санкт-Петербургская Межрегиональная конференция «Информационная безопасность регионов России (ИБРР-2007)», Санкт-Петербург, 23–25 октября 2007 г.: Материалы конференции – СПб: СПОИСУ. – 2007. – 153 с.
2. Арефьев Д.Б., Верещагин В.Л., Галанов А.И. Метод разбора исходных текстов по упрощенной грамматике языка. Сборник тезисов V Всероссийской межвузовской конференции молодых ученых. – СПб: СПбГУ ИТМО. – 2008. – 330 с.
3. Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» по 3 уровню контроля, Гостехкомиссия России (в настоящее время ФСТЭК). – Москва. – 1999.

УДК 004.056

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ БАНКОВСКОЙ СИСТЕМЫ

Е.О. Калашник
Научный руководитель – к.т.н., доцент А.В. Любимов

Статья посвящена объектно-процессному моделированию стандарта ЦБ по информационной безопасности СТО БР ИББС-1.0-2008, дата ввода которого планируется 2009-05-01.
Ключевые слова: модель, сертификация, банковская система, информационная безопасность

Введение

Банковская система (БС) Российской Федерации (РФ) включает в себя Банк России, кредитные организации, а также филиалы и представительства иностранных банков [1]. Развитие и укрепление БС РФ, а также обеспечение эффективного и бесперебойного функционирования платежной системы РФ являются целями деятельности Банка России [2]. Важнейшим условием реализации этих целей является обеспечение необходимого и достаточного уровня информационной безопасности (ИБ) организаций БС РФ, их активов (в т.ч. информационных), который во многом определяется уровнем ИБ банковских технологических процессов (платежных, информационных и пр.), автоматизированных банковских систем, эксплуатирующихся организациями БС РФ.

Особенности БС РФ таковы, что негативные последствия сбоев в работе отдельных организаций могут привести к быстрому развитию системного кризиса платежной системы РФ, нанести ущерб интересам собственников и клиентов. В случаях наступления инцидентов ИБ значительно возрастают результирующий риск и возможность нанесения ущерба организациям БС РФ. Поэтому для организаций БС РФ угрозы ИБ представляют существенную опасность.

Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов ИБ (их влияния на операционный, репутационный, стратегический и иные риски) в организациях БС РФ следует обеспечить достаточный уровень ИБ. Необходимо также сохранить этот уровень в течение длительного времени. По этим причинам обеспечение ИБ является для организаций БС РФ одним из основополагающих аспектов их деятельности.

Деятельность, относящаяся к обеспечению ИБ, должна контролироваться. В связи с этим, Банк России является сторонником регулярной оценки уровня ИБ в организациях БС РФ, оценки риска нарушения ИБ и принятия мер, необходимых для управления этим риском.

Исходя из этого, разработан настоящий стандарт по обеспечению ИБ организаций БС РФ, который является базовым для развивающей и обеспечивающей его группы документов в области стандартизации, в целом составляющих комплекс документов в области стандартизации по обеспечению ИБ организаций БС РФ [3].

Основные цели стандартизации по обеспечению ИБ организаций БС РФ:

- развитие и укрепление БС РФ;
- повышение доверия к БС РФ;
- поддержание стабильности организаций БС РФ и на этой основе – стабильности БС РФ в целом;
- достижение адекватности мер защиты реальным угрозам ИБ;
- предотвращение и (или) снижение ущерба от инцидентов ИБ.

Основные задачи стандартизации по обеспечению ИБ организаций БС РФ:

- установление единых требований по обеспечению ИБ организаций БС РФ;
- повышение эффективности мероприятий по обеспечению и поддержанию ИБ организаций БС РФ.

Метод и инструментарий

В качестве метода и инструментария была выбрана методология объектного моделирования UML.

Ее преимущества:

- возможность построения иерархических информационных моделей;
- простота модификации (благодаря использованию парадигмы наследования).

Ее недостатки:

- сложность синтаксиса (оборотная сторона богатства примитивов);
- сложность верификации (в значительной степени – благодаря сложности синтаксиса, но также и вследствие богатства семантики).

В качестве инструментального средства моделирования выбран продукт Enterprise Architect компании Sprax Systems.

Контекст модели и нотация

Основа объектного моделирования – это преобразование базового словаря и простейших отношений концептов в полную объектную модель методологии, включение в объектную модель процессной составляющей, согласование статической и динамической компонент синтетической модели.

Основное назначение моделей объектного уровня: межметодологическое согласование стандартов; проектирование (создание внутренних проектных спецификаций) и разработка программного обеспечения (ПО) поддержки деятельности в предметной области; создание концептуальных моделей как основы для построения начальных онтологий.

Под согласованием понимается целенаправленная модификация двух или более моделей, где в качестве целей могут выступать: взаимное дополнение (расширение), гармонизация (унификация), обобщение (универсализация) и пр. При этом согласование может быть как межуровневым, которое представляет наибольший научный интерес, так и межметодологическим, которое представляет наибольший практический интерес.

Свойства модели

Определение модели

Модель содержит структурированное по UML вербально-графическое представление системы процессов оценивания безопасности информационных технологий по стандарту СТО БР ИББС-1.0-2008

Цели моделирования

Основная цель моделирования – представление для целевой аудитории базовой системы объектов и процессов стандарта в максимально компактной, наглядной и формализованной форме, допускающей как дальнейшую детализацию, так и коррекцию в соответствии с последующими версиями стандарта. Модель также может использоваться как базовая часть функциональных спецификаций для инструментального программного обеспечения поддержки процессов оценивания.

В состав целевой аудитории входят: оценщики систем ИТ, разработчики, поставщики и пользователи систем ИТ; проектировщики программного обеспечения поддержки процесса оценивания.

Точка зрения моделирования

Моделирование проводится с точки зрения оценщика безопасности информационных технологий. Эта роль является ключевой в процессе оценки, и ее использование позволяет построить наиболее универсальную объектную модель.

Описание модели и границы моделирования

Модель содержит подробное описание концептуальной схемы (парадигмы) обеспечения информационной безопасности организаций БС РФ. В основе исходной концептуальной схемы ИБ организаций БС РФ лежит противоборство собственника и злоумышленника с целью получения контроля над информационными активами. Однако другие, незлоумышленные действия или источники угроз, также лежат в сфере рассмотрения настоящего стандарта.

Если злоумышленнику удается установить такой контроль, то как самой организации БС РФ, так и клиентам, которые доверили ей свои собственные активы, наносится ущерб.

Организация БС РФ осуществляет свою деятельность путем реализации совокупности процессов, среди которых возможно выделение следующих групп:

-основные процессы, обеспечивающие достижение целей и задач организации БСРФ;

-вспомогательные процессы, обеспечивающие качество, в том числе, обеспечение ИБ организации БС РФ;

-процессы менеджмента (управления), обеспечивающие поддержку параметров основных и вспомогательных процессов в заданных пределах и их корректировку в случае изменения внешних или внутренних условий.

Совокупность защитных мер, реализующих обеспечение ИБ организации БС РФ, и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение, составляет систему ИБ (СИБ) организации БС РФ.

Совокупность процессов менеджмента ИБ, включая ресурсное и административное (организационное) обеспечение этих процессов, составляет систему менеджмента ИБ (СМИБ) организации БС РФ.

Совокупность СИБ и СМИБ составляет систему обеспечения ИБ (СОИБ) организации БС РФ.

Группы процессов СМИБ организации БС РФ организуются в виде циклической модели Деминга «… – планирование – реализация – проверка – совершенствование – планирование –…», которая является основой модели менеджмента стандартов качества ГОСТ Р ИСО 9001 и ИБ ISO/IEC IS 27001-2005 [4]. Организация и выполнение процессов СМИБ необходимы, в том числе, для обеспечения уверенности в том, что хороший практический опыт организации БС РФ документируется, становится обязательным к применению, а СОИБ совершенствуется.

Выводы

Необходимо понимать, что если процесс сертификации одного банка может и не занимать длительного времени, то процесс подготовки к сертификации может потребовать значительных ресурсов и времени, в зависимости от степени зрелости системы управления ИБ банка. Поэтому, как говорят, «готовь сани летом», и о процессе подготовки к сертификации стоит задуматься уже сейчас. В любом случае, начинать эту ра-

боту необходимо с анализа стандарта, обследования и аудита ИБ. При этом экспертная оценка, а заодно и рекомендации по возможному улучшению системы управления ИБ будут полезными как для существующей системы управления ИБ банка, так и для системы менеджмента в целом.

Литература

1. Федеральный Закон «О банках и банковской деятельности» от 01.12.1990 № 395-1 в ред. ФЗ от 03.02.1996 №17-ФЗ, от 31.07.1998 № 151-ФЗ, от 05.07.1999 № 126-ФЗ, от 08.07.1999 № 136-ФЗ, от 19.06.2001 № 82-ФЗ, от 07.08.2001 № 121-ФЗ, от 21.03.2002 № 31-ФЗ, с изм., внесенными постановлением Конституционного Суда РФ от 23.02.1999 № 4-П.
2. Федеральный Закон «О Центральном Банке Российской Федерации (Банке России)» от 10 июля 2002 года № 86-ФЗ.
3. СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положение».
4. ISO/IEC IS 27001-2005 Information technology. Security techniques. Information security management systems. Requirements.

УКД 004.056

МЕТОДЫ И СРЕДСТВА ВЫЯВЛЕНИЯ НЕДЕКЛАРИРОВАННЫХ ВОЗМОЖНОСТЕЙ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ, АЛЬТЕРНАТИВНЫЙ ПОДХОД

А.Ю. Потехонченко, Н.Н. Дацун
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В современном мире достижение эффективности и экономической выгодности в различных сферах деятельности невозможно без правовой регламентации процессов, составляющих эту деятельность, и обязанностей субъектов, в ней задействованных. Особенную актуальность правила, регламенты и стандарты приобретают в областях, связанных с риском нанесения того или иного ущерба. Одной из таких областей, имеющих в настоящее время важнейшее значение, является информационная безопасность. Данная статья описывает один из подходов к сертификации основанный на нормативной, и инструментально-технической базе выявления недекларированных возможностей.

Ключевые слова: недекларированные возможности, открытый перечень требований

Введение

Предлагаемый подход позволит усовершенствовать существующую нормативную, а так же инструментально-техническую базу выявления недекларированных возможностей (НДВ) [1]. Недекларированные возможности – функциональные возможности программного обеспечения (ПО), не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Открытый перечень требований

За основу открытого перечня требований (ОПТ) взяты такие специальные нормативные документы как:

- РД СВТ, защита от НСД;
- РД АС, защита от НСД;
- Концепция защиты информации СВТ и АС от НСД;
- РД НДВ;
- РД по «Межсетевым экранам»;
- «Общие критерии».

В связи с тем, что ОПТ представляет собой совокупность организационных мер и расширенных требований к ПО на наличие НДВ, мною был произведен анализ приведенной выше нормативно-методической литературы и на основе этого анализа была построена методика проверки ПО на наличие НДВ [8].

Проверка ПО на наличие НДВ предполагает проведение следующих видов испытаний:

- контроль состава и содержания документации;
- контроль исходного состояния ПО;
- статический анализ исходных текстов программ;
- динамический анализ исходных текстов программ.

Каждый из перечисленных видов испытаний ПО характеризуется определенной совокупностью технологических операций.

Документация ПО должна содержать следующие разделы:

- общие сведения;
- функциональное назначение;

- описание логической структуры;
- используемые технические средства;
- вызов и загрузка;
- входные данные;
- выходные данные.

При контроле исходного состояния ПО производится фиксация исходного состояния ПО и сравнение полученных результатов с приведенными в документации.

Производя статический анализ исходных текстов ПО производятся следующие технологические операции:

- контроль соответствия исходных текстов программного обеспечения по его объектному (загрузочному) коду;
- контроль полноты и отсутствия избыточности исходных текстов ПО на уровне файлов;
- контроль полноты и отсутствия избыточности исходных текстов ПО на уровне функциональных объектов (процедур);
- контроль связей функциональных объектов (модулей, процедур, функций) по управлению;
- контроль связей функциональных объектов (модулей, процедур, функций) по информации;
- контроль информационных объектов различных типов (например, локальных переменных, глобальных переменных, внешних переменных и т.п);
- синтаксический контроль наличия заданных конструкций в исходных текстах ПО из списка (базы) потенциально опасных программных конструкций;
- построение по исходным текстам контролируемого ПО блок-схем, диаграмм и т.п., и последующий сравнительный анализ алгоритма работы функциональных объектов (процедур, функций) и алгоритма работы, приведенного в документации;
- формирование перечня маршрутов выполнения функциональных объектов (процедур, функций);
- анализ критических маршрутов выполнения функциональных объектов (процедур, функций) для заданных экспертом списков информационных объектов.

Производя динамический анализ исходных текстов ПО производятся следующие технологические операции:

- контроль выполнения функциональных объектов (процедур, функций);
- сопоставление фактических маршрутов выполнения функциональных объектов (процедур, функций) и маршрутов, построенных в процессе проведения статического анализа.

Достижение наилучших результатов в проверке ПО на наличие НДВ возможно только в комплексе проверочных мероприятий. Причем работа по проверке должна производится на таких этапах как:

- реализация проекта ПО;
- выпуск ПО на рынок;
- предсертификационные испытания ПО.

Для этапов «Реализация проекта ПО» и «Выпуск ПО на рынок» построены предполагаемые модели угроз и модели нарушителей. Накладывая ту или иную предполагаемую модель на конкретное ПО, можно оценить и выявить расхождения и узкие места проверяемого ПО.

За счет данного способа проверки выделятся три метода самопроверок такие как:

- самостоятельная самопроверка;
- самопроверка сторонней организацией;
- смешенная самопроверка.

На основе проведенных самопроверок возможна более качественная оценка по степеням доверия к тому или иному методу.

Заключение

Применение разрабатываемого перечня, видится достаточно обширным. Это может быть как сектор по созданию ПО для выявления НДВ в ПО, так и сектор, потребляющий ПО для выявления НДВ. Каждый представитель обоих секторов будет иметь возможность провести проверку в соответствии со своими узконаправленными требованиями, и в тоже время в соответствии с нормативной базой. Это в свою очередь позволит обеспечить многогранность проверки, и тем самым повысить надежность проверяемого ПО. В свою очередь, повышая качественные показатели, можно уменьшить трудозатраты на производство ПО. Если говорить простым языком, то любой программный продукт делится на отдельные сегменты, и если за основные составляющие принимать уже проверенные части. То тем самым мы снижаем, ни только временные показатели на производство, но и повышаем надежность производимого продукта.

Литература

1. РД НСД.
2. РД СВТ, защита от НСД.
3. РД АС, защита от НСД.
4. Концепция защиты информации СВТ и АС от НСД.
5. РД по «Межсетевым экранам».
6. ГОСТ Р ИСО/МЭК 15408-2002 «Общие критерии оценки безопасности информационных технологий».
7. Компаниец Р.И., Ковалев В.В., Маньков Е.В. Экспертиза и защита кода программ на основе автоматов динамического контроля// Защита информации. Инсайд. – 2007. – № 3.
8. Марков А., Никулин М., Цирлов В. Сертификация средств защиты персональных данных: революция или эволюция// Защита информации. Инсайд. – 2008. – № 5.
9. Темнов О.Д. Анализ и исследование методов средств обнаружения недекларированных возможностей//Научно-технический вестник СПбГУ ИТМО. – 2008. – №39. С. 45–50.

УДК 004.056.57

МОДЕЛЬ ОЦЕНКИ УРОВНЯ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ В ОБЩЕМ ПОЛЕ УГРОЗ

А.В. Разумовский
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В настоящее время активно развиваются различные стандарты по обеспечению информационной безопасности. Они описывают формальные критерии, достигая которых можно полагать на определенный момент что был достигнут некий приемлемый уровень безопасности. Но в современном мире всегда необходимо иметь возможность сравнить уровень безопасности организации с другими, оценить уровень безопасности организации по отношению к другим. Также необходимо иметь возможность узнать, как влияет изменение отдельных элементов на общий уровень безопасности.

Ключевые слова: информационная безопасность, модель, оценка

Введение

Для создания такой модели необходимо использование биологических моделей эволюции. Ведь по сути, предприятие должно постоянно развиваться чтобы оставаться по карйней мере на одном уровне безопасности, так как безопасность это процесс, а не состояние. В современном быстроменяющемся мире угроз это является актуальной и трудной задачей. Для упрощения задачи будет использоваться биологическая модель эволюции, только вместо живого организма у нас будет выступать абстрактная организация. История вопроса общей модели эволюции такова. В 1910-1930-х годах классическими работами Р. Фишера (R.A.Fisher), Дж. Холдейна (J.B.S. Haldane), и С. Райта (S.Wright) были заложены основы популяционной генетики. Классическая теоретическая популяционная генетика была основана на синтетической теории эволюции, т.е. на синтезе Дарвиновской концепции естественного отбора и Меделевской дискретной генетики. Согласно синтетической теории эволюции, главный механизм прогрессивного развития - естественный отбор тех организмов, которые смогли получить выгодные мутации. Математическая популяционная генетика на базе синтетической теории эволюции интенсивно развивалась до 60-х годов, когда возникли определенные трудности, связанные с экспериментальными достижениями молекулярной генетики (оценки скорости эволюционной замены аминокислот в белках и полиморфизма белков). Чтобы проинтерпретировать экспериментальные результаты, М. Кимура предложил так называемую теорию нейтральной эволюции [1]. Основное предположение теории М. Кимуры: мутации на молекулярном уровне (замены нуклеотидов в ДНК и аминокислот в белках) преимущественно нейтральны, или слабо невыгодны. Используя математические методы популяционной генетики, М. Кимура вывел ряд следствий теории нейтральности, которые находятся в довольно хорошем согласии с экспериментальными данными. Образно говоря, теория нейтральности – это популяционная генетика на базе достижений молекулярной биологии.

Среди работ, посвященных моделированию общих кибернетических закономерностей биологической эволюции, отметим также интересный цикл исследований С. Кауффмана, посвященный анализу автоматов, состоящих из множества случайно связанных логических элементов [2]. Отдельный автомат можно рассматривать как модель молекулярно-генетической системы управления живой клетки, при этом каждый логический элемент интерпретируется как регулятор синтеза определенного фермента. Наиболее поздними разработками являются работы Эйгена и Шустера [3]. В их работе Принцип самоорганизации молекул они предложили модель гиперциклов.

Постановка задачи

В настоящее время организациям все чаще приходится задумываться не только о информационной безопасности как таковой, но и об уровне безопасности. Можно выделить абсолютный и относительный уровень безопасности. Абсолютный уровень достигается за счет соблюдения правил неких стандартов, например, Общих Критериев. Подбирая набор атрибутов можно формально соответствовать некоему стандартному уровню безопасности. Это хорошо, но не достаточно, так как существуют другие фирмы, угрозы постоянно меняются, появляются новые угрозы, старые угрозы изменяются. Это постоянный процесс и стандарты не успевают за столь динамично развивающейся областью как информационная безопасность. Новые технологии несут в себе и новые угрозы. Необходимо динамически реагировать на их появление и поддерживать свой уровень безопасности на неком приемлемом для организации уровне. Для оценки уровня необходимо использовать модель, которая позволила бы отслеживать текущий уровень безопасности, а также, по возможности, показывала изменение уровня при изменении того или иного показателя. Похожие модели существуют в природе. По сути они описывают эволюцию организма, в нашем случае фирмы, в природе, что для нас является полем информационной безопасности. Таким образом, проведя параллели между биологическими моделями и информационными можно получить подобие эволюционной модели развития фирмы в общем поле угроз.

Методы исследований

Для решения вышеописанной задачи используем модель квазивидов. В модели квазивидов анализируется эволюция популяции последовательностей символов (информационных аналогов цепочек ДНК или РНК). Последовательности обладают определенными селективными ценностями. В процессе эволюции происходят отбор последовательностей в соответствии с их селективными ценностями и мутации – случайные замены символов в последовательностях.

Характерная эволюция распределения последовательностей схематически показана на рис. 1.

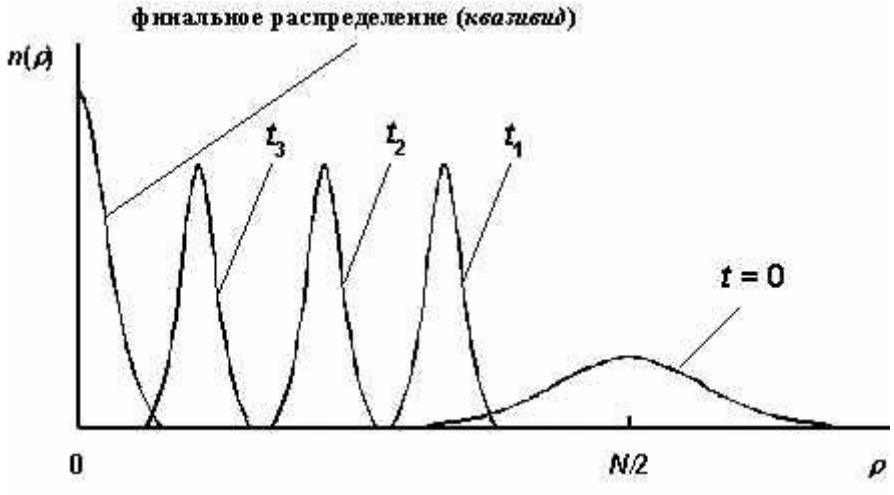


Рис. 1. Динамика распределения последовательностей *n(ρ)* (схематически) в модели квазивидов: t – время, $t_1>t_2>t_3$

Для простоты предполагается, что последовательности бинарны, т.е. критерии безопасности каждой фирмы представляет собой последовательность нулей и единиц. Длина последовательностей равна N (N>>1). Есть одна оптимальная последовательность, обладающая максимальной селективной ценностью. Селективные ценности ос-

тальных последовательностей тем меньше, чем больше расстояние по Хеммингу r (число несовпадающих символов) между рассматриваемой и оптимальной последовательностями. Исходное распределение (t = 0) случайно. В результате эволюции формируется квазивид: популяция, в которой наряду с оптимальной последовательностью есть множество сходных с ней мутантов.

Приведем формальное описание модели квазивидов.

Квазивид – модель эволюции информационных последовательностей [3–5]. Эволюционирующая популяция есть множество $\{S_k\}$, состоящее из n последовательностей S_k, k = 1,..., n. Каждая последовательность представляет собой цепочку из N символов, S_{ki}, i = 1,..., N. Символы выбираются из набора атрибутов безопасности, содержащего n различных критериев. Например, мы можем рассматривать алфавит с двумя критериями (n = 2, S_{ki} = 1, –1) или с четырьмя критериями (n = 4, Ski = Г, Ц, А, У). Предполагается, что длина последовательностей N и численность популяции n велики: N, n >> 1.

Последовательности представляют собой наборы атрибутов безопасности модельных фирм, фирмы характеризуются определенными неотрицательными приспособленностями f(S). В простейшем случае предполагается, что имеется оптимальная последовательность S_m, имеющая максимальную приспособленность. Приспособленность произвольной особи S определяется расстоянием по Хеммингу r (S, S_m) между S и S_m (числом несовпадающих компонент в этих векторах), причем f(S) экспоненциально уменьшается с ростом r (S, S_m).

Эволюционный процесс состоит из последовательности поколений. Новое поколение $\{S_k(t+1)\}$получается из старого $\{S_k(t)\}$ путем отбора и мутаций последовательностей S_k (t) ; здесь t – номер поколения.

Опишем шаги общей схемы, которые приводят к появлению нового уровня безопасности.

0. Формирование начальной популяции $\{S_k (0)\}$. Для каждого k = 1, ..., n, и для каждого i = 1,..., N , выбираем случайно символ S_{ki}, полагая его равным произвольному символу данного алфавита.

1. Отбор

1.1. Расчет приспособленностей. Для каждого k = 1, ..., n, вычисляем величину $f(S_k)$.

1.2. Формирование новой популяции $\{S_k(t+1)\}$. Отбор n особей в новую популяцию $\{S_k (t+1)\}$ с вероятностями, пропорциональными $f(S_k)$.

2. Мутации особей в новой популяции. Для каждого k = 1, ..., n, для каждого i = 1, ..., N, заменяем $S_{ki}(t+1)$ на произвольный символ алфавита с вероятностью P. Параметр P характеризует интенсивность мутаций.

Организация последовательности поколений. Повторяем шаги 1, 2 для t = 0, 1, 2,…

Схему отбора проиллюстрируем следующим образом. Представим, что у нас есть рулетка. Для каждого поколения отмечаем на рулетке n секторов, долю k-го сектора (отнесенную ко всей площади круга) полагаем равной $q_k = f_k [S_l f_l]^{-1}$ (Рис. 2). Здесь мы обозначили: $f_k=f(S_k)$. Далее n раз крутим рулетку, каждый раз определяем номер сектора, на котором останавливается стрелка, и соответствующую этому номеру особь выбираем в популяцию следующего поколения. Таким образом в следующее поколение будут отобраны n особей. При этом для каждого вращения рулетки вероятность k-й особи попасть в следующее поколение пропорциональна ее приспособленности f_k.

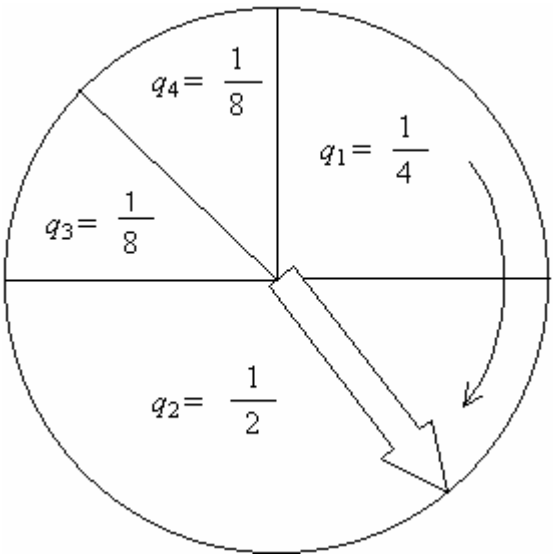


Рис. 2. Схема отбора, при которой особи выбираются в популяцию нового поколения с вероятностями q_k, пропорциональными их приспособленностям f_k. Показан пример, для которого n = 4, f1 = 2, f2 = 4, f3 = 1, f4 = 1

Рассмотрим детерминированный случай – численность популяции высока: $n >> n^N$.

Характер эволюции существенно зависит от численности популяции n. Если n очень велико ($n >> n^N$), то численности особей каждого вида можно рассматривать как большие числа, и эволюция может рассматриваться как детерминированный процесс. В этом случае эволюционная динамика популяции может быть описана системой обыкновенных дифференциальных уравнений (или системой разностных уравнений), методы, исследования которых хорошо известны.

В противоположном случае ($n^N >> n$) эволюционный процесс существенно стохастический, и здесь для характеристики основных особенностей эволюции целесообразно использовать разумные количественные оценки и методы компьютерного моделирования.

Можно работать в дискретном времени, следуя непосредственно вышеприведенному формальному описанию модели. Каждый шаг по времени при этом соответствует одному поколению. Можно работать и в непрерывном времени, предполагая, что при переходе от поколения к поколению численности «видов» меняются незначительно (либо, считая, что поколения существенно перекрываются, так что процесс эволюции можно считать непрерывным).

Основное рассмотрение проведем для случая непрерывного времени. Динамику популяции будем характеризовать следующими уравнениями:

$$dx_k/dt = W_k x_k + S_l f_{kl} x_l - E x_k ,$$

где x_k – численность особей k-го вида; W_k – селективная ценность особей k -го вида; f_{kl} – параметры, характеризующие мутационные потоки (символы S_l обозначают суммирование по l); E – параметр, характеризующий общее разбавление популяции, при этом будем считать, что этот параметр таков, что суммарная численность популяции постоянна:

$$S_l x_l = n = \text{const} .$$

Если ввести частоты $p_k = x_k/n$, характеризующие вероятности нахождения особей разных видов в популяции, то мы получаем:

$$dp_k /dt = W_k p_k + S_l f_{kl} p_l - E p_k, \; S_l p_l = 1 .$$

Заключение

В настоящее время существует множество угроз, которые заставляют адекватно реагировать на них. В современной быстроменяющейся среде это делать достаточно не просто. Появляющийся и существующие стандарты не дают такой возможности. Одним из возможных решений является создание модели динамической оценки уровня безопасности предприятия на основе биологических моделей эволюции.

В статье была предложена модель динамической оценки уровня безопасности предприятия. Данная модель предполагает наличие первоначальных критериев безопасности, а также определенного количества фирм конкурентов. Данная модель требует, и будет иметь дальнейшее развитие для усовершенствования определения оценки уровня защищенности предприятия.

Данная модель не претендует на абсолютную точность, но позволяет получить представление об общем уровне безопасности предприятия. На основе ее результатов уже можно предпринимать шаги по устранению проблем безопасности. В дальнейшем предполагается развитие модели для повышения уровня оценки уровня безопасности.

Литература

1. Кимура М. Молекулярная эволюция: теория нейтральности. – М.: Мир. – 1985. – 400 с.
2. Кауффман С. Антихаос и приспособление // В мире науки. – 1991. – N.10. – С. 58–65.
3. Эйген М., Шустер П. Гиперцикл. Принципы самоорганизации макромолекул. – М.: Мир. – 1982. – 270 с.
4. Эйген М. Самоорганизация материи и эволюция биологических макромолекул. – М.: Мир. – 1973. – 216 с.
5. Fosterling H.D., Kuhn H., Tews K.H. Computermodell zur Bildung selbstorganisierender Systeme // Angew. Chem. – 1972. – N.18. – PP. 862–856.

УДК 004.4+355.4

ВЕДЕНИЕ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ МЕЖДУ КОНКУРИРУЮЩИМИ СУБЪЕКТАМИ

М.В. Григорьева
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В статье рассматриваются понятия «информационное противоборство», «информационное оружие», «информационные операции». Исследуется переход к противодействиям с применением информационных операций, основные проблемы применения научного подхода к описанию информационного противодействия. Представлена общая объектная модель ведения информационного противодействия между двумя субъектами.
Ключевые слова: информационное противодействие, информационная война, стратегии

Введение

Лучшее из лучшего – покорить нужную армию, не сражаясь. Хорошо разгромить противника на поле боя, еще лучше – отбить у него желание воевать, сделать так, чтобы ему даже не пришла в голову мысль о возможности войны. Так говорил Сунь-Цзы – древнекитайский философ, мыслитель, предположительно, живший в VI или, по другим источникам, в IV веке до н.э.

Для достижения этой последней цели и ведутся информационные войны, проводятся информационные операции, в задачу которых входит не просто обмануть или запугать противника, а изменить структуру его сознания, категории его мышления, его цели [1].

Цель данной работы – исследование ведения информационного противодействия, перехода к противостоянию с применением информационных операций, а также построение моделей, с разной степенью формализации описывающих стратегии ведения информационного противоборства между конкурирующими субъектами, в зависимости от их целей, стратегической информации о конкуренте и других факторов.

Основные проблемы и задачи

Многообразие угроз в области информационных операций и взаимодействий можно свести к двум важнейшим проблемам: защите информации и защите от информации, то есть противодействию информационным воздействиям.

Применение научного подхода к описанию информационного противодействия сдерживает наличие следующих проблем:

(a) отсутствие общепринятого определения понятия информационного противодействия, отсутствие устоявшейся базовой терминологии в этой области;
(b) отсутствие теоретической основы (цели, задачи, принципы, закономерности, сущность и содержание информационного противоборства);
(c) отсутствие методик анализа целей, задач, потенциала конкурирующей стороны по доступным признакам;
(d) недостаточная правовая поддержка, отсутствие законодательной базы, регулирующей отношения в сфере информационного противоборства.

Для достижения поставленной цели с учетом имеющих место проблем решаются следующие задачи:

(a) Определение смысла, вкладываемого в понятие «информационное противодействие» («информационная война») в данной работе, формулирование основных его признаков.

(b) Исследование методов информационного противодействия, факторов, влияющих на ведение противодействия.
(c) Выделение и характеристика основных сущностей, участвующих в информационном противоборстве, определение их составляющих.
(d) Построение модели, описывающей выбранные сущности и их отношения.

Для выявления основных сущностей применялся онтологический анализ текстов, при построении модели использован объектно-ориентированный подход.

Основные положения и результаты работы

При осуществлении 1 и 3 этапов проводился анализ некоторых существующих систем взглядов на сущность информационного противодействия, информационной войны [1–6].

В первую очередь был определен смысл, вкладываемый в понятие «информационная война». Для этого был рассмотрен ряд работ, отражающих разные подходы к трактовке понятия [1–6].

Человечество с незапамятных времен сталкивалось с проблемой информационных войн на всех уровнях, и лук, стрелы, мечи, пушки и танки, в конце концов, только завершали физический разгром сообщества, уже потерпевшего поражение в информационном противостоянии.

«Война» в соответствии с используемыми в большинстве стран мира определениями представляет собой «наличие вооруженной борьбы между государствами» [2]. Таким образом, информационная война – это борьба с использованием исключительно информационного вооружения, т. е. информационных технологий, базирующихся на производстве, распространении и навязывании информации.

В качестве наиболее точного и емкого выбрано определение, предложенное д.т.н. профессором С.П. Расторгуевым:

«Информационная война – открытые и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере» [1].

Приведенное положение составляет содержание термина «информационная война» («информационное противоборство») в контексте данной работы.

Совокупность таких успешно выполненных *информационных воздействий* приводит к достижению цели, как правило, заключающейся во взятии под контроль системы управления противника (государства) или слому этой системы управления и замены ее на другую – контролируемую.

Информационная война не детище сегодняшнего дня. Многие приемы информационного воздействия возникли тысячи лет назад вместе с появлением информационных самообучающихся систем — история обучения человечества это и есть своего рода постоянные информационные войны.

Но понятно, что чем лучше развиты конкретные технологии, тем дешевле и эффективнее их применение в войне. Поэтому история войн неразрывно связана с историей развития соответствующего оружия и увеличения эффективности его применения.

Эволюция средств вооружения базируется на следующих принципах эффективности [3]:

(a) оружие тем эффективнее, чем большее количество информационных систем (людей), оно позволяет перепрограммировать или уничтожать;
(b) оружие тем эффективнее, чем меньше времени требуется для его изготовления и применения;

(c) оружие тем эффективнее, чем больше расстояние, при требуемой точности, при его применении;
(d) оружие тем эффективнее, чем меньше в конкретных условиях стоимость его производства;
(e) оружие тем эффективнее, чем меньше накладных расходов по его применению.

Информационное оружие – это средства, применяемые для активации, уничтожения, блокирования или создания в информационной системе процессов, в которых заинтересован субъект, применяющий оружие.

Переход к информационным войнам, к борьбе с применением технических средств и информационных технологий стал возможным только с момента должного уровня развития и распространения таких технологий, т.е. со второй половины 20 века.

Условиями для такого перехода стали:

(a) резкое удешевление производства данных благодаря появлению средств вычислительной техники;
(b) создание автоматизированных средств для получения знания из данных (средств сбора, обработки, передачи и хранения информации);
(c) удешевление и сокращение времени на доставку сообщений практически в любую точку планеты благодаря развитию телекоммуникационных средств;
(d) повышение эффективности информационного воздействия благодаря появлению развитых технологий в области перепрограммирования информационных самообучающихся систем: теория программирования для ЭВМ и НЛП-программирования для социальных систем, включая большое количество методов и приемов информационно-психологического воздействия.

Развитие информационного оружия происходило как в технической, так и в гуманитарной составляющей. История информационного оружия в гуманитарной сфере – это история СМИ, включая сетевые СМИ, пропаганды и технологий скрытного управления человеком (гипноз, реклама, специальные учения, НЛП-программирование и т.п.) [4]. История оружия в технической сфере – это история программных средств скрытого информационного воздействия (вирусы, закладки, средства подавления информационного обмена в телекоммуникационных сетях) и информационные технологии их применения [5].

В рамках данной работы были выделены основные признаки информационной войны:

(a) основная тактическая задача – получение конкурирующими сторонами материального преимущества, причем в процессе информационной войны одни стороны получают преимущество, а другие его теряют;
(b) осуществляется посредством открытых и скрытых информационных воздействий;
(c) сопровождается применение информационного оружия;
(d) особые формы реализации намерений: дезинформирование, манипулирование, пропаганда, лоббирование, управление кризисами, шантаж.

Стратегия применения информационного оружия носит исключительно наступательный характер [1], что позволяет выйти на следующее утверждение. Наступательный характер информационного оружия во многом определяет лицо информационной войны и позволяет априори определить потенциального информационного агрессора. А это значит, можно предположить, что объем информации, целенаправленно передаваемый от одной страны к другой, и является мерой информационной агрессивности.

В качестве основных сущностей, участвующих в информационном противоборстве, были выделены объект и субъект информационного противоборства. Основная характеристика объекта – ценность, субъекта – его интересы. Далее описаны отношения между этими понятиями:

- объект информационного противоборства имеет некоторую ценность;
- субъект информационного противоборства может владеть объектами информационного противоборства и использовать его;
- субъект имеет интересы в информационном пространстве, представляет и защищает их;
- субъект может обладать информационным оружием, а также применять его;
- один субъект информационного противоборства противодействует другому субъекту информационного противоборства;
- один субъект информационного противоборства пытается заполучить объект другого субъекта информационного противоборства.

Сформулированные сущности, их характеристики и соответствующие отношения представлены в виде объектной модели с использованием методики UML. Разработанная модель представлена на рис. 1.

Важным результатом моделирования является возможность установления зависимостей для конкретных субъектов между различными факторами взаимодействия.

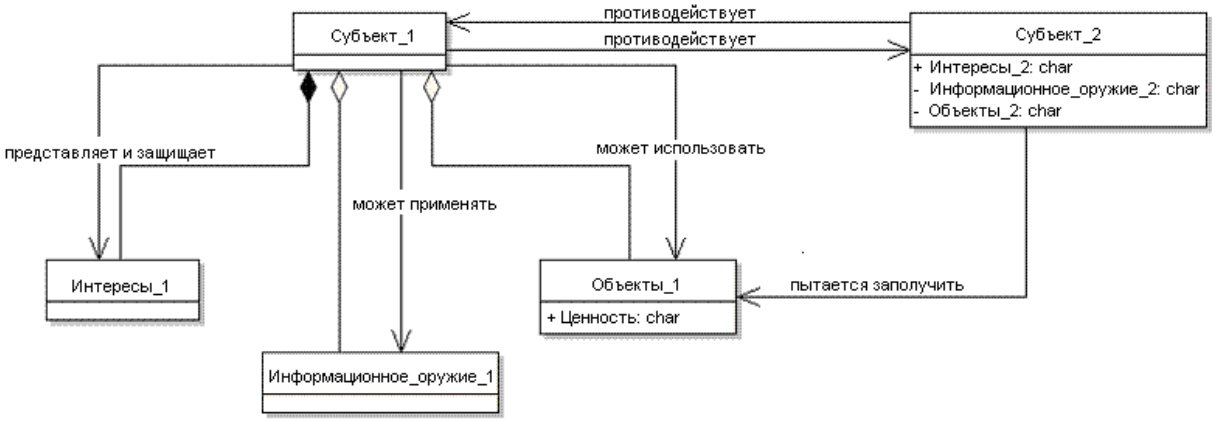


Рис. 1. Общая объектная модель ведения информационного противоборства между двумя субъектами

Последовательность ходов ведения информационного противодействия между субъектами от начала до конца конфликта – стратегия информационного противодействия. Стратегия является выигрышной, если обеспечивает победу вне зависимости от стратегии, выбранной противником.

Проблема скрытости многих информационных воздействий имеет не последнее значение при применении информационного оружия. Жертвы данного вида оружия, даже владея теорией и соответствующей материально-технической базой, приходят к осознанию себя как жертвы только потом.

Обучение также является процессом информационного воздействия и может использоваться как информационное оружие. В таком случае выйти победителем в информационном противодействии – это значит вовремя понять, чему можно обучаться, а чему нельзя, т.е. какие входные данные можно обрабатывать, а какие – ни в коем случае.

С.П. Расторгуевым была предложена следующая типовая стратегия информационной войны, представленная на рис. 2 [1].

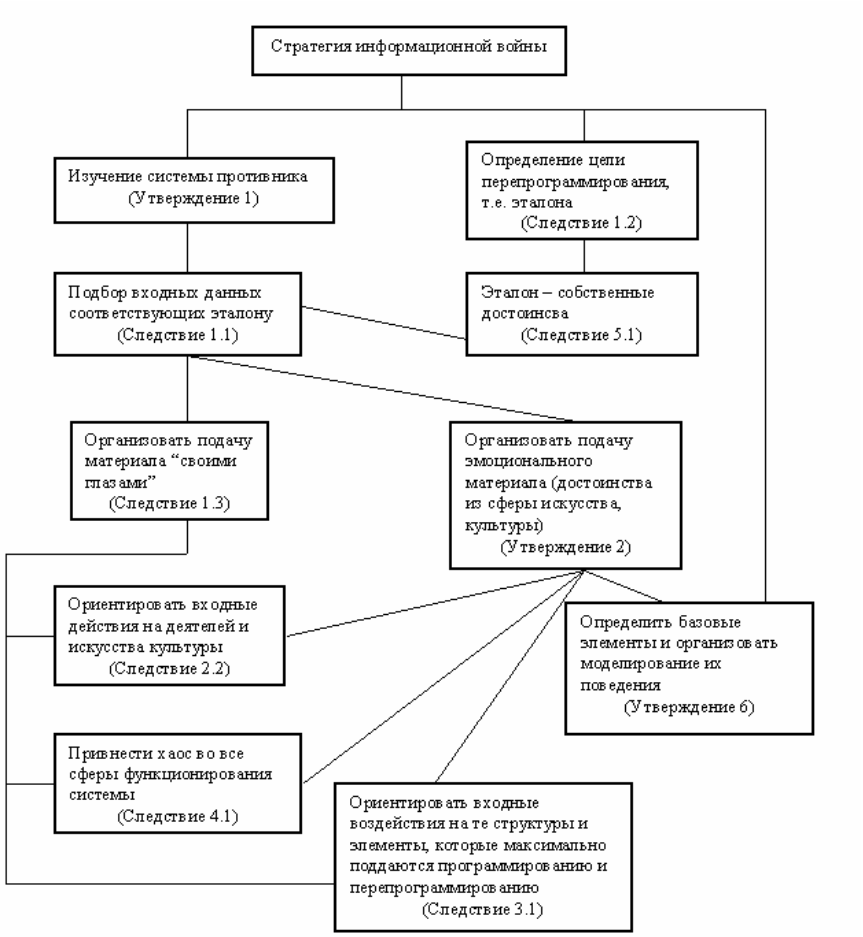


Рис. 2. Типовая стратегия информационной войны

Приведенная схема, безусловно, не отражает всех возможных подходов и приемов к организации и проведению операций по информационному воздействию. Но любая информационная обучающаяся система обладает базовым набором смыслов или знаний, который во многом и определяет поведение этой системы. И данная стратегия может быть усложнена и уточнена с увеличением базового набора смыслов и показаний состояния субъекта: количеством элементов, ответственных за доставку данных, сбор входных данных, их обработку, представление результата, и эффективностью их функционирования, количеством и качеством связей между элементами, защищенностью («жизненной силой») перечисленных выше элементов и связей между ними. При этом имеется в виду, что понятие «информационная защищенность элемента» подразумевает защиту этого элемента от информационных воздействий.

Заключение

Информационные технологии коренным образом изменили способы ведения и развития конфликтов. Новые технологии позволяют собирать, анализировать и распространять информацию о конкуренте для получения преимущества над ним. Однако наряду с преимуществами информационные системы несут в себе ряд серьезных недостатков. В первую очередь, они уязвимы для противника, пытающегося всеми способами обладать информационным превосходством, воздействуя на информационные системы и информационные процессы противостоящей стороны.

Все, живя в этом мире, полном противоречий и взаимоисключающих интересов, ведут информационные войны разных уровней [6]. Это и государственные деятели,

которым необходимо квалифицированно защищать интересы государства от сторонних угроз; политики, которым необходимо выплыть из моря информационных угроз со стороны других партий и движений; руководители банков, финансово-промышленных групп, фирм, желающие победить в конкурентной борьбе, которая является по своей сути вариантом информационной войны; и просто индивидуумы, обреченные на ежедневные информационные стычки со средствами массовой информации, с семьей, коллегами по работе и т.п.

Чтобы выиграть, нужно помнить, что информация правит миром, а человек – информацией. «Кто владеет информацией - тот владеет миром» (Ротшильдт).

В рамках данной работы было проведено исследование ряда проблем предметной области. В частности было проведено исследование понятий «информационная «война», «информационная операция», «информационное оружие», перехода к противодействиям с применением информационных операций, сформулированы основные проблемы применения научного подхода к описанию информационного противодействия. По результатам анализа нескольких систем взглядов на сущность информационной войны сформирован контекст моделирования и построена общая объектная модель, описаны возможности ее практического применения. Создан методический задел и разрабатываются уточненные модели стратегий взаимодействия субъектов.

Литература

1. Расторгуев С.П. Информационная война. – М.: Радио и связь. –1999. – 416 с. – ISBN 5-256-01399-8.
2. Свиридов И.В. Информационная война: определения, подходы, взгляды... – журнал «Безопасность информационных технологий». – 1998. – № 4. – 24 с.
3. Расторгуев С.П. Информационная война. Проблемы и модели. Экзистенциальная математика: учебное пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности / С.П. Расторгуев – М.: Гелиос АРВ. – 2006. – 240 с. – ISBN 5-8-438-145-1.
4. Комов С.А. Информационная борьба в современной войне: вопросы теории // Военная мысль. – 1996. – № 3. – С. 73.
5. Манойло А.В. Государственная информационная политика в особых условиях, монография. – М.: Изд. МИФИ. – 2003. – 388 с.
6. Остапенко Г.А. Информационные операции и атаки в социо-технических системах. Учебное пособие для вузов / Под ред. чл. – корр. РАН В.И. Борисова. – М.: Горячая линия – Телеком, 2007. – 134 с.

УДК 004.056

ПРОБЛЕМА ВЫЯВЛЕНИЯ НАИБОЛЕЕ БЕЗОПАСНОГО ПУТИ СЛЕДОВАНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ

А.И. Спивак
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Управление потоками данных в открытой сети интернет возложено на протоколы динамический маршрутизации. В их реализации не заложено механизмов для принятия решения о пути следования информации на основе данных о безопасности того или иного узла сети. Расширение функционала возможно с помощью моделирования процесса принятия решения о направлении данных по тому или иному пути на основе показателей безопасности.

Ключевые слова: безопасность, канал связи, маршрутизация, угроза безопасности

Введение

Движение потоков информации в открытой сети интернет управляется протоколами динамической маршрутизации. Основное их предназначение это возможность быстрого перестроения в соответствии с изменяющимися условиями среды передачи данных. А такие изменения могут быть связаны, прежде всего, со следующими явлениями:

- выход из строя телекоммуникационного оборудования;
- нарушение работоспособности каналов передачи данных;
- автоматическая балансировка нагрузки каналов передачи данных;
- ошибки конфигурирования оборудования.

Аспекты безопасности

Все механизмы функционирования систем маршрутизации направлены главным образом на обеспечение работоспособности. Если взглянуть на вопрос передачи данных с точки зрения безопасности, то очевидно, что этому вопросу уделяется достаточное малое внимание. Необходимо помнить, что обеспечение безопасности это не набор мер, а комплексный подход, который учитывает все аспекты защищенного функционирования заданной системы. Другими словами использование только аутентификации и шифрования при передаче данные не может гарантировать безопасность такого взаимодействия. Ни одним из аспектов информационной безопасности не стоит пренебрегать, всеми необходимо пользоваться в комплексе, дополняя одни другими. Вопросу выбора пути следования защищаемой информации также необходимо уделять внимание с целью повышения общего уровня безопасности всего сеанса связи.

Угрозы безопасности

Следует понимать каким угрозам может подвергаться сеанс передачи информации. Если рассмотреть именно процесс следования информации от узла источника до узла назначения, то возможно следующие виды атак:

- следование транзитом через потенциально опасный узел.

В результате защищаемые данные в том или ином виде (зашифрованном или незашифрованном) будут у злоумышленника. Угрозой безопасности является то, что их наличие влечет за собой возможность накопления с целью последующего анализа (семантического, статистического др.). Кроме того, будет известен сам факт передачи,

время передачи, а также источник и назначение.

- изменение маршрута следования данных.

Опасность для передачи данных может быть вызвана прекращением возможности сообщения между отдельными узлами сети, что является атакой отказа в обслуживании. Также возможно изменение маршрута следования с целью направления собственно передачи данных на поддельный узел назначения. В таком случае возможно раскрытие передаваемых данных.

Варианты усиления безопасности

Возможность реализации описанных выше угроз безопасности свидетельствует о том, что необходимо иметь механизмы защиты против такого рода атак. Средства противодействия могут работать на различных уровнях построения комплексной системы защиты информации. Одним из вариантов усиления безопасности в рамках задачи вычисления оптимального пути следования данных может быть моделирование данного процесса с учетом факторов деструктивного воздействия со стороны злоумышленников. Возможен учет степени доверия к каждому отдельно взятому узлу в цепочке следования защищаемой информации. Данное доверие должно быть учитываемым показателем в процессе выбора наиболее безопасного пути следования защищаемой информации. Что в свою очередь сделает более затруднительным изменение маршрутных данных с целью перехвата информации, либо с целью нарушения работоспособности канала связи.

Все эти меры призваны только улучшить общую безопасность при передаче данных по открытым каналам связи, и не могут заменить другие системы защиты информации.

Литература

1. Семенов Ю.А. Протоколы и ресурсы Интернет. Радио и связь. – М.: Радио и связь. – 1996.

УДК 004.056

ПРОБЛЕМЫ ВЫЯВЛЕНИЯ НДВ В ПРОГРАММНОМ КОДЕ

Н.Н. Дацун, А.Ю. Потехонченко
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Успешное развитие рынка информационной безопасности обусловлено чрезвычайной структурной сложностью и динамичностью реализаций программного обеспечения компьютерных систем, с одной стороны, и недостаточностью внимания к тестированию безопасности программ и их обновлений, с другой. Уязвимость программных ресурсов определена объективными причинами. На сегодняшний день существует ряд проблем, связанных с выявлением недекларированных возможностей в программном коде. Нормативная, методическая и инструментальная база выявления недекларированных возможностей программ не позволяет эффективно обеспечивать безопасность программных ресурсов.

Ключевые слова: недекларированные возможности, выявление, статистический анализ, динамический анализ

Введение

Недекларированные возможности (НДВ) – функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации**.**

Наличие недекларированных возможностей обусловлено значительными объемами и сложностью современных программных продуктов. На сегодняшний день существует ряд проблем, связанных с выявлением недекларированных возможностей в программном коде. Связано это с тем, что существующая нормативная, методическая и инструментальная база выявления НДВ программном коде не позволяет гарантированно обеспечивать безопасность программ.

Проблемой защиты программ занимаются испытательные лаборатории Минобороны, ФСБ и ФСТЭК России, которые в своей работе опираются на Руководящий документ (РД) Гостехкомиссии России по контролю над недекларированными возможностями. Однако опыт выявления авторами более 20 закладок и тысяч некорректностей кода показал, что большинство из них обнаружены не только не в соответствии с указанным документом, но и порой вопреки ему.

Проблемы выявления НДВ

Участки исполняемого кода, содержащие НДВ, несут потенциальную опасность, так как в случае сбоев и неисправностей аппаратной части ПЭВМ или при выполнении условий, определённых злоумышленником, возможна передача управления на эти участки кода. Вследствие этого возможна некорректная работа исследуемого ПО или системы в целом, которая может привести к нарушению целостности, доступности и конфиденциальности защищаемой информации.

Безопасность современных информационных технологий в значительной мере определяется отсутствием в них скрытых дефектов – недекларированных возможностей.

Руководящий документ по недекларированных возможностям был создан в 90-е годы для решения задачи контроля над поставляемыми в Россию зарубежными продуктами и тогда, вне сомнений, имел большое значение. Методы, определяемые в РД, берут начало в теории надежности функционирования программ, поэтому вопросы защиты собственно кода отражены в документе недостаточно явно. Документ фактически не затрагивает вопросы безопасности ПО, а именно, наличия в нем каких-либо уязвимостей или закладок.

Испытания на отсутствие недекларированных возможностей предполагают глубокое исследование ПО и связаны с анализом, как исполняемого кода, так и исходного с целью установления факта отсутствия (либо наличия) в некотором программном решении функциональных возможностей, не документированных разработчиком.

В соответствии с РД основными видами проверок, которые проводятся на выявление НДВ, являются структурный статический и динамический анализ исходных текстов (структуры программы, формирования и прохождения всех ее путей). В отношении статического и динамического анализа следует подчеркнуть, что результаты статического анализа по сложности интерпретации сопоставимы с исходными текстами, а динамический анализ дополнительно требует составления и реализации соответствующих тестов маршрутов.

Данный подход эффективен для структурно несложного программного обеспечения. Для больших комплексов использование его проблематично. Современное программное обеспечение довольно сложное, и есть все предпосылки считать, что оно станет еще сложнее в ближайшем будущем. Например, в 1983 году программа Microsoft Word состояла только из 27000 строк кода, но, согласно данным Натана Мирвольда (Nathan Myhrvold), к 1995 году эта программа увеличилась уже до 2 млн. строк кода [1].

Существует ряд специализированных средств для проведения испытаний на выявление недокументированных возможностей. Но ни один из них не может с полной гарантией выполнить проверку ПО. На это влияет целый ряд факторов. Совершенно очевидно, что эти средства не позволяют оперативно включать признаки современных уязвимостей кода в сигнатуры в меняющейся среде защиты и в новых средах программирования. В некоторых средствах эти сигнатуры вообще отсутствуют.

Заключение

В настоящее время основной уязвимостью в программном обеспечении является наличие недекларированных возможностей. На сегодняшний день ни одно из существующих средств выявления НДВ не дает гарантий их обнаружения. Необходимы разработка и внедрение методов и средств выявления уязвимостей программного кода.

Литература

1. Хогланд Г., Мак-Гроу Г. Взлом программного обеспечения: анализ и использование кода. – М.: Вильямс. – 2005. – 34 с.
2. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. – М.: Гостехкомиссия России. – 1998.
3. Цирлов В., Миронов С., Марков А. Выявление уязвимостей в программном коде//Открытые системы. – 2005. – № 9. – С. 64–69.
4. Компаниец Р.И., Ковалев В.В., Маньков Е.В. Экспертиза и защита кода программ на основе автоматов динамического контроля// Защита информации. Инсайд. – 2007. – № 3.
5. Марков А., Никулин М., Цирлов В. Сертификация средств защиты персональных данных: революция или эволюция?// Защита информации. Инсайд. – 2008. – № 5.
6. Марков А.С., Щербина С.А. Испытания и контроль программных ресурсов//InformationSecurity. – 2003. – № 6 – 25 с.
7. Темнов О.Д. Анализ и исследование методов средств обнаружения недекларированных возможностей//Научно-технический вестник СПбГУ ИТМО. – 2008. – №39. С. 45–50.

УДК 004.7

ИММУНОЛОГИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В.В. Кузнецов
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Статья посвящена проблеме применения интеллектуальных технологий для решения задач обеспечения информационной безопасности компьютерных систем. Предложено создавать сложные технические системы в едином процессе с встроенными интеллектуальными средствами защиты информации, способными к адаптации к изменению поля угроз и использующие подобные иммунным механизмы для распознавания и нейтрализации атак на информационные ресурсы компьютерных систем.
Ключевые слова: безопасность, иммунология, корпоративная сеть, угроза

Введение

Теория защиты информации в информационных технологиях (ИТ) и телекоммуникационных системах переживает период переосмысления базовой методологии. Классическая теория и практика защиты информации в ИТ и телекоммуникационных системах, базирующаяся на тактике фиксации поступающих угроз, их изучении и анализе, создании методов и средств защиты от них, приводит к все большему отставанию темпов создания средств и методов защиты от темпов нарастания действия угроз безопасности, неоправданным экономическим и социальным потерям.

Иммунная система в теории защиты информации

Рост распространенности и применимости ИТ, по видимому, приводит к объективному росту угроз безопасности с ростом сложности ИТ. Ситуация аналогична развитию и эволюции системы защиты живых организмов, которая привела к созданию иммунной системы, методология защиты которой существенно отличается от тактики «жареного петуха» существующей в теории защиты информационных технологий в настоящее время.

К сожалению, конструктивное использование биогенетической аналогии в теории защиты информационных технологий затруднено из-за повального применения очень красивых терминов без детального анализа применимости в теории защиты информационных технологий и непонимания существенной разницы между классической теорией защиты информации и иммунологией информационных технологий.

Принципиальная разница в методологии защиты отдельного рабочего места ИТ и методологии защиты корпоративной вычислительной сети, состоящей из сотен и тысяч рабочих мест, заключается в различии уровня требований по безопасности к этим объектам. Если для защиты одного рабочего места при частоте атак 10^{-6} допустимая вероятность их реализации составляет 10^{-3}, то для корпоративной сети из сотен рабочих мест допуск такой реализации атак приводит к гибели всей сети. Используя принятую аналогию, изменение одной клетки (одного рабочего места ИТ) в организме (корпоративная сеть) приводит к гибели всего организма (корпоративной сети). Понятно, что уровень требований по безопасности для корпоративной сети должен быть на два-три порядка выше, что приводит к необходимости использования и создания принципиально иной методологии защиты.

Заключение

Необходимы научные работы направленные на решение перспективных задач приближающих науку защиты информации в информационных технологиях к иммуно-

логии информационных технологий. Какое из этих направлений определит качественный скачок в науке защиты информации в информационных технологиях предсказать невозможно. По-видимому, необходимо развивать все направления исследований и разработок в этой области.

Литература

1. Нестерук Г.Ф., Осовецкий Л.Г., Харченко А.Ф. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов (Иммунология систем информационных технологий). – СПб.: Изд-во СПбГУЭФ. – 2003. – 364 с.: ил.

УДК 004.056

ПРИМЕНЕНИЕ ПОДХОДА MODEL CHECKING ДЛЯ СОЗДАНИЯ МОДЕЛИ АНТИВИРУСНОГО ДВИЖКА

О.В. Чиков

Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Целью исследования является описание применения подхода Model Checking для создания модели ядра антивирусного программного обеспечения. Рассматриваются достоинства и ограничения предложенного метода.

Ключевые слова: антивирус, Model Checking, модель Крипке, верификация

Введение

Чем критичнее для бизнеса программа, тем дороже обходятся дефекты в ее защите. Но, к сожалению, создание априори безопасных программ дело чрезвычайно нетривиальное, если не сказать, невозможное.

Математический аппарат для изучения динамики «обычных» биологических эпидемий был разработан достаточно давно. Биологический подход к моделированию вирусной проблемы по общему признанию начался с работ J. O. Kephart и S. R. White из IBM, однако, актуальным это направление стало только в 2001 г. Введена концепция «Warhol», так называемый «блицкриг червей» [1], а также исследованы различные концептуальные алгоритмы размножения самовоспроизводящихся кодов, кардинально повышающие эффективность их распространения.

Исследование особенностей распространения вирусов становится все более популярной темой, о чем свидетельствует рост количества не только специальных научных работ [2], но и магистерских диссертаций. Интерес этот вызван внезапным осознанием того крайне неприятного факта, что в результате вирусных эпидемий под контролем злоумышленников оказываются вычислительные ресурсы фантастической мощности как корпоративного, так и государственного характера. По здравому размышлению их можно использовать не только для организации классических распределенных DoS-атак или рассылки спама с зараженных компьютеров, но и более рационально: например, для распределенных вычислений корпорациями, неспособными приобрести необходимое количество суперкомпьютеров.

Разработаны изощренные модели, которые позволяют учесть влияние нюансов топологии программы на поведение злонамеренного кода, провести детальный анализ червей с комбинированными механизмами размножения, а также учесть человеческие факторы риска и даже оценить стоимость еще только надвигающейся угрозы.

Метод поиска

Почти каждый разработчик антивирусных продуктов реализует какие-то свои технологии, позволяющие сделать работу программы эффективнее и производительнее. Некоторые из этих технологий имеют прямое отношение к устройству «движка», так как именно от его работы часто зависит производительность всего решения.

Антивирусный «движок» (*Anti-Virus Engine*) – это программный модуль, который предназначен для детектирования вредоносного программного обеспечения. «Движок» является основным компонентом любой антивирусной программы, вне зависимости от ее назначения.

В данной статье предполагается представить формальную логику действий антивирусного движка (верификатора) на основе верификации моделей – наборе идей и методов для построения модели потенциально зараженной программы, математической

формулировки требований к ней и создания алгоритмов для формальной проверки этих требований.

Примем, что в частном случае для исследования и распознавания, факт заражения является ошибкой выполнения кода.

Существует несколько методов поиска ошибок:

- Имитационное моделирование.
- Тестирование.
- Дедуктивный анализ.
- Верификация модели программы.

В данной статье будет рассмотрен вопрос поиска ошибок (фактов заражения) в программе при использовании метода верификации модели самого движка. Основная цель исследований в этой области состоит в том, чтобы сформулировать ясную логическую методику для создания автоматических систем верификации программ.

Основными этапами стадии верификации являются:

1. Моделирование – изучение объекта, путем его упрощения, выбора тех параметров, которые существенны.
2. Спецификация – формулирование основных требований, предъявляемых модели.
3. Верификация модели – анализ работы алгоритма и его корректировка.

Внимание будет сконцентрировано на особой технике верификации, которая базируется на так называемых темпоральных логиках и позволяет уменьшить участие разработчика в верификационном процессе – техника *Model Checking* – проверка на моделях.

Model Checking – это автоматизированный подход, позволяющей для заданной модели поведения системы с конечным (возможно, очень большим) числом состояний и логического свойства (требования) проверить, выполняется ли это свойство в рассматриваемых состояниях данной модели [3].

Основная идея состоит в моделировании – описании разработчиком поведенческой модели системы, подлежащей верификации, и спецификации – формулировке требований (желаемого поведения системы). Однако, модель программы не всегда полно отражает ее поведение. Разработчик при построении модели, как правило, абстрагируется от несуществующих свойств. Такая концепция дает возможность уменьшить размер самой модели и ускорить процесс ее проверки.

Если модель удовлетворяет указанным требованиям, то верификатор сообщает об этом. Если же факт заражения (т.е. ошибки) подтвердится, то он предоставляет контрпример, который показывает, при каких условиях могло возникнуть данное несоответствие.

Контрпример представляет собой сценарий, в котором модель ведет себя нежелательным образом. Это означает, как правило, что модель ошибочна и подлежит пересмотру. Правда в некоторых случаях это может означать, что формальные требования неверны, в том смысле, что верификатор проверяет то, что разработчик не желал проверять – вариант ложного срабатывания.

Проверка модели программы позволяет разработчику обнаружить факт заражения и предусмотреть меры защиты. Если факт заражения не обнаружен, разработчик может усовершенствовать описание модели (сделать ее более реалистичной, приняв во внимание больший набор свойств) и перезапустить процесс верификации.

Основная трудность моделирования – не потерять важные детали программы, а трудность задания требований – сформулировать их корректно и исчерпывающе.

Алгоритмы *Model Checking* обычно базируются на полном просмотре пространства состояний модели: для каждого состояния проверяется, удовлетворяет ли оно сфор-

мулированным требованиям. Алгоритмы гарантированно завершаются, так как модель конечна (рисунок).

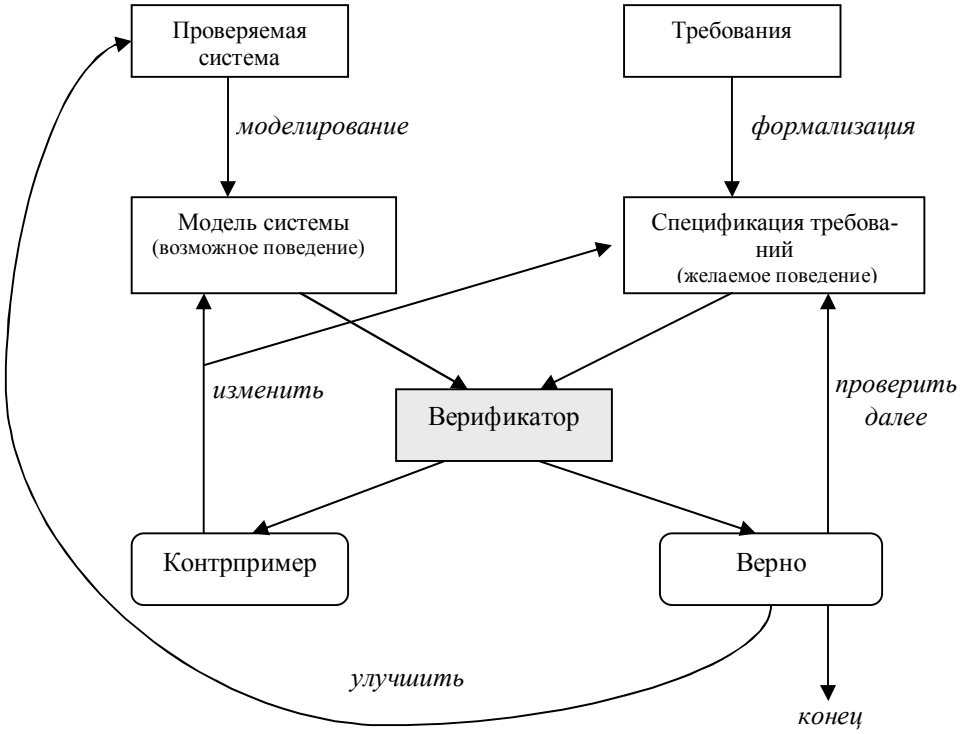


Рисунок. Принципиальная схема Model Checking

В проблематике верификации сформировалось два направления: аксиоматическое и алгоритмическое. При первом из них разрабатывается набор аксиом, с помощью которого может быть описана сама система, так и ее свойства. Основу второго направления составляет *Model Checking*.

Достоинства *Model Checking:*

1. Эффективность – программы для верификации способны работать с достаточно большим пространством состояний благодаря концепции упорядоченных двоичных разрешающих деревьев.
2. Контрпримеры.

Ограничения *Model Checking:*

1. Поддержка только конечных моделей – для большинства классов систем с бесконечным числом состояний необходимо выполнять формальную верификацию системы, то есть математическое доказательство свойств самой программы, а не ее модели.
2. Ограниченность верификации – проверяется только модель системы вместо реальной системы. Следовательно, любое применение метода *Model Checking* настолько же качественно, как и сама модель.
3. Для многопроцессорных систем размер пространства состояний в худшем случае пропорционален произведению размеров пространств состояний их индивидуальных компонент – эффект экспоненциального взрыва состояний.

Основное отличие *Model Checking* от классической формальной верификации состоит в том, что он позволяет проверять динамические свойства программы – те, которые можно записать с помощью темпоральной (временной) логики, а второй метод – соответствует ли состояние переменных на выходе из программы условиям, которые были наложены на входном состоянии.

Первым шагом при проверке корректности системы является спецификация свойств, которыми она должна обладать. Например, желательно показать, что некоторая параллельная программа никогда не попадает в тупик. Как только станет известно, какие свойства являются важными, вторым шагом будет построение формальной модели системы. Чтобы модель была пригодна для верификации, в ней должны проявляться те свойства, анализ которых необходим для установления ее корректности. С другой стороны, она должна быть свободна от частных особенностей, не влияющих на проверяемые свойства, но усложняющих верификацию.

В этой статье мы будем иметь дело главным образом с реагирующими системами и их поведением во времени. Для таких систем характерна потребность в частом взаимодействии с окружающей средой, и они работают, как правило, бесконечно долго.

Поэтому для адекватного моделирования их поведения нельзя ограничиться рассмотрением отношения *вход-выход*. Первой характерной чертой реагирующей системы, которую нам хотелось бы выделить, является ее состояние.

Состояние — это моментальный снимок или мгновенное описание системы, в котором зафиксированы значения переменных в конкретный момент времени. Нам нужно также знать, как изменяется состояние системы в результате выполнения этой системой тех или иных действий. Мы можем описать это изменение, указав состояние системы до выполнения действия и ее состояние после выполнения действия. Такая пара состояний определяет переход системы. Вычисления реагирующей системы можно определить в терминах переходов системы. *Вычисление* – это бесконечная последовательность состояний, каждое из которых получено из предыдущего посредством некоторого перехода.

Для формализации наших интуитивных представлений о поведении реагирующих систем мы воспользуемся разновидностью графа переходов, которая называется *моделью Крипке*. *Модель Крипке* состоит из множества состояний, множества переходов между состояниями и функции, которая помечает каждое состояние набором свойств, истинных в этом состоянии. Пути в *модели Крипке* соответствуют вычислениям системы. Хотя модели такого вида очень просты, они достаточно выразительны, чтобы отражать те аспекты *темпорального* поведения, которые наиболее важны для анализа реагирующих систем.

Параллельные системы обычно задаются текстом программы или диаграммой электронной схемы. Существуют различные типы параллельных систем (синхронные и асинхронные схемы, программы с разделяемыми переменными, программы, взаимодействующие путем обмена сообщениями, и т.д.). Ввиду такого разнообразия, нужен универсальный формализм, в рамках которого можно было бы представлять параллельную систему любого типа. Мы воспользуемся для этой цели формулами логики предикатов первого порядка. По формуле, представляющей параллельную систему, легко построить модель Крипке, адекватно соответствующую этой системе.

В этой логике атомарные высказывания и булевы связки, такие как конъюнкция, дизъюнкция и отрицание, используются для построения сложных выражений, предназначенных для описания свойств состояний. В реагирующих системах нас также интересуют описания переходов между состояниями. Это важно, поскольку такие системы взаимодействуют с окружением и реагируют на внешние воздействия. Традиционные методы верификации программного обеспечения, разработанные Флойдом и Хоаром, имеют дело с программами, семантика которых определяется отношениями между входными и выходными данными.

Подробности того, как осуществляется вычисление, никак не отражаются в тех свойствах, которые могут быть специфицированы и доказаны; описываются только входные данные в начале выполнения программы и выходные данные по завершении ее выполнения. Но для реагирующих систем наиболее важна именно последователь-

ность шагов вычисления, и к тому же многие реагирующие системы проектируют так, чтобы их вычисления вообще никогда не завершались.

Темпоральные логики как раз и являются тем формализмом, который предназначен для описания последовательностей переходов между состояниями реагирующей системы. В темпоральных логиках, которые будут рассматриваться нами, время явно не упоминается; вместо этого формулы позволяют записывать утверждения о том, что некоторое выделенное состояние будет когда-нибудь пройдено или что состояние ошибки никогда не будет достигнуто. Свойства, в которых упоминаются события, происходящие когда-нибудь или никогда, специфицируются при помощи специальных темпоральных операторов.

Заключение

В данной статье представлена формальная логика работы модели антивирусного движка на основе метода верификации его модели. Основной целью являлось формирование ясной логической основы для создания верификатора, действующего на основе *Model Checking* – алгоритмы которого базируются на полном просмотре пространства состояний модели: для каждого состояния проверяется, удовлетворяет ли оно сформулированным требованиям. Алгоритмы гарантированно завершаются, так как модель конечна.

Тем не менее, нельзя не отметить, что задача написания полноценного эмулятора является довольно трудоемкой, не говоря уже о том, что при использовании эмулятора приходится постоянно контролировать действия каждой команды. Это необходимо для того, чтобы случайно не выполнить деструктивные компоненты алгоритма вируса. Следует особо отметить, что приходится именно эмулировать работу инструкций вируса, а не трассировать их, поскольку при трассировке вируса слишком велика вероятность вызова деструктивных инструкций или кодов, отвечающих за распространение вируса.

Литература

1. S. Staniford, V. Paxson and N. Weaver. «How to Own the Internet in Your Spare Time» 11th Usenix Security Symposium – San Francisco, August. – 2002. [http://www.icir.org/vern/papers/cdc-usenix-sec02/]
2. The Workshop on Rapid Malcode (WORM), October 27, 2003, The Wyndham City Center Washington DC, USA. [http://pisa.ucsd.edu/worm03/]
3. Кларк Э., Грамберг О., Пелед Д. Верификация моделей программ. – М.: МЦНМО. – 2002.

УДК 004.056

ПРОГНОЗИРОВАНИЕ УЯЗВИМОСТЕЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ ОБЗОРА ХАКЕРСКИХ КОНФЕРЕНЦИЙ

Э.Р. Хусаинова, Ю.А. Торшенко
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Чтобы углубиться в тонкости защиты и взлома, создаются специальные конференции. События состоят из различных выступлений лекторов на тему хакинга. В рамках подобных конференций проводится большое количество конкурсов и соревнований. В данной статье описывается, каким образом изучение материалов подобных конференций может повысить надежность и защищенность информационных систем и программных продуктов.

Ключевые слова: хакерские конференции, прогнозирование атак, защита информации

Введение

Предотвращение компьютерных атак со стороны злоумышленников – очень актуальная задача для специалистов, работающих в IT-сфере. С ростом уровня безопасности снижается число «безобидных» вирусов, не нарушающих штатный режим функционирования ЭВМ, но при этом следует учитывать, что опасные, повреждающие файловую структуру и аппаратуру, вирусы, пишут люди умные, и зачастую им удаётся обходить разработанные компаниями средства защиты информации. Это происходит оттого, что при создании программных систем разработчики спешат и допускают оплошности. Поэтому очень важно устраивать конференции, помогающие прогнозировать возможные угрозы.

Настоящая защита IT зависит от умения и способности бороться с «киберзлоумышленниками» их же методами. Этого можно достичь путем сбора информации, которая будет использована против них во время проведения мероприятий по безопасности, а также с помощью надзора за деятельностью нарушителей и предупреждения их действий. Кроме того, уровень доверия к «инсайдерам» также должен оцениваться очень осторожно. Докладчики делятся своим опытом борьбы с «кибертерроризмом». Они демонстрируют пути устранения основных угроз безопасности и помогают слушателям составить представление о целостной инфраструктуре, где легко реализуются предупреждающие стратегии; так же демонстрируются новейшие решения в области управления информационной безопасностью; участники конференции стремятся опередить злоумышленников и защитить системы от возможных угроз: разрабатываются инструменты, позволяющие определять уязвимые места систем еще до того, как они подвергаются атакам.

Содержание конференций

Чтобы углубиться в тонкости защиты и взлома, создаются специальные конференции. События состоят из различных выступлений лекторов на тему хакинга. Эти конференции являются достаточно популярными, например в 2006 году аудитория DEFCON составила 6500 человек, а впервые она прошла в 1993.

Подобные конференции проводятся ежегодно во многих странах мира (см. табл. 1 и табл. 2).

Название	Проводится с …	Место проведения	Участники	Сайт
DefCon	1993 года, ежегодно	Лас-Вегас	5000чел, Хакеры и сотрудники федеральных спец. Служб [1]	www.defcon.org
LAYER ONE	2004 года, ежегодно	Лос-Анджелес	хакеры, специалисты по безопасности, представители спецслужб [2]	www.layerone.info
H2K2	1994 года, Каждые 3 года [3]	Нью-Йорк	------	www.h2k2.net
Toorcon	1998 года, ежегодно	Сан-Диего	500 человек. Участники-специалисты в компьютерной безопасности [4]	www.toorcon.org
BlackHat	С 1997 г., ежегодно	Вашингтон (а также в Европе и Азии)	хакеры, специалисты по безопасности, представители спецслужб [5]	www.blackhat.com

Таблица 1. Конференции хакеров в США

Название	Проводится с …	Место проведения	Участники	Сайт
CCC (Chaos Communication Congress)	1984 года, ежегодно	Берлин	хакеры, специалисты по безопасности, представители спецслужб [6]	www.ccc.de
What the Hack?	1989 года, каждые 4 года	Нидерланды	хакеры, разработчики open source software и заинтересованные лица	www.whattehack.org
y2hack	2000 года, ежегодно	Израиль, Тель-Авив	хакеры, люди, интересующиеся безопасностью специалисты по безопасности, представители спецслужб	www.y2hack.com
Hack in the Box	с 2003 г., ежегодно	Малайзия, АОЭ, Дубай	хакеры, специалисты по безопасности	www.hackinthebox.org

Power of Community	С 2006 г. ежегодно	Южная Корея	Более 350 чел. хакеры, специалисты по безопасности	www.powerofcommunity.org
CanSecWest	С 2001 г., ежегодно	Ванкувер, Канада	хакеры, специалисты по безопасности	http://cansecwest.com/
PacSec	С 2002 г., ежегодно	Токио, Япония	хакеры, специалисты по безопасности	http://pacsec.jp/index.html
EUSecWest	С 2005 г., ежегодно	Лондон, Англия	хакеры, специалисты по безопасности	http://eusecwest.com/
BA-Con	2008 г.	Буэнос-Айрес, Аргентина	хакеры, специалисты по безопасности	http://ba-con.com.ar/
BlackHat	С 2000 г., ежегодно	2008 г. Амстердам, голландия	хакеры, специалисты по безопасности	www.blackhat.com

Таблица 2. Конференции хакеров в Европе и других странах

Информация как инструмент прогнозирования

Участники конференций – это специалисты по компьютерной безопасности, юристы, хакеры и даже журналисты. Кроме стандартных докладов на тему компьютерной безопасности, здесь проходят множество различных конкурсов. Например, в одном из них участники должны будут обработать вирусный код таким образом, чтобы он смог обойти антивирус. Также обсуждается поднимаются вопросы на тему безопасности современных программ и операционных систем. Так, на одной из конференций обсуждалась проблема конфиденциальности программы для совершения телефонных разговоров Skype, а также уязвимость последней операционной системой Windows Vista.

Участники конференции получают уникальную возможность в сжатой и ясной форме ознакомиться с современными теориями и концепциями, методами и технологиями анализа уязвимости объектов, оценки эффективности систем безопасности, получившими мировое признание в практике построения систем защиты и организации охраны различных объектов.

В программе конференций:

– Цели, задачи и базовые принципы построения системы безопасности объекта. Структурные компоненты системы безопасности и их взаимодействие.

– Методика организации работ по проведению анализа уязвимости. Аудит системы безопасности.

– Основные этапы проведения анализа уязвимости, аудита системы физической защиты объекта.

– Аудит безопасности информационных систем.

– Выявление жизненно важных целей и предметов защиты предприятия, организации, объекта.

– Угрозы объекту и его жизненно-важным центрам – терминология, классификация возможных угроз и последствий их реализации. Разработка модели угроз.

– Разработка модели нарушителя. Моделирование сценария, тактики действий нарушителей, реализации угроз.

– Категорирование объектов

– Оценка эффективности и выработки предложений по модернизации системы безопасности.

– Оценка эффективности организационных мероприятий административных решений, тактики и организации сил охраны и разработка предложений по их совершенствованию.

– Оформление результатов анализа уязвимости; оценка.

– Управление информационной безопасностью.

Детальный анализ подобной информации является мощным инструментом прогнозирования и помогает решить многие проблемы адаптации и совершенствования методов защиты информационных систем и программного обеспечения.

Заключение

Современные форумы помогают специалистам в области компьютерной безопасности обмениваться опытом и выводить новые способы защиты, в том числе и на основе старых. Здесь объединяются не только защитники, но и взломщики. Вечные враги объединяются и раскрывают друг перед другом все карты. Хакеры соревнуются друг с другом и делают это законно, не нанося вред. Ведь, в конечном счете, каждый пользователь сети будет вычислен по IP адресу, поэтому виновные будут всегда наказаны. Именно здесь раскрываются темы, такие как настройка безопасности web-сайтов, оптимизация web-браузеров. Ведь кроме проблемы взлома и воровства информации ради собственной выгоды, существуют вредоносные программы, которые не несут прямой выгоды ее автору, а только моральное удовлетворение. Такие программы чаще всего являются безвредными, но есть и те, что несут за собой искажение и уничтожение информации. Таким образом, подобные конференции, сплачивают людей и, когда новые идеи за год уже истощились, как бы подталкивают защитников на создание новых методов и подходов к защите.

Литература

1. Сайт конференции DefCon [Электронный ресурс] / 2008. – Режим доступа: www.defcon.org, свободный. – Яз. англ.
2. Сайт конференции LAYER ONE [Электронный ресурс] / 2008. – Режим доступа: www.layerone.info, свободный. – Яз. англ.
3. Сайт конференции H2K2 [Электронный ресурс] / 2006. – Режим доступа: www.h2k2.net, свободный. – Яз. англ.
4. Сайт конференции Toorcon [Электронный ресурс] / 2008. – Режим доступа: www.toorcon.org, свободный. – Яз. англ.
5. Сайт конференции BlackHat [Электронный ресурс] / 2008. – Режим доступа: www.blackhat.com, свободный. – Яз. англ.
6. Сайт конференции Chaos Communication Congress [Электронный ресурс] / 2008. – Режим доступа: www.ccc.de, свободный. – Яз. англ., нем.

УДК 004.056.57

МЕТОД ВОЗМОЖНОСТНОЙ КОРРЕЛЯЦИИ СОБЫТИЙ БЕЗОПАСНОСТИ ДЛЯ ПОСТРОЕНИЯ ВЕКТОРА АТАКИ

И.В. Головков
Научный руководитель – к.т.н., доцент А.В. Птицын

Анализ событий безопасности, обнаружение и предотвращение вторжений являются одними из краеугольных камней обеспечения информационной безопасности в информационных системах. Дальнейшее развитие методов обработки событийной информации сможет позволить не только выявлять и предотвращать такие нежелательные воздействия, но и прогнозировать их распространение.

Ключевые слова: анализ, событие, безопасность, обнаружение, корреляция, прогнозирование

Введение

С увеличением числа применяемых в организации информационных технологий растет и количество используемых средств защиты. В связи с этим, задача сбора, анализа и контроля событий информационной безопасности становится все более актуальной.

События (далее также записи) безопасности генерируются различными средствами и подсистемами обеспечения безопасности – маршрутизаторами, межсетевыми экранами, системами обнаружения и предотвращения вторжений, антивирусными системами – и информируют о возможном нарушении политики безопасности, будь то сканирование сетевых портов, атаки отказа обслуживания, эпидемии сетевых вирусов либо внутренние нарушения. Чем масштабнее информационная система и чем агрессивнее окружающая ее среда, тем больше событий поступает от средств защиты, тем сложнее произвести их анализ, выдать соответствующее управляющее воздействие и проконтролировать его выполнение. В крупномасштабных системах часть функций по сбору, обработке и анализу событий безопасности возложены на специализированные комплексы, так называемые системы управления информационной безопасностью (Security Information Management System, SIMS). SIMS позволяют переложить с администратора часть задач по обработке записей, таких как [1]:

(а) Консолидация – сбор и централизованное хранение;

(б) Фильтрация – отсеивание событий, не относящихся к безопасности;

(в) Нормализация – устранение избыточности, появляющейся в связи с повторением одного и того же события от разных устройств;

(г) Агрегирование – группирование однотипных событий;

(д) Корреляция – выявление взаимосвязи между разнородными событиями от различных устройств, приложений и систем безопасности;

(е) Приоритезация – выставление значимости и критичности произошедшего события или группы событий на основании как предустановленных в системе правил, так и на основании разработанных и настроенных критериев.

Метод возможностной корреляции

Ключевым моментом при обработке событий безопасности является их корреляция, так как именно на данном этапе определяется взаимосвязь событий от различных источников, происходит логический переход от группы взаимосвязанных событий к понятию мета-событие, идентифицируется принадлежность мета-события к инцидентам. Фактически, именно на этапе корреляции определяется, является ли

событие частью воздействия на информационную систему, нарушающего политику безопасности.

Существующие методы корреляции работают с фактами, т.е. случившимися событиями, что позволяет получить достоверную картину воздействия на информационную систему (рис. 1).

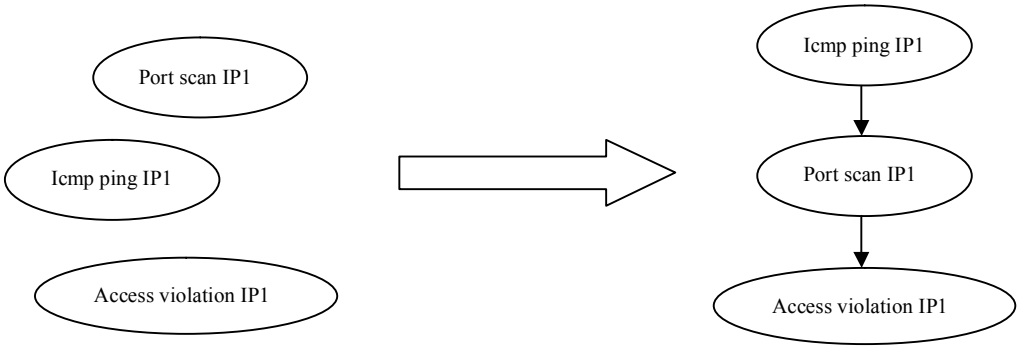


Рис. 1. Корреляция событий

Однако именно по тому, что при обработке участвуют только фактические события, возможность прогнозирования у данных методов отсутствует.

Метод возможностной корреляции событий безопасности основан на построении предположений о возможном состоянии системы в следующие моменты времени за возникновением события безопасности, осуществляя выбор дальнейших фактов (воздействий) из информации о системе и базы знаний (общего возможного множества воздействий на систему).

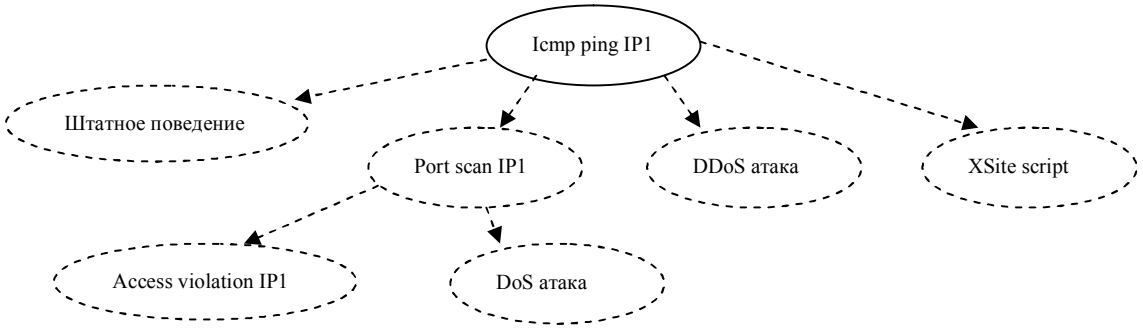


Рис. 2. Общее поле возможных состояний системы

Дальнейшая обработка общего поля возможных состояний системы заключается в следующем:

(1) Выбор наиболее вероятного вектора перехода состояния (прогнозирование).

(2) Обработка новых фактов (событий) и исключение из общего поля состояния системы, векторов, неудовлетворяющих фактам (сужение области воздействия на систему или подтверждение прогноза).

Заключение

Метод возможностной корреляции событий предназначен для прогнозирования вероятных векторов атак на информационную систему. Дальнейшая работа по данному направлению заключается в подключении математического аппарата для формализации механизмов выбора векторов атак.

Литература

1. Лукацкий А.В. Корреляция на службе безопасности // Журнал BYTE. – 2003. – №10.

УДК 004.725.7

АНАЛИЗ МЕТОДОВ ОРГАНИЗАЦИИ ТРАНЗИТНЫХ ПОТОКОВ ДАННЫХ ПРОВАЙДЕРАМИ

Д.А. Алексеев
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

Целью исследования является разработка адаптивной системы управления динамикой транзитных провайдеров в режиме реального времени в сети Internet. В настоящей статье рассматриваются методы организации транзитных потоков данных провайдерами российского сегмента Internet на основе протоколов внешней маршрутизации.

Ключевые слова: методы взаимодействия, транзитные потоки данных, внешняя маршрутизация

Введение

Основная задача сетей – организация потока данных от компьютера отправителя к компьютеру получателя. В большинстве случаев поток данных будет проходить через транзитные узлы. Проблему выбора транзитных узлов решают алгоритмы маршрутизации. Если транспортировка данных осуществляется по протоколу, не требующему подтверждений о доставке пакетов, для каждого пакета эта задача решается независимо. В случае организации виртуальных соединений определение транзитных узлов осуществляется на этапе формирования этого соединения. В Интернет в случае протокола UDP реализуется первый вариант (исключением являются виртуальные сети), а в сетях ISDN и ATM – второй. Специальные устройства, решающие вопросы маршрутизации, называются маршрутизаторами [1].

Структура провайдеров

Internet организован как сообщество автономных систем, каждая из которых обычно администрируется независимо от остальных. Магистраль (backbone) NSFNET с точки зрения Internet это автономная система, так как все маршрутизаторы, входящие в состав магистрали, управляются в пределах одного административного контроля. Автономные системы подразделяются на транзитные, многоинтерфейсные и ограниченные автономные системы [2]. Для каждой автономной системы выбирается собственный протокол маршрутизации, с помощью которого осуществляется взаимодействие между маршрутизаторами в этой автономной системе.

- Транзитная автономная система соединяется с несколькими автономными системами и согласно ограничений пропускает локальные и транзитные потоки данных.
- Многоинтерфейсная автономная система соединяется с несколькими автономными системами, но не пропускает транзитные потоки данных.
- Ограниченная автономная система соединяется только с одной внешней автономной системой. Данная автономная система пропускает только локальные потоки данных.

Многоинтерфейсные и ограниченные автономные системы для передачи данных используют только протоколы внутренней маршрутизации. В транзитных автономных системах для передачи транзитных потоков данных и взаимодействия с другими автономными системами необходимо использовать протоколы внешней маршрутизации.

Из протоколов внешней маршрутизации можно выделить EGP – exterior gateway protocols и BGP – Border Gateway Protocol [3].

Системы, в которых используется протокол BGP, обмениваются сведениями о доступности сети с другими системами, поддерживаемыми данный протокол. Эти сведения включают в себя путь по автономным системам, по которым необходимо

пройти потоку данных от сети-источника к сети-получателю. Эти сведения используются при построении графа соединений автономных систем.

BGP позволяет использовать маршрутизацию на основе предопределенной политики (policy-based routing). Все правила политики задаются администратором автономной системы в конфигурационных файлах протокола. Политика не входит в состав протокола, однако предоставляет возможность выбора между маршрутами в случае, когда существуют альтернативные маршруты, а также позволяет управлять перераспределением потоков данных. Правила политики определяются в соответствии с вопросами безопасности информации или экономической выгоды и конкурентоспособности.

Транзит потоков данных

При организации передачи потоков данных важно разделять локальные и транзитные потоки данных. В случае если источник и получатель потока находятся в пределах одной автономной системы он классифицируется как локальный. Все остальные потоки данных классифицируются как транзитные.

Транзит потоков данных провайдерами осуществляется на основе маршрутизации. Маршрутизация представляет два параллельных процесса: формирование таблицы маршрутов и передача пакетов данных в соответствии с записями этой таблицы. Формирование таблицы маршрутов осуществляется с использованием протоколов маршрутизации или путем инструкций администратора.

Метод организации транзитных потоков должен обладать определенными свойствами: стабильностью, надежностью, простотой и оптимальностью. Свойство оптимальности не так ясно, как это может показаться вначале, оно зависит от параметров, по которым выполняется оптимизация [4]. Эта задача порой находит нетривиальные решения даже в условиях сравнительно простых локальных сетей (например, рис.1).

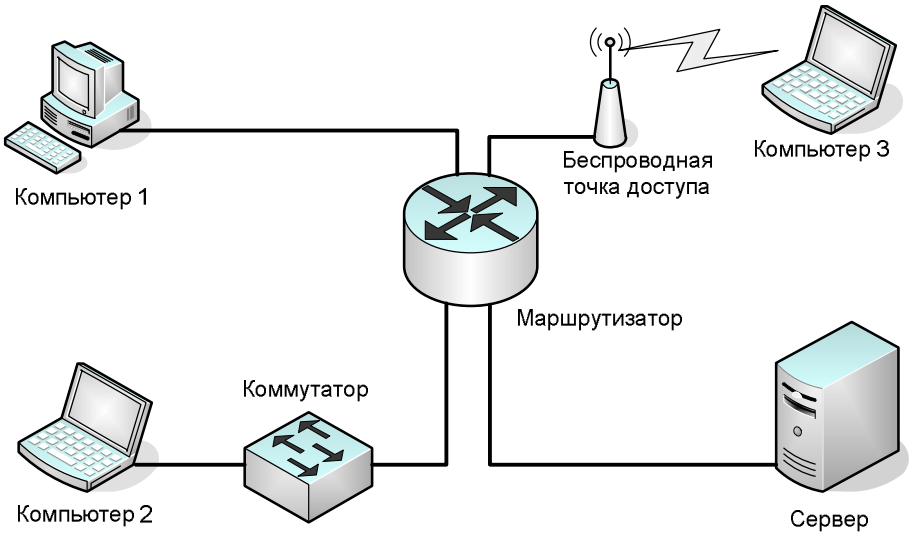


Рис. 1. Схема локальной сети

Предположим, что поток данных между компьютером 3 и сервером, соединенных через маршрутизатор весьма интенсивен, что значительно повлияет на обмен между компьютерами 1 и 2. Но эту ситуацию затруднительно установить на компьютере 1 или 2. Проявляется это только в виде увеличившейся задержки и снижении пропускной способности транзита компьютеров 1–2.

Методы организации транзитных потоков могут быть адаптивными и неадаптивными. Неадаптивные методы, осуществляя выбор транзитных узлов, не учитывают имеющуюся в настоящий момент топологию или загрузку каналов. Такие методы на-

зываются также статическими. Адаптивные методы подразумевают периодическое измерение параметров каналов и регулярное исследование топологии транзитных узлов. Выбор того или иного транзитного узла осуществляется на основании этих измерений.

Российский сегмент Internet, с точки зрения пиринговых отношений, фактически разделен на две части – «Ростелеком», «МТУ-Интел», «Голден Телеком» и все остальные провайдеры (рис. 2). Значительная часть российских транзитных потоков данных между этими частями российского сегмента Internet передаются через Европейских провайдеров, что регулярно становится причиной затруднений в обмене данными между сетями противоположной части провайдеров.

В данном случае под пирингом понимается взаимовыгодный бесплатный обмен потоками данных между двумя и более провайдерами. Под пиринговыми соглашениями понимаются соглашения о таком обмене потоками данных.

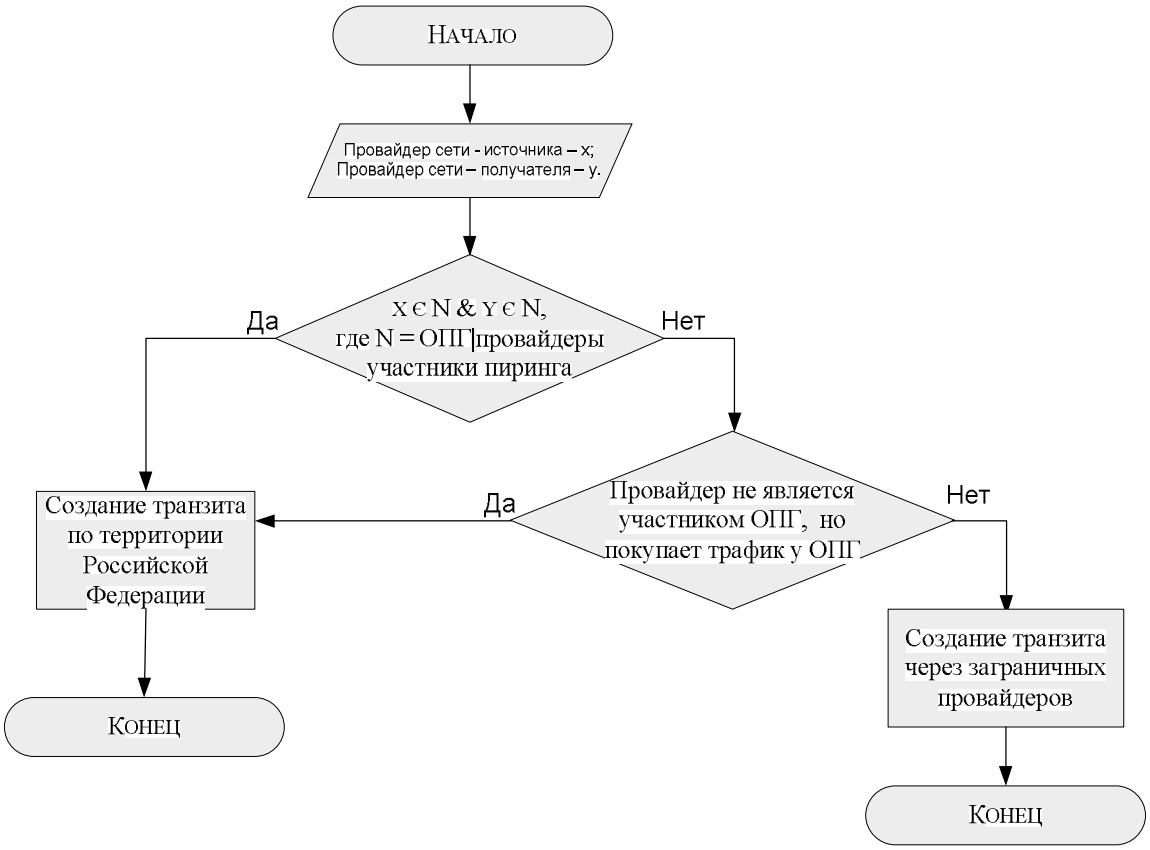


Рис. 2. Блок-схема алгоритма организации транзита провайдерами на территории Российской Федерации

В среде провайдеров союз «Ростелеком», «МТУ-Интел», «Голден Телеком» обозначают как ОПГ (отдельная пиринговая группа, отделившаяся пиринговая группа). Между провайдерами ОПГ заключено соглашение, покоторому они бесплатно обмениваются потоками данных между собой, но просят плату за транзит с остальных провайдеров.

Заключение

Таким образом, в статье рассмотрены и проанализированы методы организации транзитных потоков данных провайдерами. Оптимизация существующих и разработка собственных подходов к организации управления транзитными потоками данных позволит повысить безопасность передаваемых данных.

Литература

1. Спортак Марк А. Компьютерные сети. Книга 2: Networking essentials. Энциклопедия пользователя. К.: «Диа Софт» . – 1999. – 432 с.
2. Семенов Ю.А. Протоколы и ресурсы Интернет. – М.: Радио и связь. – 1996.
3. Lougheed, K., and Rekhter, Y. 1991. A Border Gateway Protocol 3 (BGP-3). – RFC 1267. – PP. 35 (Oct.).
4. Хелеби С., Мак-Ферсон Д. Принципы маршрутизации в Internet. – М.: изд. дом «Вильямс». – 2001. – 448с.

УДК 004.75:004.772

БЕЗОПАСНОЕ ХРАНЕНИЕ ИНФОРМАЦИИ В ГЛОБАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Д.А. Пикулькин, А.А. Ловыгин
Научный руководитель – к.т.н., доцент А.Г. Карманов

Целью исследования является, разработана методика, которая позволяет безопасно хранить и передавать данные в глобальных вычислительных сетях. В методике применяются технологии усложнения пользовательского пароля, которая позволяет уменьшить вред от применения простых пользовательских паролей, методика распределённого хранения информации, которая позволяет значительно повысить надёжность всей системы и способствует её защищенности. Кроме того применена технология обезличивания, которая позволит сохранить конфиденциальность зашифрованного документа даже в том случае, если злоумышленнику удастся получить доступ к серверам и списку файлов на них. В результате всего этого планируется получить систему хранения и передачи файлов, которая отвечает основным требованиям к доступности целостности и конфиденциальности информации.

Ключевые слова: информационная безопасность, безопасность, распределенные системы, шифрование, хранение информации

Введение

Проблемы, решаемые в этой работе, делятся на 3 аспекта.

Целостность – разработка алгоритма для контроля целостности хранимой и передаваемой информации на основе хэш-функций.

Для каждого фрагмента файла сервер возвращает клиенту универсальный хэш-идентификатор, который сверяется с хэш-идентификатором, который находится у клиента. При совпадении этих хэш-идентификаторов файл записывается на хранение на сервере с именем хэш-идентификатора, а сам хэш-идентификатор записывается в ключ клиента для возможности дальнейшего обращения к сохраненному фрагменту файла на сервере при операции восстановления файла.

Доступность – разработка методики хранения информации, предусматривающей избыточность хранимой информации для повышения ее доступности в случае неработоспособности части серверов хранения информации [1].

При сохранении файл разбивается на 4 части. В комбинациях по 2 части эти фрагменты файла рассылаются на 6 из 9 серверов хранения таким образом, что на каждом из 6 серверов находятся одновременно 2 части файла. То есть для восстановления файла достаточно 2–3 серверов [6].

Конфиденциальность – комбинация алгоритмов шифрования, разделения и обезличивания информации позволит с достаточной долей уверенности сказать, что злоумышленник, не имея изначальных данных о файле, не сможет его полностью восстановить [2].

Исходный файл после преобразования разделяется случайным образом на 4 фрагмента, каждый из которых шифруется.

Шифрование каждого фрагмента происходит при помощи md5-хэша пользовательского пароля.

Каждый фрагмент файла имеет свой уникальный размер, который почти не зависит от размера исходного файла. И при хранении практически не имеет имени, несущего смысловую нагрузку (имя соответствует хэш-идентификатору фрагмента).

У пользователя хранится только зашифрованный список хэш-идентификаторов, список серверов, на которых хранятся фрагменты файла, имя исходного файла и остаточная служебная информация для восстановления файла [1].

Шифрование

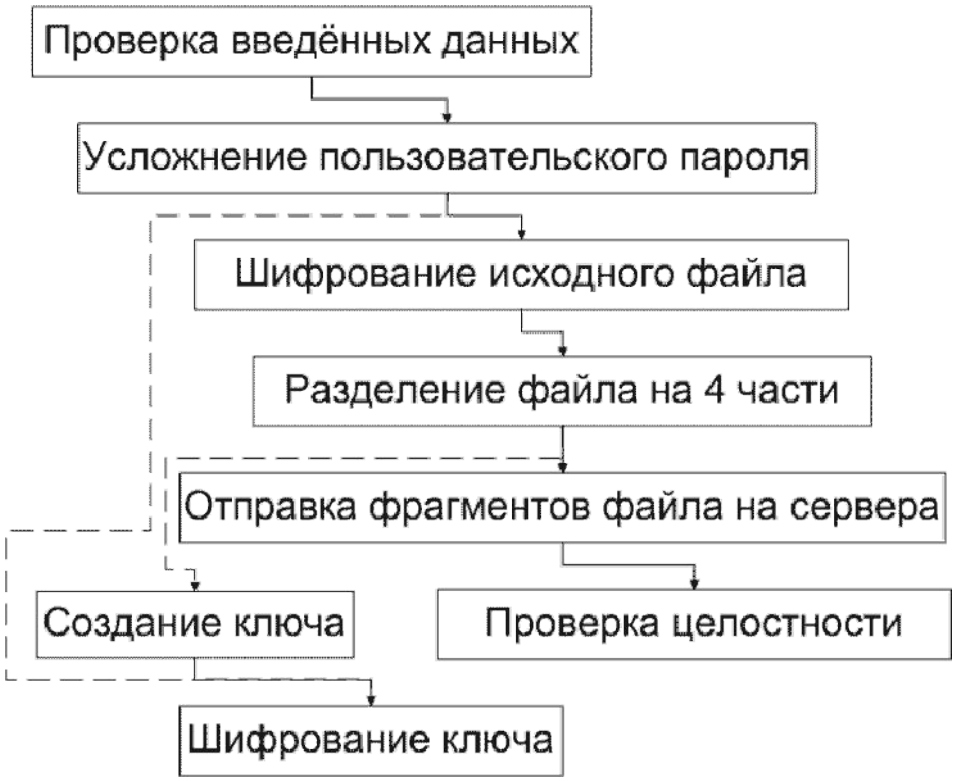


Рис. 1. Шифрование

1) На вход программе подаётся 3 параметра: путь к шифруемому файлу, путь куда следует записать ключевой файл и пароль для шифрования.

2) Все эти параметры проверяются:

- должна быть возможность прочитать исходный файл;
- должна быть возможность записи ключа в указанный файл (папку);
- пароль не должен быть пустым.

3) Происходит усложнение введённого пароля [6]:

- представляем пользовательский пароль в бинарном виде;
- находим биты, которые неизменны во всех байтах пароля (такое происходит в том случае, когда пароль набран на одном языке или состоит только из цифр);
- исключая биты, найденные в прошлом пункте, составляем «маску уникальности», которая показывает, какие биты в пароле менялись от байта к байту; берутся биты по маске уникальности, записываются подряд, а затем к ним побитово дописывается исходный пользовательский пароль. Это не только позволяет увеличить пользовательский пароль сам по себе, но ещё и усложняет его нестандартными символами: редко количество бит взятых по маске уникальности кратно 8, что означает практическое отсутствие символов пользовательского пароля в получившемся пароле;
- если после всех этих преобразований количество символов недостаточно (в примере указано 16 символов), то производим преобразование полученного усложнённого пароля при помощи одностороннего шифрования.

4) Размешиваем файл: побайтно записываем его в 4 разных массива и собираем эти массивы обратно в одну строку. (0123456789->048,159,26,37->0481592637).

5) Шифруем обратимым шифром исходный текст, где ключом будет выступать изменённый пользовательский пароль (0481592637->AEIBFJCGDH) [7].

6) Разделяем полученный зашифрованный исходный текст на 4 части случайным образом. (AEIBFJCGDH->AEI,BFJC,GD,H) [6].

7) Записываем получившееся в отдельные файлы.

8) Вычисляем хэш идентификатор для каждого из этих файлов. (хэш-идентификатор – это контрольная сумма файла, т.е. функция от содержимого и размера файла) [6].

9) Файлам с фрагментами исходного текста присваивается имя его хэш-идентификатора.

10) Определяется список серверов, на которые будут направлены фрагменты файла [5].

– Для обеспечения избыточности в примере используется 6 серверов, но при разделении файла не на 4 фрагмента количество серверов может меняться.

– В примере фрагменты размещаются на 6 из 8 серверов. Общее количество серверов может меняться свободно, но желательно не делать их значительно больше, чем серверов непосредственного размещения.

– Фрагменты распределяются на серверах таким образом, что файл невозможно восстановить с одного сервера, но возможно восстановить с минимального количества серверов (на случай недоступности части из них)

– естественно, что сервера выбираются случайным образом, а не идут по порядку

11) Согласно списку фрагменты исходного файла распределяются по серверам. При этом очень важно исключить аудит этой операции: не должно быть иной возможности восстановить, из каких фрагментов состоял исходный файл. Так же желательно на сервере убрать с файла временные метки, чтобы даже при доступе к серверу невозможно было определить по времени пары фрагментов файла, хранящихся на сервере [4].

12) После окончания загрузки сервер должен проверить хэш-идентификаторы полученных файлов и сверить с названиями файлов (хэш-идентификаторами, которые предоставил клиент). При совпадении идентификатора файл отправляется на хранение, а клиент получает об этом уведомление. Если хэш-идентификатор отличается от заявленного, клиенту передаётся соответствующее сообщение и клиент повторяет передачу. Если и второй раз хэш-идентификатор не совпал, то клиент заново вычисляет хэш-идентификатор файла и передаёт его на сервер [7].

13) Клиент записывает в свой ключевой файл хэш-идентификаторы всех четырёх частей файла по порядку.

14) Затем шифрует ключевой файл обратимым шифром, в котором ключом будет усложнённый пользовательский пароль [7].

15) На выходе мы имеем 1 ключевой файл, который хранится у пользователя и 4 зашифрованных фрагмента исходного файла на серверах

Дешифрование

1) На вход программе подаётся 3 параметра: путь к дешифрованному файлу, путь к ключевому файлу и пароль для дешифрования.

2) Все эти параметры проверяются:

– должна быть возможность прочитать ключевой файл;

– должна быть возможность записи дешифрованного файла в указанный файл (папку);

– пароль не должен быть пустым.

3) Происходит усложнение введённого пароля [6]:

– представляем пользовательский пароль в бинарном виде;

– находим биты, которые неизменны во всех байтах пароля (такое происходит в том случае, когда пароль набран на одном языке или состоит только из цифр);

– исключая биты найденные в прошлом пункте составляем «маску уникальности», которая показывает, какие биты в пароле менялись от байта к байту;

– берутся биты по маске уникальности, записываются подряд, а затем к ним побитово дописывается исходный пользовательский пароль. Это не только позволяет увеличить пользовательский пароль сам по себе, но ещё и усложняет его нестандартными символами: редко количество бит взятых по маске уникальности кратно 8, что означает практическое отсутствие символов пользовательского пароля в получившемся пароле;

– если после всех этих преобразований количество символов недостаточно (в примере указано 16 символов), то производим преобразование полученного усложнённого пароля при помощи одностороннего шифрования.

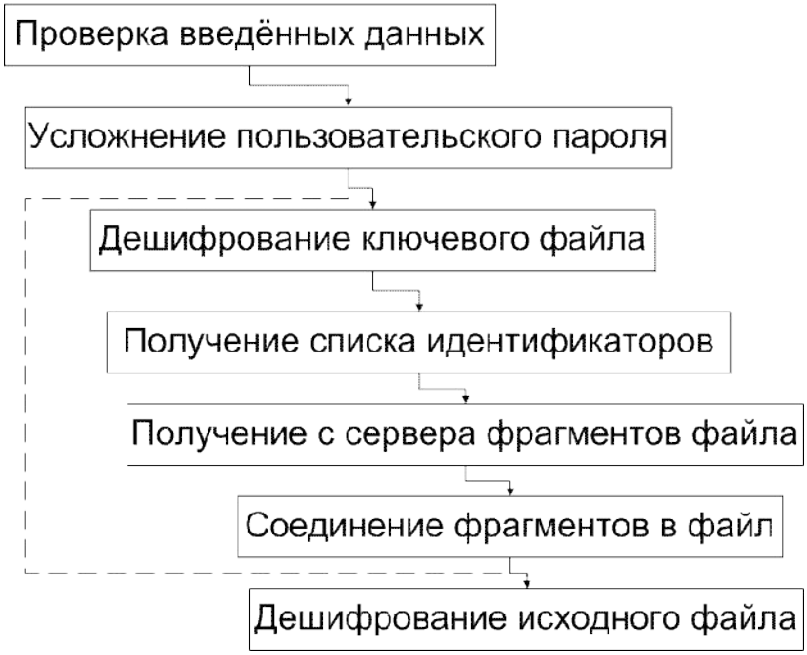


Рис. 2. Дешифрование

4) При помощи обратимого шифра расшифровываем ключевой файл при помощи усложнённого пользовательского пароля [7].

5) Полученный из ключевого файла список файлов запрашиваем на серверах, пока не получаем все 4 фрагмента файла [5].

6) Соединяем файл в порядке указанном в ключе и расшифровываем его при помощи усложнённого пользовательского пароля [4].

7) Восстанавливаем исходный порядок символов в расшифрованном тексте.

8) Записать результат в указанный файл.

Вывод

В результате разработки методики были решены следующие задачи:

Контроль целостности производится на стороне сервера и на стороне клиента при помощи хэш-идентификаторов, которые допускают ошибку целостности с вероятностью 0,00000000000000000000000827%.

Обеспечение доступности происходит благодаря системе избыточного распределения фрагментов зашифрованной информации по серверам таким образом, что в предложенном варианте методики шанс доступности информации в данную конкретную минуту равен 99,999996%.

И только конфиденциальность всё ещё зависит от человеческого фактора. Минимальная близость шифра к идеальному (в отношении ключа) – 20% и достижение идеального шифра возможно. Плюс к тому использование нетривиального алгоритма, который при необходимости возможно изменить, а значит для организации прямого перебора либо придётся использовать тривиальные алгоритмы с неприемлемо большим набором вариантов, либо использовать более сложные алгоритмы каждый раз, что во-первых значительно увеличит время на подбор каждого варианта, а во-вторых не даст гарантии нахождения правильного варианта. Тем более, что при работе с шифрами близкими к идеальному прямой перебор начинает терять смысл.

Кроме того, этот алгоритм достаточно обладает достаточной гибкостью и может быть изменён в любой момент в соответствие с потребностями данной конкретной системы.

Литература

1. Гроувер Д. Сатер Р. Защита программного обеспечения. – М.: Мир. – 1992.
2. Левин М. E-mail ‘безопасная’». – М.: Майор. – 2000.
3. Мак-Клар С. Скембрей Д. Безопасность сетей – готовые решения. – М.: Вильямс. – 2001.
4. Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб: БХВ-Петербург. – 2003.
5. Осовецкий Л.Г. Немолочнов О.Ф. Основы корпоративной теории информации. – СПб: Университетские Телекоммуникации. – 2004.
6. Пикулькин Д.А. Методика распределенного защищенного хранения информации // Информационная безопасность регионов России (ИБРР-2007). – Санкт-Петербург. – 2007.
7. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – СПб: БХВ-Петербург. – 2007.

УДК 600-699.69

СИСТЕМЫ РАСПРЕДЕЛЕННОГО ХРАНЕНИЯ ДАННЫХ: АСПЕКТЫ БЕЗОПАСНОСТИ

В.Д. Стремоухов
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В статье рассмотрены основные аспекты защиты систем распределённого хранения данных, такие как сохранение целостности виртуальной файловой системы, защиту от DDoS-атак, оптимизацию хранения данных в рамках распределённого кластера.
Ключевые слова: РХД, IFS

Введение

Необходимость хранения больших объёмов данных вынуждает создавать распределённые хранилища, на определённом уровне абстракции представляющие собой как бы 1 непрерывное хранилище. Связь модулей такой системы осуществляется как правило при помощи сетевых протоколов под управлением единого координатора, что создаёт предпосылки для существования ряда уязвимостей, таких как DDoS-атаки, непроизвольное забивание отдельного канала, нарушение целостности IFS и т.п. Данная статья посвящена созданию системы распределённого хранения данных, оптимального с точки зрения защищённости.

Основная часть

Понимание IFS

1. Каждый объект хранения данных (файл) имеет уникальный n-битный идентификатор. Доступ к любому объекту данных осуществляется на основе простого интерфейса основанного на этом идентификаторе, состоящего из («объекта»; длины блока данных (файла)) (рис. 1).

2. Структура и типы объектов: Root – определяет само устройство хранения (номер модуля, номер диска модуля, атрибуты диска – общий размер, объем свободного места). Group – определяет директорию, хранящую набор объектов. User – содержит непосредственно данные пользовательского приложения.

Объект User – является непосредственным хранилищем для данных так и для атрибутов двух типов (рис. 2):

Данные – эквивалент данным в файле для традиционных систем. Для доступа используются традиционные команды: Open, Close, Read и Write.

Атрибуты хранения (Storage Attributes) – эти атрибуты используются устройством хранения для управления размещением данных на уровне блока. Включают в себя идентификатор объекта, указатели на блоки, логическую длину, использованную емкость.

Пользовательские атрибуты – эти атрибуты скрыты для устройства хранения и используются ПО и IFS для хранения высокоуровневой информации об объектах. Эти атрибуты могут включать в себя информацию файловой системы о владельце, а также информацию о контроле доступа (ACL). Атрибуты могут описывать уровень качества обслуживания (QoS), применяемый непосредственно к объекту. Эти атрибуты могут содержать информацию о RAID-уровне, размер квоты или характеристики производительности, необходимые для работы с данными.

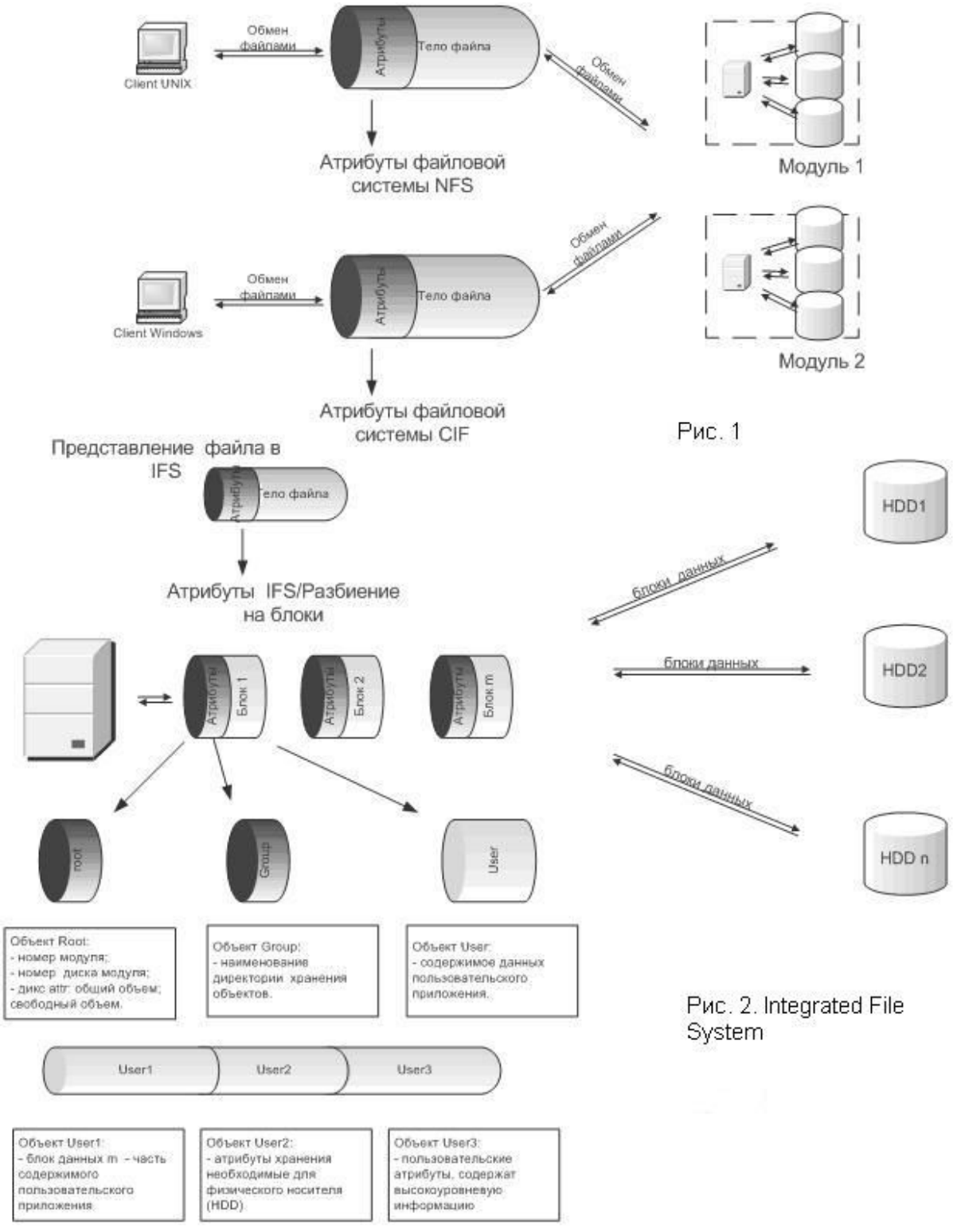


Рис. 1

Рис. 2. Integrated File System

Функции управления хранилищем

1. ПО должно выполнять функции:

– Подключение/удаление новых Модулей.

– Создание/удаление новых виртуальных томов на базе HDD.

– Подключение/удаление HDD к виртуальному тому.

– Выбор/изменение уровня RAID тома.

– Создание/удаление вложенных папок в случае CIF.

– Операции удаления, перемещения, копирования папок и файлов в случае CIF.

– Создание/удаление вложенных папок в случае NFS.

– Операции удаления, перемещения, копирования папок и файлов в случае NFS.

2. Управление политиками доступа хостов к томам, папкам и файлам.

3. Понимание оптимизации управления и размещения данных.

– 10.1.1 ПО должно содержать систему управления оптимальным размещением информации. Под этим понимается:

– Оптимизация распределения данных/блоков на дисках в целях обеспечения скорости доступа к данным.

– ПО предоставляет Администратору возможность выбрать уровень RAID для обеспечения требуемого уровня скорости доступа к данным + надежность их хранения.

IFS RAID 0 – распределение блоков данных по всем HDD Модулей входящих в конфигурацию виртуального тома на котором считываются или записываются блоки данных.

IFS RAID1/10 – распределение блоков данных с организацией зеркал на уровне Модулей или виртуальных томов (с учетом соблюдения симметрии в виртуальных томах дисков на каждом из Модулей пары); с возможностью создания зеркальных пар дисков внутри Модуля. Предусмотреть возможность создания N-го количества пар в системе.

IFS RAID5 – распределение блоков данных с циклическим распределением четности по всем дискам виртуального тома Модуля.

– ПО предоставляет возможность задать оптимальный размер блока на которые дробится исходный файл в зависимости от размера файла.

– ПО позволяет задать минимальный размер исходного файла, который не подлежит разбиению на блоки.

– ПО позволяет задать автоматический режим оптимизации распределения блоков принятых файлов в зависимости от загрузки каждого Модуля или виртуальных томов всей системы – приоритет менее загруженных.

– ПО позволяет выбрать автоматическую оптимизацию уже сохраненных данных/блоков в зависимости от частоты обращения к ним (перераспределение блоков файлов на Модули с меньшей загрузкой ЦП, RAM кэша, нагрузки на диски, свободного объема) [1].

– ПО позволяет выбрать ручной режим назначения приоритетных Модулей или виртуальных томов для хранения данных определенного типа или от определенных хостов пользователей.

– ПО позволяет автоматически распределять нагрузку по сети между Модулями (в зависимости от: загруженности сетевых интерфейсов; загрузки ЦП модулей; от нагрузки на диски)

4. ПО позволяет создавать виртуальные тома как в рамках одного Модуля, так и на нескольких Модулях (Виртуальный том – это объединение дисков одного или нескольких Модулей).

– Каждая часть виртуального тома в рамках Модуля может иметь свой уровень IFSRAID.

– Виртуальный том может состоять из любого набора комбинаций типовIFSRAID.

– ПО позволяет «на лету» увеличивать/уменьшать размер виртуального тома за счет добавления/изъятия дисков Модулей, добавления/удаления новых Модуле [2].

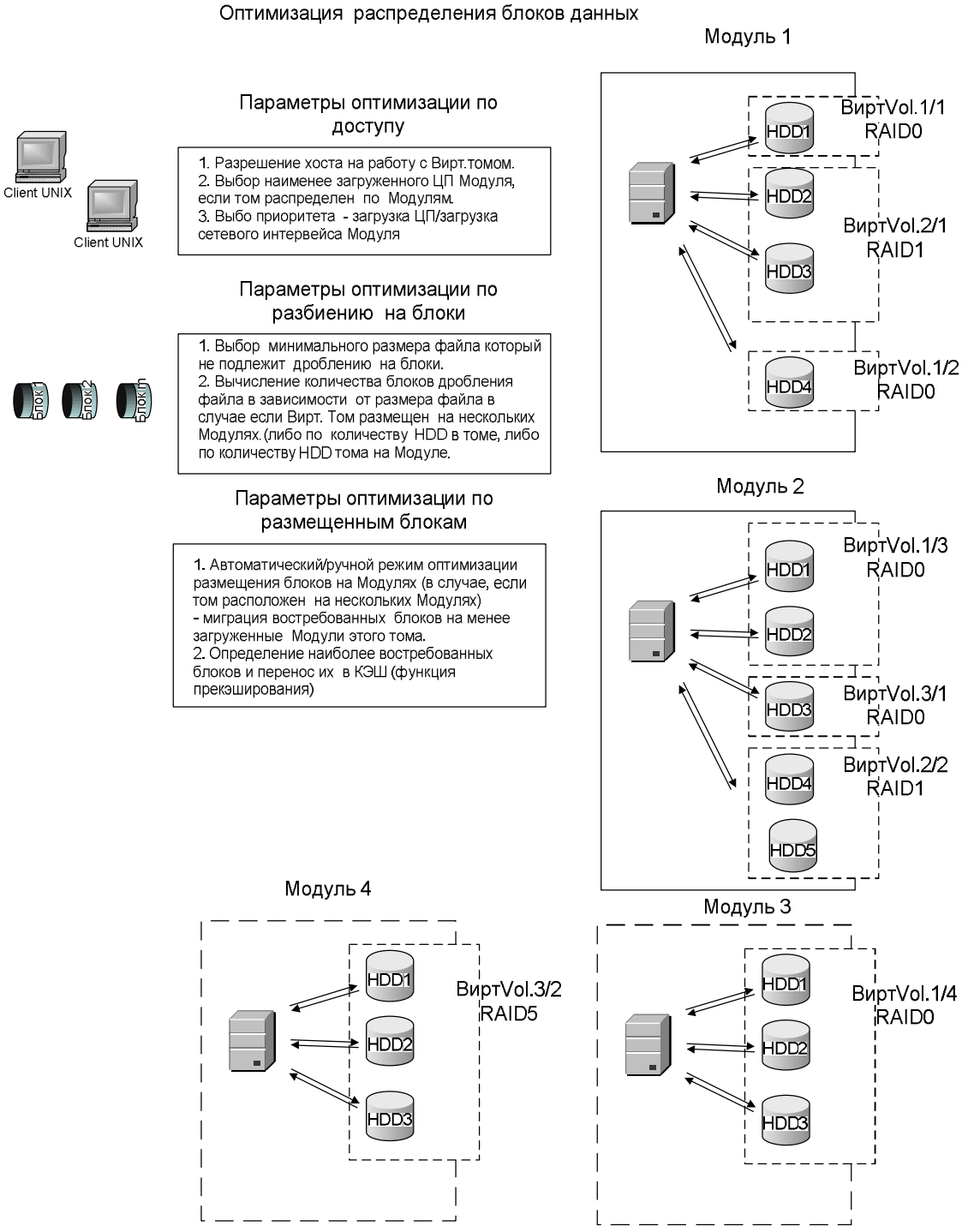


Рис. 3. Модули IFS

Заключение

В рамках проекта разработано ТЗ и принципиальная схема описанного ПО, написана система РХД, которая в настоящее время проходит нагрузочное тестирование.

Литература

1. Е. Касперский Вирусы и средства борьбы с ними. – М. – 2005.
2. Крис Касперски. Образ мышления – дизассемблер IDA. – М.: СОЛОН-Р. – 2001.
3. Крис Касперски. Техника сетевых атак. – М.: СОЛОН-Р. – 2001.
4. Хакер. Спец-выпуск [anti]cracking. – 2005. – № 57.

УДК 681.3

КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ЭЛЕКТРОННЫХ НОСИТЕЛЯХ

А.В. Клеймёнов
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В данной работе рассмотрены основные принципы, необходимые при создании криптосистемы, главной задачей которой будет являться в первую очередь защита информации. Рассматриваются недостатки существующих программных решений в данной области и предлагаются пути их исправления. На основании всех этих данных будут приведены общие и конкретные алгоритмы реализации данного проекта.

Ключевые слова: криптографические системы, электронные носители, криптоалгоритмы, атаки, программная реализация, алгоритм шифрования, драйвер-фильтр

Введение

Криптографические системы представляют собой особое направление в защите информации. В первую очередь, его уникальность определяется огромным числом функций, которые можно реализовать на его основе. В частности, это и защита хранимых данных на физических носителях – секретных, личных, составляющих коммерческую или государственную тайну. Это и необходимость передачи секретных сведений с уверенностью, что даже перехваченные данные не принесут врагу никакой пользы. Это и защита от вредоносного кода, который будет неспособен стабильно выполнять свои функции в защищаемой среде, также будет невозможна какая-либо шпионская деятельность. Сфера применения поистине огромна. Отдельную категорию занимают криптографические атаки, использующие слабые места существующих криптоалгоритмов с целью их взлома.

Автора данной статьи в первую очередь интересует развитие данной области в направлении защиты информации, хранящейся на электронных носителях. На сегодняшний момент во всём мире разработан сравнительно небольшой набор программных проектов, способных обеспечить защиту данных пользователей с применением криптоалгоритмов. Самые популярные среди них:

Super File Encryption	*ProtectDrive*	*BestCrypt*	*SafeBit*
PrimaSoft Encryption – Service Edition	*Dekart Private Disk Multifactor*	*Encryption Workshop*	*Secure Hive*
Krickit Data Encryption	*High Power Encryption*	*Tiasoft Secured Drive*	*TrueCrypt*

Целью данного исследования является разработка собственных принципов построения криптографической системы, направленной на защиту данных на электронных носителях, а также их программная реализация.

Данная разработка будет интересна как людям, стремящимся защитить свои конфиденциальные сведения, так и крупным организациям, заинтересованным в невозможности вынести сведения, составляющие коммерческую тайну, обычными методами вроде использования flash-накопителей, передаче через средства общения по сети Интернет, такие как электронная почта, онлайн-мессенджеры (icq, jabber, irc, msn, netmeeting, skype и т.п.).

Общие положения по разработкам в области программных продуктов защиты на основе шифрования

Основные уязвимости реализаций криптосистем

Во многих журналах классификация продуктов шифрования чаще всего сводится к алгоритму и длине ключа. Однако в криптографии все далеко не так просто: более длинные ключи отнюдь не всегда гарантируют повышенной безопасности.

1. Атаки на архитектуру.

Криптографическая система не может быть надежнее использованных в ней отдельных алгоритмов шифрования. Иными словами, для того чтобы преодолеть систему защиты, достаточно взломать любой из ее компонентов, большинство из которых не так хорошо защищены, как основные модули:

a) неправильное использование;
b) использование связанных ключей;
c) генераторы случайных чисел (ГСЧ);
d) взаимодействие по отдельности безопасными протоколами шифрования.

2. Атаки на конкретные реализации.

Многие системы подводят из-за ошибок в реализации. Некоторые продукты не гарантируют, что, зашифровав текст, они уничтожат оригинал. В других для предупреждения потери информации в случае системного сбоя используются временные файлы, а доступная оперативная память расширяется за счет памяти виртуальной; в этом случае на жестком диске могут оставаться отдельные фрагменты незашифрованного текста [3].

3. Атаки на пользователей.

Даже если система гарантирует надежную защиту при правильной эксплуатации, пользователи могут случайно нарушить ее, особенно если система спроектирована недостаточно хорошо. Классическим примером является сотрудник, предоставляющий свой пароль коллегам с тем, чтобы они имели возможность решать неотложные задачи во время его отсутствия. Атака с учетом «человеческого фактора» зачастую оказывается куда более эффективной, чем месяцы кропотливого анализа алгоритмов.

4. Атаки на средства шифрования.

Иногда слабые места можно найти и непосредственно в системе шифрования. Некоторые продукты создаются на базе не слишком удачных алгоритмов собственной разработки. Как правило, вскрыть известные алгоритмы шифрования удается лишь в исключительных случаях. Если же разработчик делает ставку на собственные методы, шансы взломщиков повышаются многократно. Незнание секрета алгоритма не является особым препятствием. Квалифицированному специалисту достаточно пары дней, чтобы по объектному коду восстановить исходный алгоритм шифрования [4].

Последние данные

В январе 2009 года шесть крупнейших производителей жестких дисков обнародовали финальные спецификации единого стандарта шифрования, который можно будет использовать на всех традиционных жестких дисках, твердотельных накопителях SSD и в приложениях для управления ключами шифрования. В состав Trusted Computing Group (TCG), создавшей новый стандарт, входят Fujitsu, Hitachi GST, Seagate Technology, Samsung, Toshiba, Western Digital, Wave Systems, LSI Logic, ULink Technology и IBM. Сам стандарт включает в себя три базовых спецификации – Opal для настольных ПК и ноутбуков, ESSCS (Enterprise Security Subsystem Class Specification) для накопителей, используемых в центрах обработки данных и промышленных приложениях и SIIS (Storage Interface Interactions Specification). В частности, стандарт

полностью определяет поддержку параллельного и последовательного интерфейса ATA, SCSI SAS, Fibre Channel и ATAPI [5].

Общие принципы построения программной реализации

В настоящее время существует довольно значительное количество способов перехвата информации «на лету» при её передаче по любым каналам. Задача криптографической системы заключается именно в её модификации, причём крайне необходимо, чтобы преобразования происходили в обоих направлениях – и от пользователя, и к пользователю, поскольку сам пользователь не должен работать непосредственно с зашифрованными данными.

В разных реализациях используются разные подходы к решению данной задачи. Крайне распространённой техникой является внедрение кода в функции системных библиотек. Простейший способ представляет собой модификацию первых нескольких байт функций, отвечающих за операции ввода-вывода.

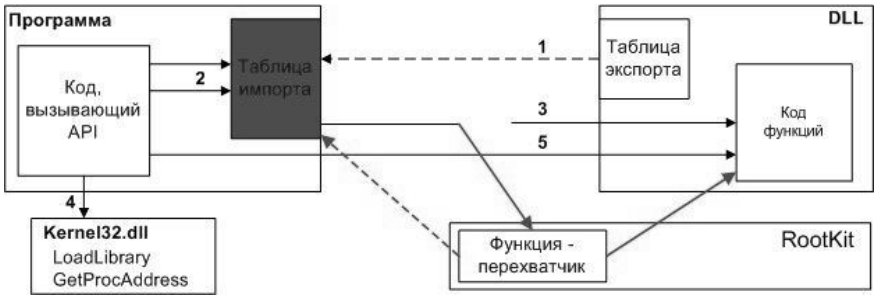


Рис. 1. Перехват экспортируемой функции DLL

Очень распространён метод изменения кода функций на уровне ядра и передача управления на себя с последующим возвратом в исходную функцию [6].

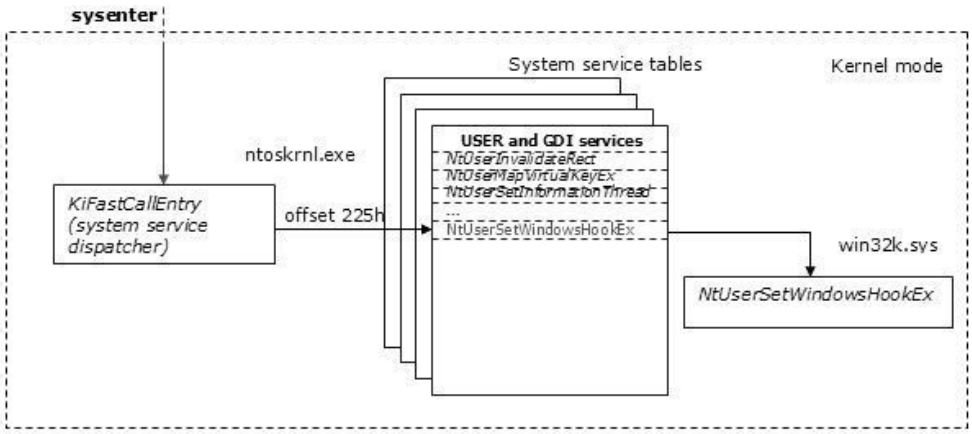


Рис. 2. Перехват функции на уровне ядра

Данная техника очень часто используется вирусописателями, вследствие чего большинство подобных техник расценивается защитными программными средствами в системе как подозрительные и вредоносные. Данный подход совершенно неприемлем.

Основу криптографической системы должен составлять драйвер-фильтр, перехватывающий на native-уровне все обращения к дисковым устройствам и соответствующим образом их обрабатывать. Это полностью легальный метод, который не может нанести серьёзного урона системе в случае его грамотной реализации.

Обработка представляет собой шифрование незашифрованных данных, подлежащих данному действию и дешифрование в обратную сторону. Алгоритм выбирает разработчик ПО. Среди отечественных разработок большой популярностью пользуется криптоалгоритм ГОСТ 28147-89.

Алгоритм шифрования ГОСТ 28147-89 относится к разряду блочных шифров работающих по архитектуре сбалансированных сетей Файстеля, где две части выбранного блока информации имеют равный размер. Для работы данного метода алгоритма необходимо разбить информацию на блоки размером в 64 бита, сгенерировать или ввести в систему шифрования, следующую ключевую информацию: ключ и таблицу замен. К выбору ключа и таблицы замен при шифровании следует отнестись очень серьезно, т.к. именно это фундамент безопасности защищаемой информации [7].

Готовые реализации данного алгоритма доступны в свободной форме в сети Интернет [8].

Итак, основная задача драйвера-фильтра – модификация информации по заданному алгоритму «на лету». С этой целью мы должны внедрить его в цепочку драйверов каждого дискового устройства, существующего в системе, и обрабатывать появление новых дисковых устройств. С этой целью драйвер перехватывает все irp-пакеты типа IRP_MJ_PNP, генерируемые системой при изменении числа устройств. Мы определяем, удалилось или прибавилось новое устройство, его тип. За это отвечает параметр MinorFunction стека irp-пакета, принимая, соответственно, значения IRP_MN_REMOVE_DEVICE и IRP_MN_START_DEVICE. Если он удовлетворяет нашим требованиям, мы добавляем себя в стек его драйверов.

В перехвате нуждаются пакеты, отвечающие за чтение/запись информации, а также за открытие/закрытие файлов для проверки, были ли они изначально шифрованы. Это легко реализуется, например, с помощью какой-нибудь дополнительной сигнатуры в начале файла.

```
pDriverObject->MajorFunction[IRP_MJ_CREATE]=PsdoDispatchCreate;
pDriverObject->MajorFunction[IRP_MJ_CLOSE]=PsdoDispatchClose;
pDriverObject->MajorFunction[IRP_MJ_READ] = PsdoDispatchRead;
pDriverObject->MajorFunction[IRP_MJ_WRITE] = PsdoDispatchWrite;
pDriverObject->MajorFunction[IRP_MJ_PNP] = DispatchPnp;
```

Рис. 3. Перехватываемые IRP-пакеты

Перебор всех дисков осуществляется в цикле, за добавление каждого диска отвечает одна функция, поскольку в дальнейшем потребуется её динамический вызов при изменении количества обрабатываемых электронных носителей.

```
for (i=0;i<26;i++)
{
    DriveHookDevices[i]=NULL;
}

status = GetDrivesToHook(&d_hDrives);
if(!NT_SUCCESS(status))
{
    return status;
}
DrivesToHook = HookDriveSet(d_hDrives, pDriverObject);
```

Рис. 4. Обход в цикле всех дисковых устройств и их обработка

Процедура перехвата пакетов, отвечающих за открытие файла перед работой с ним, IRP_MJ_CREATE – PsdoDispatchCreate – отвечает за определение, является ли данный запрос запросом на создание файла или открытие, если создание – сразу создаём новый запрос на запись и прописываем в начало файла свою сигнатуру, чтобы его пометить, если на открытие – проверяем, если сигнатура есть, значит данный файл надо будет шифровать/дешифровать, иначе пропускаем его.

Процедура перехвата пакетов, отвечающих за чтение информации IRP_MJ_READ – PsdoDispatchRead – должна пропустить запрос по стеку драйверов до самого последнего драйвера и установить свою процедуру обработки с помощью API-функции IoSetCompletionRoutine. Это необходимо, поскольку до того, как запрос не попадёт непосредственно к устройству, мы не будем иметь считанных данных, а значит модифицировать нам будет нечего.

Процедура, отвечающая за перехват IRP_MJ_WRITE – PsdoDispatchWrite – проверяет, нужно ли нам обрабатывать данный файл, и если да – модифицирует на лету передаваемые данные по криптоалгоритму.

И процедура, перехватывающая IRP_MJ_CLOSE – PsdoDispatchClose – отвечает за корректность закрытия файлов.

Отдельными модулями идёт графический интерфейс (GUI), процедура инсталляции драйвера, модуль реализации криптоалгоритма, а также модуль, отвечающий за первоначальную обработку всех заданных при инсталляции директорий в системе.

Данное ПО было разработано в экспериментальных целях и успешно протестировано на машине Pentium IV 2,8 GHz 1024 Mb RAM, ОС Windows XP Professional SP3. Среда разработки – Visual Studio 2005.

Преимущества данной реализации

В первую очередь, используемый метод внедрения в систему совершенно легален, используется во многих системных утилитах, таких как всемирно известный Filemon. Таким образом, исключается конфликт с установленными в системе программными средствами защиты. Во-вторых, он обеспечит стабильную работу системы даже в случае установки другого программного обеспечения, занимающегося перехватом, поскольку драйверов-фильтров может быть сколько угодно. Очень часто системные функции модифицируют при установке антивирусные программы. И, в-третьих, данный подход позволяет великолепно защитить информацию от вредоносных программ, поскольку в случае кражи информация передастся в зашифрованном виде, корректная и незаметная модификация или подлог также становятся невозможны.

Заключение

В данном исследовании рассматриваются общие проблемы, связанные с разработкой криптосистем, направленных на защиту информации на электронных носителях. Приводятся последние данные в этом направлении, новые течения и перспективы дальнейшего развития. Также предлагается собственный подход к разработке данного программного проекта, приводятся все необходимые для реализации функции. Подчёркиваются и аргументируются преимущества выбранного подхода.

Литература

1. P. Gutmann. Software Generation of Random Numbers for Cryptographic Purposes, Proc. 1998 Usenic Security Symp., Usenix Assoc., Berkeley, Calif. – 1998. – PP. 243–257.
2. J. Kelsey, B. Schneier и D. Wagner. Protocol Interactions and the Chosen Protocol Attack. – Security Protocols, 5th Int'l Workshop, Springer-Verlag, New York. – 1996. – PP. 91–104.
3. H. Abelson и др. The Riscs of Key Recovery, Key Escrow and Trusted Third-Party Encryption. – World Wide Web J. – No. 3. – 1997. – PP. 241–257.
4. http://www.pgpru.com/biblioteka/statji/slabyemestakriptograficheskihsistem
5. http://www.securitylab.ru/news/367140.php
6. G. Hoglund, J. Butler. Rootkits. Subverting the Windows Kernel, Addison-Wesley. – 2007. – PP. 111–129.
7. http://www.wasm.ru/article.php?article=gost29147-89
8. http://www.enlight.ru/crypto/frame.htm

УДК 004.056.4

ОБЗОР СОРЕВНОВАНИЙ ПО КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ CTF

Д.О. Жукова
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В статье представлены и рассмотрены примеры заданий из различных областей информационной безопасности, затрагиваемые при проведении соревнований по компьютерной безопасности CTF. Рассмотрена роль подобных соревнований в обучении специалистов информационной безопасности.
Ключевые слова: соревнования, безопасность, информационная, роль, специалисты

Введение

В условиях быстрого роста информатизации общества возникает проблема безопасности компьютерных систем. В связи с этим очень важна подготовка квалифицированных специалистов по защите информации. Одной из возможностей получения навыков в данной области является участие в соревнованиях по компьютерной безопасности. Capture The Flag дословно переводится как «захват флага». В компьютерной безопасности под «захватом флага» подразумевают командные соревнования, целью которых является оценка умения участников атаковать и защищать компьютерные системы. Каждая команда получает выделенный сервер или небольшую сеть для поддержания её функционирования и защиты. Во время игры команды получают очки за корректную работу сервисов своего сервера и за информацию (флаги), полученную в результате использования уязвимостей сервисов других участников. Подобные соревнования позволяют участникам закрепить практические навыки, обменяться опытом в области компьютерной безопасности и дают существенный импульс для профессионального роста их участников. Первые удалённые международные межвузовские соревнования iCTF UCSB были проведены университетом Калифорнии, город Санта-Барбара в 2004 году. Участникам необходимо было проявить знания в таких областях, как анализ машинного кода программы (reverse engineering), анализ входящего и исходящего трафика (network sniffing), анализ протоколов (protocol analysis), системное администрирование, программирование, криптоанализ, стеганоанализ. Подобные соревнования проводятся и в России и проходят в два этапа.

Отборочные соревнования

В настоящее время значение стеганографии в компьютерном мире в полной мере не оценено, в связи, с чем этот метод защиты информации является недостаточно развитым. В отличие от криптографии, стеганография не просто засекречивает передаваемое сообщение, а скрывает сам факт его передачи. Организаторы конкурса CTF, используя метод стеганографии зашифровали некоторую фразу в изображении (рис. 1).

Рис. 1. Изображение с засекреченным сообщением

Для успешного решения данного задания следовало подобрать необходимую яркость изображения (рис. 2), затем обратить цвета, применить некоторые специализированные фильтры для работы с изображениями и получить так называемый бар-код – штрих-код в двухмерном формате (рис. 3).

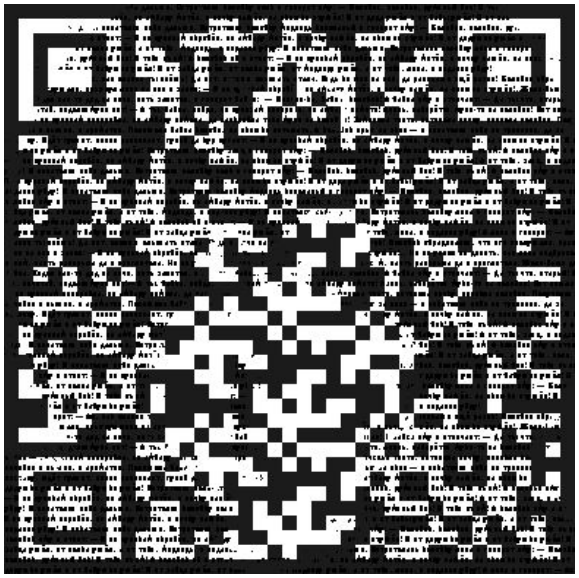


Рис. 2. Изображение после изменения яркости

Рис. 3. Полученный бар-код

После использования программы для расшифровки бар-кодов ZXing Decoder был получен результат – сообщение «JURY LIKES VERY LITTLE PENGUINE DISTROS».

В данном задании стеганография используется совместно с криптографией, что является очень мощным методом передачи секретной информации.

Из рамок цифровой стеганографии вышло наиболее востребованное легальное направление – встраивание цифровых водяных знаков (ЦВЗ), являющееся основой для систем защиты авторских прав и DRM (Digital rigts management) систем. Методы этого направления настроены на встраивание скрытых маркеров, устойчивых к различным

преобразованиям контейнера (атакам).

На RuCTF2009 участникам было необходимо найти ЦВЗ в следующем изображении:

Рис. 4. Изображение со встроенным ЦВЗ

Ни одна из существующих программ распознавания не могла помочь в нахождении ЦВЗ в этом изображении. В качестве подсказки к данному заданию была дана программа, с помощью которой этот ЦВЗ был вставлен в картинку. Следовало дизассемблировать данную программу, после чего можно было увидеть алгоритм встраивания ЦВЗ, и соответственно, следуя алгоритму, обнаружить сам цифровой водяной знак. Сложность удаления подобного рода защиты изображений от копирования говорит о надежности данного метода защиты авторских прав.

Финальный этап

Во время финала каждая команда получает от жюри сервер с предустановленным набором уязвимых сервисов. На момент начала игры сервера команд идентичны. Задачи участников: поддерживать свои сервисы в рабочем состоянии, предотвращать попытки вторжения и проводить аудит серверов других команд. Командам необходимо обнаружить уязвимости на своем сервере и попытаться закрыть их, не нарушив работоспособности сервисов. В то же время, используя знания о найденных уязвимостях, становится возможным провести аудит состояния уязвимостей у других команд. На финальном этапе можно выделить два основных направления, на которые участникам следует обратить особое внимание.

1. Поиск уязвимостей. Поиск уязвимостей необходимо проводить как с использованием инструментальных средств (сканеров безопасности), так и вручную (reverse engineering).

2. Закрытие найденных уязвимостей, которое заключается в исправлении ошибок, найденных в исходном коде сервиса, либо путем написания эксплоита для закрытия существующих уязвимостей в нужном сервисе.

Заключение

Участие в соревнованиях подобного рода имеет огромное значение для изучения методов защиты информации на практике. Следует учитывать важность проведения таких соревнований среди студентов, так как они дают возможность применить полученные в процессе обучения навыки на практике, опробовать существующие методы обеспечения информационной безопасности в условиях, приближенных к реальным, а также в полной мере оценить всю сложность и важность защиты информации, компьютерных и телекоммуникационных систем в современном мире.

ББК Ч 481.44:С55.511

ПРОБЛЕМА ПОНЯТИЯ «КУЛЬТУРА ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ ЛИЧНОСТИ»

А.А. Ахметвалиева
(Южно-Уральский государственный университет)
Научный руководитель – д.п.н., профессор Л.В. Астахова
(Южно-Уральский государственный университета)

В статье подчеркивается роль информационной безопасности и информационно-психологической безопасности, в упрочении демократии, создании правового социального государства, духовном обновлении России, сохранении нравственных ценностей, в предотвращении манипулирования массовым сознанием. Обосновывается необходимость и формулируется на основе деятельностного подхода понятие «культура информационно-психологической безопасности».

Ключевые слова: культура, информационно-психологическая безопасность, культура информационной безопасности, информационная культура, культура информационно-психологической безопасности

Введение

В «Концепции национальной безопасности Российской Федерации», утвержденной Указом Президента РФ от 17.12.97г. №1300 (в редакции Указа Президента РФ от 10.01.2000г. № 24), отмечается, что в современных условиях всеобщей информатизации и развития информационных технологий усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере. В «Доктрине информационной безопасности Российской Федерации», утвержденной Президентом РФ 9.09.2000г. в качестве одного из приоритетных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации выступает совершенствование подготовки кадров, развитие образования в области информационной безопасности. Поднимается вопрос не только защиты информации на различных уровнях, а проблема защиты от информации, проблема формирования у подрастающего поколения и поддержания в обществе общественно необходимых нравственных ценностей. Также в «Стратегии развития информационного общества в Российской Федерации» от 7 февраля 2008 г. № Пр.-212 ставятся задачи обеспечения национальной безопасности в информационной сфере, сохранения культуры многонационального народа Российской Федерации, укрепления нравственных и патриотических принципов в общественном сознании, развития системы культурного и гуманитарного просвещения [4, 6, 14].

Л.В. Астахова, формулируя понятие «информационная безопасность» на основе деятельностного подхода, определяет его как состояние защищенности субъектов информационных отношений, включающее в себя качественную информационную среду (качество потребляемой информации, защищенность субъектов от негативных информационных воздействий), (информационно-психологическая безопасность) и защищенность их информации (безопасность информации) и обеспечивающее полное удовлетворение информационных потребностей субъектов [1, С. 97]. Информационно-психологическая безопасности личности в качестве самостоятельной предметной области изучения рассматривается такими авторами как А.В. Брушлинский, Г.В. Грачев, В.В. Лепский, И.Н. Панарин, С.Ю.Решетникова, Г.Л. Смолян, Д.С. Синицын. Однако теоретический анализ состояния проблемы информационно-психологической безопасности как педагогической проблемы позволяет сделать вывод о её недостаточной разработанности, поскольку различные её аспекты находят пока отражение большей частью в политологии, социологии, естественно-научной, технической, правовой облас-

тях. Вместе с тем, одним из главных субъектов обеспечения информационно-психологической безопасности личности выступает ВУЗ.

Основная часть

В настоящее время в педагогике высшей школы решение проблем информационной безопасности реализуется через формирование информационной культуры личности и формирование культуры информационной безопасности личности. Информационная культура, являясь продуктом разнообразных творческих способностей человека, проявляется в следующих аспектах: в конкретных навыках по использованию технических устройств; в способности использовать в своей деятельности компьютерно-информационную технологию, базовой составляющей которой является многочисленные программные продукты; в умении извлекать информацию из различных источников; во владении основами аналитической переработки информации; в знании особенностей информационных потоков в деятельности [13, С. 24]. Культура информационной безопасности личности представляет «такой способ организации и развития жизнедеятельности, при котором гражданин знает и способен реализовать свои конституционные права и свободы в информационной сфере (владеет технологиями доступа к государственным информационным ресурсам, может сохранить свою личную тайну, интеллектуальную собственность), умеет распознать негативные информационные воздействия, угрожающие его здоровью, и владеет технологиями защиты от них» [1, С. 98]. Таким образом, мы видим, что, формируя информационную культуру личности, педагог не ставит цель сформировать, например, качества личности или развить способности, обеспечивающие именно информационно-психологическую безопасность. В рамках же формирования культуры информационной безопасности личности, информационно-психологическая безопасность рассматривается недостаточно, либо в контексте защиты информации от субъектов информационных отношений, либо, затрагивая только вопросы умения распознания негативных информационных воздействий.

Таким образом, перед теорией и методикой профессионального образования стоит задача разработки понятийного аппарата (формулирование понятия культура информационно-психологической безопасности, определение ее составляющих и т.п.), построения модели формирования культуры информационно-психологической безопасности, позволяющей обеспечить необходимое качество подготовки студентов различных специальностей в области информационно-психологической безопасности с учётом уровня развития современных информационных и коммуникационных технологий, реалий конкурентной рыночной среды и информационного противоборства.

С целью определения понятия «культура информационно-психологической безопасности личности» рассмотрим смыслообразующие составляющие данного феномена: «культура», «информационно-психологическая безопасность».

Теоретический анализ существующих подходов к пониманию культуры позволяет нам констатировать, что понятие и термин «культура» используется для описания и объяснения широкого круга деятельности, моделей поведения, событий и структур в нашей жизни, причем, в философии, психологии, педагогике данный термин имеет различные значения. Д. Мацумото (D. Matsumoto) на основе опыта А.Л. Крёбера и К. Клакхольна (A.L. Kroeber, C. Kluckholn) описывает шесть общих категорий, в которых обсуждается культура.

- Дескриптивное использование делает акцент на различных видах деятельности или поведения, связанных с культурой.

- Исторические определения относятся к наследию и традициям, связанным с группой людей.

- Нормативное использование описывает правила и нормы, которые связанны с культурой.

- Психологические описания делают упор на научение, решение проблем и другие поведенческие подходы, относящиеся к культуре.

- Структурные определения акцентируют внимание на общественных и организационных элементах культуры.

- Генетические описания касаются происхождения культуры [10, С.31].

Л.В. Астахова выделяет следующие значения понятия «культура»: обыденное значение; ведомственно-отраслевое прикладное понимание культуры; гуманистическая концепция культуры; информационно-семиотическая концепция; духовно-производственная; этно-археологическая концепция и, связанная с ней, деятельностная (функциональная, технологическая) концепция культуры. В рамках формулирования понятия «культура информационно-психологической безопасности» считаем наиболее адекватным подходом к рассмотрению определения «культура» именно деятельностную концепцию, которая понимает под культурой – специфический способ организации и развития человеческой жизнедеятельности, представленный в продуктах материального и духовного труда, в системе социальных норм и учреждений, в духовных ценностях, в совокупности отношений людей к природе, между собой и к самим себе [1, С. 93–95]. Деятельностный подход к рассмотрению культуры (Н.С. Злобин, М.С. Каган, Э.С. Маркарян и др.) понимает ее как общий способ человеческого существования. Данный подход трактует культуру как важную характеристику разнообразных видов человеческой деятельности. Можно говорить о культуре технологической, правовой, политической, педагогической, философской, математической, теоретической, методологической и др.

Вышеобозначенный подход распадается на два основных направления: одно рассматривает культуру в контексте личностного становления (Э.А. Баллер, Н.С. Злобин, Л.Н. Коган, В.М. Межуев и др.), другое — характеризует ее как универсальное свойство общественной жизни (Л.П. Буева, В.Е. Давидович, Ю.А. Жданов, М.С. Каган, Э.С. Маркарян, О.В. Ханова и др.). Личностно-творческая концепция трактует культуру как «процесс творческой деятельности человека» (Н.С. Злобин), как «систему, выступающую мерой и способом формирования и развития сущностных сил человека в ходе его социальной деятельности» (Л.Н. Коган) [2, 5, 7]. Технологически-деятельностное представляет культуру как «специфический способ человеческой деятельности» (Э.С. Маркарян), «продуктивную силу деятельности», «совокупность плодов и способов деятельности субъекта» (М.С. Каган). Согласно позиции этих авторов, фундаментальное свойство культуры – быть средством деятельности людей, концентрированно выражает саму суть культуры и интегрирует все остальные ее характеристики. Э.С. Маркарян пишет: «Термин «способ деятельности» понимается в широком значении, несводимым лишь к навыкам, умению, а предполагающим так же и охват многообразных объективных средств осуществления активности людей... К ним относятся социогенные потребности, знания, орудия труда, юридические установления, одежда, пища, жилища и множество других явлений. Все они системно объединяются в единый структурный ряд, благодаря тому, что выполняют общую функцию средств осуществления соответствующих звеньев человеческой деятельности... Этнические культуры представляют собой исторически выработанные способы деятельности, благодаря которым обеспечивалась и обеспечивается адаптация различных народов к условиям окружающей их природной и социальной среды» [9, С. 325].

Таким образом, авторы двух направлений деятельностного подхода, раскрывая динамичность понятия культура, подчеркивают взаимовлияние и взаимозависимость культуры и человеческой деятельности. Аналитическое осмысление существующих подходов к определению культуры, раскрывающих различные аспекты данного поня-

тия, позволило нам констатировать, что независимо от подхода к определению исследуемого нами феномена, культура характеризует жизнедеятельность личности, группы, общества в целом; является специфическим способом бытия человека, имеет свои пространственно-временные границы; раскрывается через особенности поведения, сознания и деятельности человека.

Теоретический анализ показывает, что определение информационно-психологической безопасности является весьма размытым, так Г.В. Грачев говорит о «состоянии защищенности групповой и общественной психологии», о «состоянии защищенности личности», под информационно-психологической безопасностью личности автор понимает «состояние защищенности ее психики от действия многообразных информационных факторов, препятствующих или затрудняющих формирование и функционирование адекватной информационно-ориентировочной основы социального поведения человека в целом, жизнедеятельности в обществе, а также адекватной системы субъективных (личностных, субъективно-личностных) отношений к окружающему миру и самому себе». В.Е. Лепский о «состоянии защищенности субъектов деятельности…, а также информации и информационных потоков, обеспечивающих деятельность». С.Ю. Решетникова и Г.Л. Смолян представляют информационно-психологическую безопасность как такую ситуацию в системе «человек – информационная среда», которая не вызывает снижение индивидуального или популяционного психологического потенциала за допустимые пределы (ситуация – качественно своеобразное состояние элементов системы, их связей между собой и динамических параметров информационного обмена. Индивидуально-психологический потенциал – интегральная характеристика совокупности всех психологических свойств индивида, лежащих в основе возможностей осуществлять продуктивную жизнедеятельность). В проект Федерального закона «Об информационно-психологической безопасности» дается следующее толкование данного термина: «состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере» [3, 8, 11, 12].

Опираясь на данные определения, рассмотрим понятие «информационно-психологическая безопасность» на основе методологии деятельностного подхода, предполагающего анализ следующих компонентов деятельности: цель, объект, субъект, процессы, средства, результат. Целью деятельности по обеспечению информационно-психологической безопасности, а, следовательно, и результатом данной деятельности выступает состояние защищенности от негативных информационных воздействий. Объектом в условиях информационного взаимодействия с окружающей средой является личность. Соответственно, объектом выступает и общество, и государство, однако процессы, средства обеспечения данной защищенности будут отличными, в связи с этим в рамках статьи ограничимся рассмотрением только информационно-психологической безопасности личности. Для обозначения условий информационного взаимодействия воспользуемся классификацией коммуникативных ситуаций, предложенной Г.В. Грачевым Данные условия взаимодействия Г.В. Грачев, называя коммуникативные ситуации, в которых на человека оказывается информационно-психологическое воздействие, делит на три группы: межличностные коммуникативные ситуации, контакт-коммуникационные ситуации, масс-коммуникационные ситуации.

В межличностных коммуникационных ситуациях, ситуациях непосредственного общения, человек выступает одновременно и субъектом и объектом коммуникации. Данные ситуации могут подразделяться по содержанию или характеру социальных связей на следующие: общественно-политические; профессионально-деловые; социокультурные; семейно-родственные; социально-бытовые; дружеские; случайные. В группу контакт-коммуникационных ситуаций включены ситуации, определяемые нахождени-

ем человека в составе определенной общности людей, на которую оказывается непосредственное информационно-психологическое воздействие некоторым коммуникатором – личностью или группой (оратор, президиум и т.д.). В таких ситуациях (собрания, совещания, митинги, зрелищные мероприятия и т.д.) осуществляется в основном односторонняя непосредственная коммуникация по типу «коммуникатор – общность людей».

В масс-коммуникационных ситуациях осуществляется односторонняя опосредованная коммуникация по типу «СМК (средства массовой коммуникации) – человек (аудитория)». Это ситуации просмотра телепередач, прослушивания радиопрограмм, чтения газет, журналов, различных печатных изданий, взаимодействия с разнообразными информационными системами и т.п. [3].

Следовательно, объект (личность) – субъект информационного взаимодействия. Осознание личностью субъектом обеспечения защищенности от информационных воздействий, представляющих угрозу является одним из процессов данного обеспечения. Выдвижение в качестве результата данной деятельности «состояния защищенности от негативных информационных воздействий предполагает в буквальном смысле наличие угроз и противодействие им» [15, С.20]. Следовательно, процессами обеспечения состояния защищенности субъекта выступают: выявление угроз информационно-психологической безопасности и противодействие им по средствам использования субъектом знаний, умений, навыков (психических образований) в сфере информационно-психологической безопасности; памяти, критичности мышления (психических процессов); эмпатии и рефлексии /социально-психологической/ (способов познания, понимания мира и себя как части мира).

Тогда информационно-психологическая безопасность личности – это состояние защищенности субъектов информационного взаимодействия от негативных информационных воздействий.

Заключение

Выделив методологической основой деятельностный подход определения таких терминов как «культура» и «информационно-психологическая безопасность», мы имеем возможность сформулировать понятие «культура информационно-психологической безопасности личности»: это такой способ организации и развития жизнедеятельности, при котором субъект информационного взаимодействия осознает себя субъектом информационно-психологической безопасности, способен выявить угрозы информационно-психологической безопасности, владеет технологиями защиты от них, способен безопасно преобразовывать информационную среду.

Проведенный нами теоретический анализ данной проблемы показал, что «культура информационно-психологической безопасности» сегодня отсутствует как строгое, научное, обоснованное понятие, хотя потребность в его формулировании прослеживается не только в практике (негативные тенденции информационного общества, меняющаяся парадигма образования, современные требования к специалисту), но и в теории при рассмотрении таких проблем, как: безопасность личности, культура безопасности, информационно-психологическая безопасность, культура информационной безопасности, информационная культура. Данный термин позволяет подойти к проблеме обеспечения информационно-психологической безопасности с точки зрения активности самого субъекта данного обеспечения, перейти к проблеме формирования, а, следовательно, рассмотреть культуру информационно-психологической безопасности как объект педагогического исследования.

Литература

1. Астахова Л.В. Сущность понятия «Культура информационно-психологической безопасности» и ее формирование у студентов ВУЗА/ Л.В.Астахова// Экономика. Информатика. Безопасность, сборник научных трудов Международной научно-практической конференции, 2006/ Науч. ред. В.А. Киселева, Л.В. Астахова. – Челябинск: Изд-во ЮУрГУ. – 2006. – С. 93–99.
2. Большая энциклопедия: В 62 томах. Т.24. – М.: ТЕРРА. – 2006. – 529 с.
3. Грачев Г.В. Личность и общество: информационно-психологическая безопасность и психологическая защита. – Волгоград: Издатель. – 2004. – 336 с.
4. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр – 1895 [Электронный ресурс]:// www.rg.ru / official / doc / min-and – vedom / mim – bezop / doctr.shtm
5. Каган М.С. Системный подход и гуманитарное звание: Избр. ст./ Ленинградский гос.ун-т. – Л.: Изд-во ЛГУ. – 1991. – 382 с.
6. Концепции национальной безопасности Российской Федерации», утвержденной Указом Президента РФ от 17.12.97г. №1300 (в редакции Указа Президента РФ от 10.01.2000г. – № 24.
7. Крёбер А.Л. Избранное: Природа культуры / Пер. с англ. – М.: «Российская политическая энциклопедия» (РОССПЭН) . – 2004. – 1008 с.
8. Лепский В.Е. Информационно-психологическая безопасность субъектов дипломатической деятельности [Текст] / В.Е.Лепский // Дипломатический ежегодник – 2002: сборник статей колл. авторов. – М.: Научная книга. – 2003. – С. 233–248.
9. Лурье С.В. Психологическая антропология: история, современное состояние, перспективы. – М.: Академический проект, Деловая книга. – 2005. – 624 с.
10. Мацумото Д. Человек, культура, психология. Удивительнын загадки, исследования, открытия / Дэвид Мацумото. – СПб.: Прайм-ЕВРОЗНАК. – 2008. – 668 с.
11. Проект Федерального закона «Об информационно-психологической безопасности» [Электронный ресурс]: // www.MEDIALAW.RU / publications / zip / 68/ lopatin.htm
12. Решетникова С.Ю., Смолян Г.Л. Информационно-психологическая безопасность личности (контуры проблемы) [Текст] / С.Ю. Решетникова, Г.Л. Смолян // Проблемы ИПБ. Сборник статей и материалов конфереиции. – М.: Изд-во ин-та психологии РАН. – 1996. – С.18–26.
13. Синицын Д.С. Психолого-педагогические условия обучения информационно-психологической безопасности подростков [Текст] / Д.С. Синицын: Дис. …кан.пед.наук: 13.00.01: СПб. – 2005. – 168 с.
14. Стратегии развития информационного общества в Российской Федерации от 7 февраля 2008 г. № Пр.-212 [Электронный ресурс]: // www.rg.ru / 2008/ 02/ 16/ informacia – strategia – dok.html
15. Тер-Акопов А.А. Безопасность человека: Социальные и правовые основы. – М.: Норма. – 2005. – 272 с.

УДК 654.949

ВОЗМОЖНОСТИ ИНТЕГРАЦИИ СОВРЕМЕННЫХ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ

А.В. Леус
(Московский физико-технический институт (государственный университет))
Научный руководитель – к.т.н., с.н.с. В.А. Лобачев
(Московский физико-технический институт (государственный университет))

В настоящее время существует тенденция для повышения эффективности систем физической защиты (СФЗ) объединять различные подсистемы в интегрированные комплексы. В работе рассматривается эффективность этих систем с точки зрения временных задержек. Предлагается к рассмотрению несколько способов интеграции СФЗ, таких как централизованная интеграция, интеграция распределенных систем, IP-решение – интеграция на основе компьютерных сетей. Для каждого из решений оценивается время реакции системы на событие, приводится результат экспериментальных исследований, проведенных на базе лаборатории кафедры «Системы безопасности» МФТИ.

Ключевые слова: интегрированные системы безопасности, временные задержки, централизованная система, распределенная система, IP-решение

Введение

Проблема интеграции становится всё более и более актуальной. Связано это, прежде всего, с требованиями, предъявляемыми к системе почти в каждом проекте. Интеграция устройств различных подсистем практически всегда необходима для решения конкретной ситуационной задачи. И хотя сейчас многие производители делают качественные, функциональные системы, этого оказывается недостаточно. Необходима не только надёжная работа частей ФСЗ, но и корректное взаимодействие подсистем [1]. Особенно важен этот вопрос при взаимодействии оборудования разных производителей.

Очевидно, что одним из основных показателей интеграции систем является время, в течение которого обрабатывается событие в системе и выполняется ответное действие [2]. Допустимое время задержки определяется ситуационной задачей. Если время, которое необходимо для взаимодействия подсистем, превышает максимально допустимое, определенное ситуационной задачей, то такая интеграция бесполезна.

В первую очередь с временной задержкой мы сталкиваемся при обработке информации в оконечных устройствах. После того как «отработало» оконечное устройство (сработал извещатель или считалась карта на считывателе), данную информацию необходимо передать дальше. Тут задержка сигнала определяется временем опроса шлейфа или временем передачи информации по имеющемуся интерфейсу [3]. Для этого иногда необходимо дополнительное время для установления связи с устройством, куда идут данные.

После того как периферийные данные достигли центральных модулей, задержка определяется взаимодействием подсистем.

Централизованные системы безопасности

В настоящее время задачи интеграции чаще всего решаются на верхнем уровне системы. Множество производителей предлагают свое интегрирующее программное обеспечение. Естественно, что в этом случае СФЗ представляет собой централизованную систему (рис. 1). В такой системе «мозгом» является компьютер, на котором установлено соответствующее интегрирующее программное обеспечение. К компьютеру обычно по интерфейсу RS-232 подключаются центральные контроллеры системы контроля и управления доступом, системы охранно-пожарной сигнализации,

концентраторы и коммутаторы видеоподсистемы. К центральным контроллерам обычно по интерфейсу RS-485 подключатся периферийные модули, к которым по своим интерфейсам подключаются оконечные устройства. Через эти промежуточные звенья компьютер осуществляет мониторинг и управление всей периферией.

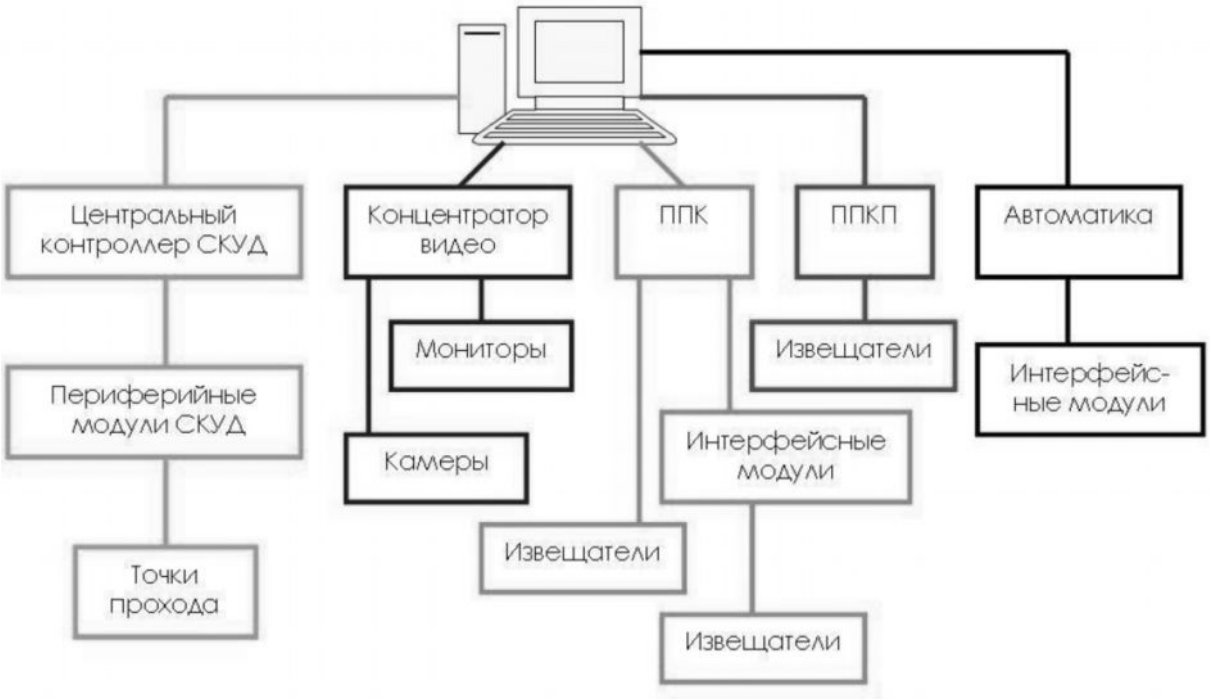


Рис. 1. Централизованная система

Рассмотрим следующую ситуационную задачу. В помещении имеются средства обнаружения и телевизионные камеры. Необходимо произвести видеоверификацию тревоги по сигналу от средств обнаружения. Временной параметр определяется временем пребывания нарушителя в поле зрения камеры. Допустимое время задержки от одной до трех секунд. Рассмотрим, какие задержки появятся в централизованной системе при решении данной задачи (рис. 2).

Рис. 2. Задержки в централизованной системе

Очевидно, что в таких системах задержка достаточно велика, и практически невозможно уложиться в предложенное время [2]. Именно поэтому зачастую используют релейную интеграцию, которая позволяет передавать тревожный сигнал на видеоподсистему, минуя центральный контроллер СОС и программное обеспечение. Кроме того, для решения поставленной задачи верификации используется постоянная предтревожная запись, которая позволяет оператору произвести верификацию тревоги не в реальном времени, но с небольшим опозданием.

Распределенные системы

Если основные блоки управления подсистем соединены в шину, могут напрямую передавать данные между собой, а также осуществлять управление, то такая система будет распределенной (рис. 3.). Многие крупные производители предлагают собственные законченные интегрированные комплексы, в которых передача данных между центральными контроллерами подсистем осуществляется по интерфейсу RS-485 или CAN шине [4]. Также к общей шине данных может быть подключено и несколько устройств одного типа для расширения системы. В такой топологии устройства могут передавать необходимые данные в шину, причем не обязательно передавать все данные, но только те, которые нужны для решения определенных задач интеграции. Остальные устройства, получая информацию по данной шине, должны выполнять необходимые операции, опираясь на заложенную в них логику. Так как обмен необходимой информацией происходит не через компьютер, а напрямую, временные задержки в такой системе значительно меньше, чем в централизованной.

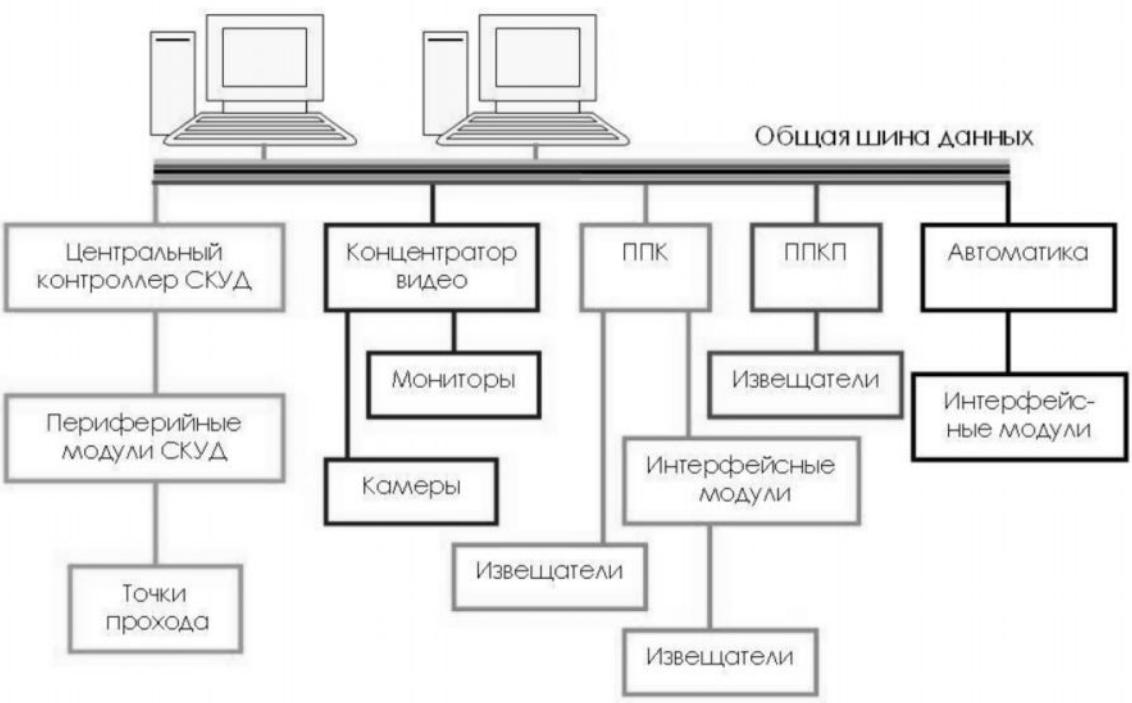


Рис. 3. Распределенная система

Задержки в распределенной системе показаны на рис. 4.

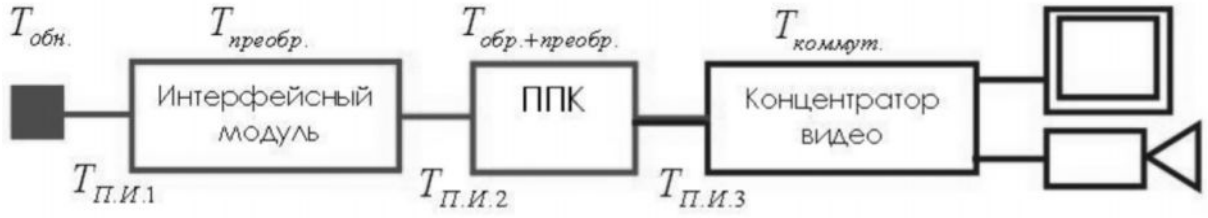


Рис. 4. Задержки в распределенной системе

Основным минусом такого подхода является то, что стандартные шины RS-485 и CAN имеют значительные ограничения по длине и пропускная способность их резко падает с увеличением длин шин. Кроме того, как и в большинстве других случаев, протоколы обмена данными обычно закрыты, а значит, в такой интегрированной системе можно использовать устройства только одного производителя [3].

IP – решение для интегрированных систем

Последнее время стало популярным использовать для систем безопасности уже имеющуюся компьютерную локальную сеть. Ведутся нескончаемые споры о целесообразности таких решений, но точно можно сказать, что данное направление развивается, и все большее число производителей начинают выпускать свое оборудование с возможностью подключения по IP. Кроме того, для повышения надежности предлагается организовывать дополнительную специализированную сеть, в которой присутствует только трафик систем безопасности, и обычные пользователи не будут иметь туда доступа. В этих условиях появляются явные преимущества использования локальных сетей. В таком случае преимущества становятся ещё более очевидными.

Рассмотрим IP-решение для интегрированной системы. В правильно организованную сеть можно подключить практически любое число устройств, таких как контроллеры СКУД, камеры, охранные и пожарные приемно-контрольные приборы. В этой же сети могут находиться видеоархивы, серверы, управляющие системой безопасности и рабочие места операторов. Основным «мозгом» такой системы все равно остается управляющий сервер, но у него в данном случае гораздо большие возможности, чем в обычной централизованной системе. К серверу по сети напрямую подключается все оборудование. Таким образом, все сигналы от периферии центр получает «без посредников», также «без посредников» может происходить и управление теми или иными системами, подключенными к локальной сети. Например, сервер может получать информацию от системы контроля и управления доступом непосредственно с интерфейсных модулей, минуя центральный контроллер, а количество подключаемых модулей будет определяться уже не ограничением интерфейса RS-485, а используемой локальной сетью и возможностями интегрирующего программного обеспечения.

Остается только сказать, что сеть не должна быть перегружена (это особенно важно учитывать, когда видеонаблюдение строится на IP-камерах), а у пакетов различных подсистем в данной сети должен быть определен приоритет, соответствующий важности подсистемы. В этом случае временные задержки для критически важных сообщений будут минимальными.

В настоящее время в лаборатории кафедры «Системы безопасности» МФТИ(ГУ) проводятся исследования временных параметров интеграции систем физической защиты. Наилучшие результаты были получены для систем, построенных на оборудовании, использующем сетевые технологии.

Литература

1. Гарсиа М. Проектирование и оценка систем физической защиты. Пер. с англ. – М.: Мир: ООО «Издательство АСТ», 2002. – 386с.
2. Леус А.В. «Интеграция систем безопасности», труды 51-й научной конференции МФТИ «Современные проблемы фундаментальных и прикладных наук»: Часть I. Радиотехника и кибернетика. – М.:МФТИ, 2008. – С. 119–121.
3. Леус А.В. «Адресные системы охранной сигнализации», журнал «Системы безопасности», раздел «ОПС, пожарная безопасность», декабрь 2008 – январь 2009, выпуск 6(84), С. 166–167.
4. Лобачев В.А., Бурмистров В.С. «Средства обнаружения в интеллектуальных интегрированных системах охраны», сборник научных трудов «Состояние и развитие систем физической защиты». – М.: Дортранспечать, 2008. – С. 27–41.

УДК 004.722.4

ОПРЕДЕЛЕНИЕ ИСТОЧНИКА ШИРОКОВЕЩАТЕЛЬНОГО ШТОРМА НА ОСНОВЕ ДАННЫХ ПРОТОКОЛА SNMP

М.Б. Будько, М.Ю. Будько
Научный руководитель – к.т.н., доцент Г.П. Жигулин

Рассматриваются методы обнаружения широковещательных штормов и динамического построения топологии сети на основе анализа потоков данных. Рассмотрен механизм обнаружения широковещательного шторма в сети, его источника и области поражения. Производится сравнение критериев, обеспечивающих поиск похожих шаблонов трафика. Предлагается метод определения источника широковещательного шторма на основе данных протокола SNMP.
Ключевые слова: безопасность сети, широковещательный шторм, топология сети

Введение

В настоящее время широкое распространение получили сети передачи данных, построенные с использованием технологии Ethernet [1]. Несмотря на то, что физическая топология таких сетей представляет собой дерево, достаточно большие сегменты могут быть объединены на втором уровне модели OSI [2]. Это приводит к возникновению угроз безопасности [3], связанных с использованием широковещательных и групповых адресов для организации штормов в сети [4]. В связи с этим возникает задача динамического анализа потоков данных с целью обнаружения источников дестабилизирующего воздействия на сеть и определения области поражения.

Существующие способы обнаружения широковещательных штормов сводятся к определению интенсивности передачи широковещательных пакетов через конкретный порт коммутатора. При превышении некоторого порога пакеты начинают отбрасываться [5]. Однако не все коммутаторы поддерживают эти функции и, как показывает опыт, они не всегда работают корректно.

Эффективность решения задачи анализа потоков данных зависит от средств и способов мониторинга сетевой инфраструктуры. Как правило, в крупных сетях в качестве основного источника информации используется протокол SNMP [6]. С его помощью собираются сведения о загрузках сетевых интерфейсов коммутирующего оборудования.

Для решения задачи поиска источника широковещательного шторма с помощью сведений протокола SNMP необходимо выполнять сравнение интенсивностей трафика на сетевых интерфейсах коммутаторов. Сложность анализа потоков данных состоит в том, что устройства опрашиваются системой мониторинга не синхронно, т.е. существует разница во времени между запросом статистики у первого и последнего устройства в списке мониторинга. Для снижения влияния задержки данные интерполируются до того момента времени, когда начался опрос первого устройства. Это приводит к несоответствию показаний статистики для двух портов, даже если весь трафик с одного из них поступает на вход другого. Соответственно показания, попадающие в базу данных системы мониторинга, являются функцией от реальных значений [7].

Поиск связей между устройствами в сети

Прежде чем перейти к поиску источника широковещательного шторма необходимо определить методы анализа статистических данных, позволяющие с высокой достоверностью обнаруживать соответствия между трафиком на различных портах сетевых устройств:

$$\mathrm{Y} = \begin{Bmatrix} y_1 = y_1(t_1, t_2, \ldots, t_n) \\ y_2 = y_2(t_1, t_2, \ldots, t_n) \\ \vdots \\ y_k = y_k(t_1, t_2, \ldots, t_n) \end{Bmatrix},$$

где Y – множество значений показаний статистики по всем портам; y_i – вектор показаний трафика на порту i; k – количество портов в сети; n – объем анализируемой выборки.

Одним из вариантов решения задачи поиска похожих последовательностей является представление ее в виде задачи нахождения нормы в k-мерном арифметическом пространстве, т.е. отклонений между векторами из множества Y:

$$\left\| y_i - y_j \right\| = \min .$$

Векторы, разница отклонений между которыми будет минимальной и не превысит некоторого порогового значения, будут относиться к связанным портам. В качестве меры похожести можно использовать следующий критерий:

$$s_{ab} = \sum_{i=1}^{n} \left| y_a(i) - y_b(i) \right|^p ,$$

где s_{ab} – коэффициент, определяющий близость между значениями трафика на портах a и b; $y_a(i)$ – значение отсчета с номером i на порту a, $y_b(i)$ – значение отсчета с номером i на порту b; n – количество отсчетов, используемых для определения связей между устройствами; p – показатель, определяющий степень влияния выбросов в выборке.

При p=1 получаем сумму абсолютных значений остаточных разностей, которую Лаплас предложил использовать для поиска нормы отклонений наблюдаемых и расчетных значений, при p=2 – сумму квадратов отклонений, которую предложили Гаусс и Лежандр для применения в методе наименьших квадратов. Увеличение значения p влияет на степень учета отклонений сравниваемых значений. Например, при p=2 наличие выбросов в сравниваемых выборках может ухудшить значение коэффициента s по сравнению с p=1.

Одним из вариантов решения задачи поиска похожих последовательностей может являться использование коэффициента корреляции. Например, стандартного коэффициента корреляции Пирсона, характеризующего степень линейной зависимости или непараметрического коэффициента корреляции, например, коэффициента ранговой корреляции Кендалла

Проведено исследование, в рамках которого оценивались следующие критерии обнаружения одинаковых последовательностей трафика:

- коэффициент, вычисленный на основе сумм абсолютных значений остаточных разностей;
- коэффициент, использующий сумму квадратов отклонений;
- коэффициент, использующий сумму остаточных разностей, возведенную в третью степень;
- выборочный коэффициент корреляции Пирсона;
- выборочный ранговый коэффициент корреляции Кендалла [8].

В качестве исходных данных использовались показания загрузки интерфейсов сетевых устройств в распределенной сети. При этом делалась попытка на основе показаний статистики найти связанные друг с другом порты оборудования, так как очевидно, что трафик между ними должен быть одинаковым. Результаты приведены на рис. 1 и рис. 2, где показаны степень совпадения обнаруженных связей с реальной структурой сети и процент ошибочно обнаруженных соответствий.

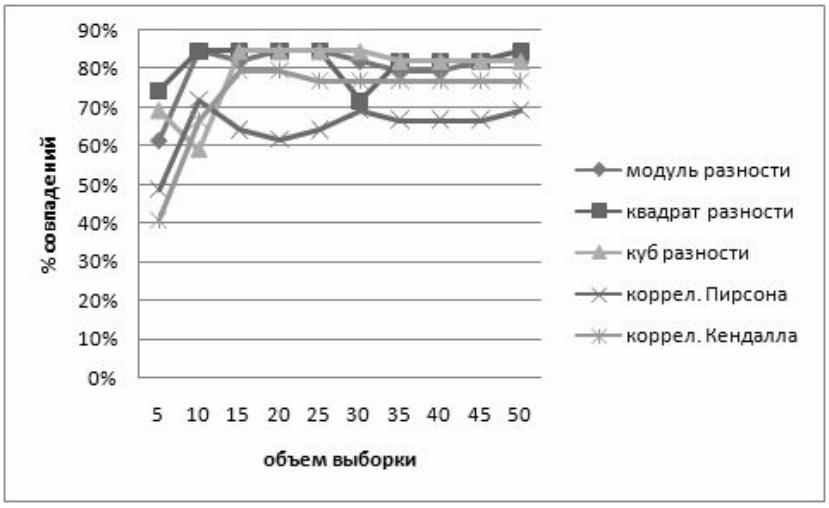


Рис. 1. Степень совпадения с реальной топологией

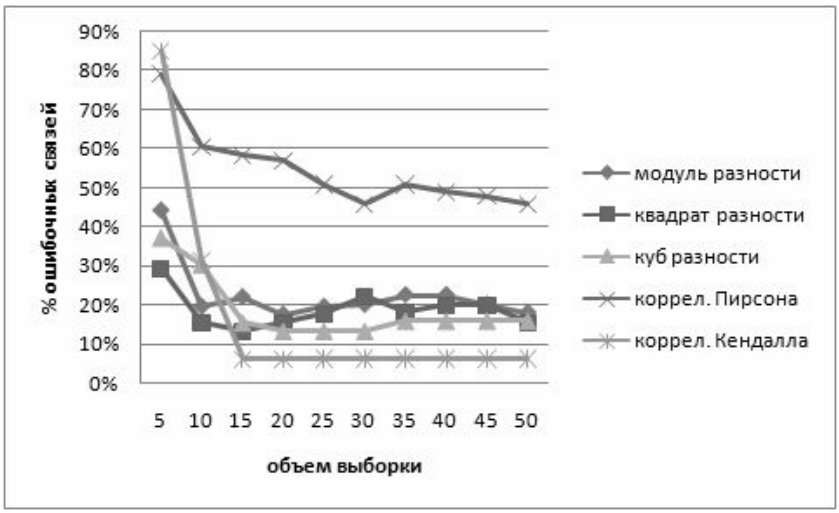


Рис. 2. Ошибочно обнаруженные связи

Из рис. 2 видно, что наиболее достоверным способом обнаружения одинаковых последовательностей трафика является использование коэффициента ранговой корреляции Кендалла. Его единственным ограничением является то, что объем анализируемой выборки должен быть не менее 15 значений. При небольшом объеме выборке оптимальным является метод использующий квадрат разности.

Обнаружение широковещательных штормов

Следующим этапом является применение похожего подхода для обнаружения аномалий трафика на примере широковещательного шторма. Суть этого явления состоит в том, что несанкционированные действия какого-либо узла сети могут привести к увеличению нагрузки на широковещательный сегмент сети, а в некоторых случаях к перегрузкам и снижению быстродействия других узлов. Это происходит вследствие того, что широковещательный трафик распространяется по всему сегменту и должен быть обработан каждым узлом сети. Пример широковещательного трафика приведен на рис. 3.

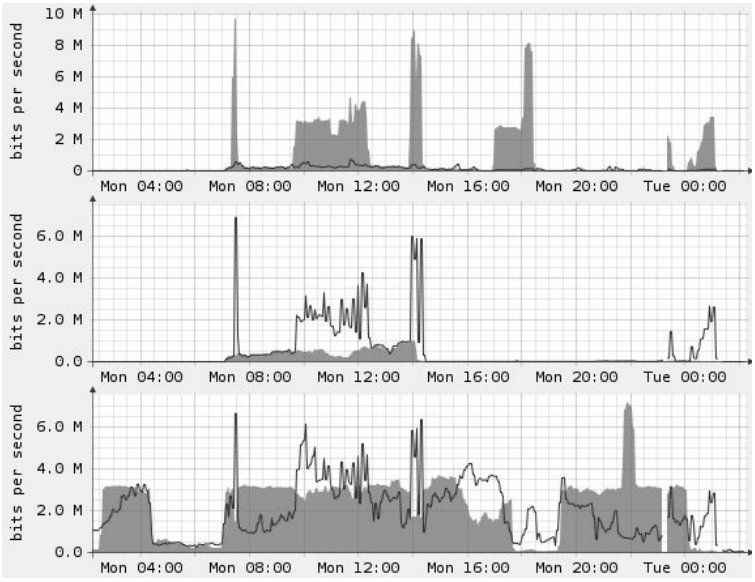


Рис. 3. Распространение широковещательного шторма в сети

Из рис. 3 видно, что широковещательный шторм имеет свойства, которые могут использоваться для его обнаружения:

- распространяется по всем портам коммутирующего оборудования в рамках одного сегмента;
- является исходящим трафиком для источника и входящим для всех остальных узлов сегмента.

Можно определить следующую последовательность действий по обнаружению широковещательного шторма:

1. Определение уровней иерархии устройств в сети с помощью предварительного построения структуры сети. Построение осуществляется динамически путем сравнения интенсивностей трафика на портах коммутирующих устройств [9]. При этом в качестве коэффициента похожести используется ранговый коэффициент корреляции Кендалла.
2. Анализ трафика на устройствах, находящихся на самом нижнем уровне каждой ветки дерева структуры. Это позволит, с одной стороны, проанализировать все широковещательные домены и, с другой стороны, исключить из рассмотрения сетевое оборудование уровня распределения, так как обнаружить шторм на этом уровне существенно сложнее, чем на уровне доступа.
3. Определение списка устройств, у которых разница между средними на порт значениями трафика предыдущих и последующих отсчетов превысила порог, установленный администратором сети:

$$d = \frac{1}{n_1}\sum y(i) - \frac{1}{n_2}\sum y(i-1),$$

где d – разница между средними значениями трафика для конкретного устройства, $y(i)$ – значение отсчета с номером i на одном из активных портов, n_1 и n_2 – количество активных портов в моменты времени, соответствующие отсчетам с номерами i и $i-1$. Под «активным» следует понимать порт, на котором зафиксирована интенсивность передачи данных не ниже порогового значения, установленного администратором сети. При этом на нем должен быть зафиксирован как входящий, так и исходящий трафик. Введение порогового значения не позволит обнаруживать широковещательные передачи с меньшей интенсивностью, однако позволит повысить достоверность поиска.

4. Момент окончания шторма определяется, как и начало, только при этом фиксируется уменьшение среднего трафика.
5. Форма шторма определяется по усредненным на порт значениям трафика за время шторма. Это возможно потому, что изменение формы широковещательного трафика будет в большей степени отражаться на суммарном трафике, чем изменение трафика на каком-либо одном интерфейсе.
6. Для поиска источника шторма просматривается исходящий трафик на всех сетевых интерфейсах в сети. При этом осуществляется сравнение с шаблоном широковещательного шторма. В качестве критерия соответствия используем коэффициент, основанный на вычислении суммы квадратов отклонений, который оказался эффективным для обнаружения похожих последовательностей трафика при малом количестве отсчетов.

Заключение

Использование рассмотренных выше методов анализа статистики позволяет повысить информированность администраторов о процессах, которые происходят в сети. Средства динамического построения структуры можно интегрировать в систему управления и наблюдения за сетью и тем самым упростить ее администрирование. Возможность обнаружения широковещательных штормов позволит своевременно принимать меры для устранения источника дестабилизирующего воздействия. Актуальными задачами исследования продолжают оставаться повышение достоверности обнаружения штормов и снижение уровня ошибочных срабатываний.

Литература

1. IEEE Standards for Local and Metropolitan Area Networks: Supplement to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Media Access Control (MAC) Parameters, Physical Layer, Medium Attachment Units, and Repeater for 100 Mb/s Operation, Type 100BASE-T (Clauses 21–30). – 1995. – 398 с.
2. ITU-T Recommendation X.200. Information technology – Open systems interconnection – Basic reference model: The basic model. – 1994. – 60 с.
3. Библиотека I2R [Электронный ресурс]. Классификация атак. – 2002. – Режим доступа: www.i2r.ru/static/450/out_14782.shtml, свободный.
4. IETF: RFC1983 Internet Users' Glossary; Под ред. G. Malkin. – 1996.
5. D-Link xStack DES-3500 Series Layer2 Managed Stackable Fast Ethernet Switch CLI Manual. Release 5.1. – 2008 – 318 с.
6. IETF: RFC1157 A Simple Network Management Protocol (SNMP) / J.D. Case, M. Fedor, M.L. Schoffstall, J. Davin. – 1990.
7. RRDtool [Электронный ресурс] / RRDtool tutorial; Alex van den Bogaerdt. – 2009. – Режим доступа: http://oss.oetiker.ch/rrdtool/tut/rrdtutorial.en.html, свободный.
8. Минько А.А. Статистический анализ в MS Excel. М.: Издательский дом «Вильямс», 2004. – 448 с.
9. Казиев В.М. Введение в математику и информатику – Санкт-Петербург: БИНОМ. Лаборатория знаний, Интернет-университет информационных технологий – ИНТУИТ.ру, 2007. – 304 с.
10. Пат. 5,926,462 USA, МКИ^6 H04L 12/28. Method of determining topology of a network of objects which compares the similarity of the traffic sequences/volumes of a pair of devices. David Schenkel, Michael Slavitch, Nicholas Dawes, 16.11.1995, 20.07.1999.
11. IEEE, “802.1AB. IEEE Standard for Local and metropolitan area networks. Station and Media Access Control Connectivity Discovery”, New York. – 2005.

УДК 004.056, 519.246.8

МНОГОШАГОВОЕ ПРОГНОЗИРОВАНИЕ НА ОСНОВЕ АНАЛИЗА ВРЕМЕННЫХ РЯДОВ В ЗАДАЧАХ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК

А.В. Гирик
Научный руководитель – к.т.н., доцент Г.П. Жигулин

В работе предложена схема использования многошаговых прогнозов для обнаружения сетевых атак. Модель основана на формировании нормального профиля показателей и сравнении фактических значений с прогнозными. Выполнена экспериментальная проверка модели и показана её применимость в статистических системах обнаружения вторжений.

Ключевые слова: информационная безопасность, обнаружение вторжений, многошаговое прогнозирование, прогнозирование сетевого трафика

Введение

Значение методов, моделей и средств выявления и идентификации угроз нарушения информационной безопасности передачи данных в телекоммуникационных сетях сегодня трудно переоценить [1]. В условиях непрерывного развития технологий и появления новых угроз разработка методов обнаружения аномалий в СПД является актуальной задачей, имеющей большое практическое значение.

Обеспечение безопасности должно решаться как часть задачи управления сетью и опираться на данные мониторинга. Как правило, эта задача возлагается на специализированный комплекс программных средств, который называется системой обнаружения вторжений (*Intrusion Detection System*, *IDS*). Одной из составляющих процесса оценки безопасности сети является обнаружение аномалий в работе сети как отклонений от нормального поведения трафика. Мониторинг состояния СПД и сравнение фактических результатов с прогнозными позволяет обнаруживать сетевые аномалии и более точно идентифицировать их характер и источник.

Методы обнаружения вторжений, которые используются в IDS, можно разделить на две группы: сигнатурные и статистические. Особый интерес в настоящее время вызывают статистические методы обнаружения вторжений, поскольку с их помощью становится возможным выявлять угрозы, сигнатуры которых не содержатся в базе IDS.
В качестве источников данных для анализа могут выступать: статистика, полученная с активного сетевого оборудования и серверов (SNMP, NetFlow, NetStream, sFlow), данные трассировки, в том числе полученные с помощью анализа сетевых пакетов, уведомления syslog и аналогичных сервисов, в том числе инструментированных приложений [2].

Постановка задачи

В случае систем обнаружения вторжений, использующих статистические методы, интерес представляет построение оперативных прогнозов в режиме рального времени, что прямо вытекает из необходимости скорейшего обнаружения отклонений в работе сети. После того, как данные мониторинга собраны и выполнена их первичная обработка – устранены выбросы и восстановлены пропущенные значения – можно переходить к следующим стадиям анализа данных.

Экспериментальные данные показывают, что многие процессы, протекающие в вычислительных сетях, являются периодическими. В этом случае становится возможным сформировать для каждого источника данных *нормальный профиль* – ряд значений, характеризующих поведение источника в условиях нормального функционирова-

ния. Такой ряд по своей сути является многошаговым прогнозом. Многошаговый прогноз не обязательно должен быть долгосрочным, как правило, количество шагов совпадает с количеством отсчетов в базовом периоде. Данные, которые будут использоваться для построения нормального профиля, назовем обучающей выборкой. Некоторые данные могут быть промаркированы как непригодные для включения в обучающую выборку. Новые данные, представляющие собой контрольную выборку, сравниваются с нормальным профилем, и если регистрируется отклонение, которое по выбранным критериям превышает допустимое [3], то делается вывод о наличии аномалии и вырабатывается предупреждение.

Таким образом, задача состоит в построении модели, учитывающей периодичность процессов, протекающих в телекоммуникационных сетях, возможные тренды, а также дополнительные уточняющие сведения различного характера.

Построение модели

Анализ автокоррелограмм различных источников сетевой статистики позволяет выявить циклические эффекты с периодом 24 часа (сутки) и в некоторых случаях 168 часов (неделя). Для того, чтобы сгладить колебания, перейдем к агрегированному ряду $X^{(m)}$, где m – количество усредняемых отсчетов исходного ряда. Поведение трафика в течение суток повторяет поведение в предыдущие сутки. Пусть $X_k^{(m)}(t,d)$ – k-тый агрегированный отсчет в сутках d, тогда можем вычислить среднее значение трафика в этот момент суток, причем желательно различать рабочие и выходные дни. Приходим к модели вида:

$$F_1(t,m,k) = \frac{1}{N}\sum_{d=1}^{N} X_k^{(m)}(t,d). \qquad (1)$$

Нагрузку, характерную для k-того агрегированного отсчета в определенный день недели, можно описать на основе (6) следующим образом:

$$F_2(t,m,k) = \frac{1}{N'}\sum_{d=1}^{N}[X_k^{(m)}(t,d)\cdot D(\delta,d)], \qquad (2)$$

где $D(\delta,d)$ – функция, принимающая значение 1, если d – день недели $\delta = \{пн, вт, ср, чт, пт, сб, вс\}$; $N' = \sum_{d=1}^{N} D(d)$ – количество таких дней в рассматриваемом ряду. Похожий подход к описанию нагрузки предложен в [4]. Для того, чтобы учесть тенденцию последних w значений, можно использовать линейную регрессию:

$$F_3(t,m,w) = \frac{1}{w}\sum_{i=t-w}^{t-1} \chi_i X_i^{(m)}(t). \qquad (3)$$

Таким образом, можем получить прогноз очередного уровня ряда с помощью модели вида:

$$F(t,m,w) = c_1F_1(t,m,k) + c_2F_2(t,m,k) + c_3F_3(t,m,w), \qquad (4)$$

где c_1, c_2, c_3 – весовые коэффициенты. Отметим, что модели $F_1(t)$ и $F_2(t)$ могут использоваться и для построения прогноза с упреждением в несколько уровней, так как значения k-тых отсчетов вычисляются независимо.

Любой прогноз основан на предположении о том, что события, происшедшие ранее, могут повториться вновь. Простая периодичность выявляется анализом автокорреляционной функции ряда, и модель (4) в большинстве случаев дает удовлетворительные результаты. Нерегулярные события, оказывающие значительное влияние на поведение трафика, не будут учитываться моделью (4).

Испытание модели

Для проверки модели (4) был выполнен ряд экспериментов. Исходные данные были получены путем мониторинга сегмента сети одного из провайдеров Санкт-Петербурга. В течение шести месяцев все L2 коммутаторы, образующие сегмент, опрашивались с помощью средств из пакета net-snmp. Интервал опроса был выбран равным 5 минутам. Сведения о количестве входящих и исходящих байт собирались для каждого порта (интерфейса) каждого коммутатора. В результате для каждого интерфейса были получены трассы значений, содержащие временную метку получения соответствующих отсчетов, усредненную по пятиминутному интервалу скорость передачи для входящего трафика bps_in (в битах в секунду) и усредненную по пятиминутному интервалу скорость передачи для исходящего трафика bps_out (в битах в секунду). В связи с тем, что в некоторые моменты времени из-за потерь пакетов, изменений конфигурации сети или сбоев в работе оборудования, значения bps_in и bps_out не были получены, была выполнена линейная интерполяция пропущенных уровней ряда. Модель (4) была опробована на ретроспективных данных с различными параметрами агрегирования отсчетов и горизонтами прогнозирования.

При работе модели с контрольной выборкой отклонение прогнозных значений трафика от фактических рассчитывалось как $q(t) = \frac{|\hat{x}_i - x_i|}{x_i}$. В случае, если H отсчетов подряд регистрировалась средняя ошибка $e_H(t) = \sum_{j=1}^{H} \frac{q_j(t)}{H}$, превышающая предельное значение $E_{\max}$, то делался вывод об обнаружении аномалии, и соответствующие отсчеты маркировались как непригодные для последующего включения в обучающую выборку.

Основные сложности применения модели связаны с большим количеством *ложных срабатываний* – обнаружением отклонений от нормального профиля, которые не соответствуют какой-либо аномальной активности. Для уменьшения количества ложных срабатываний необходимо увеличивать точность прогнозов. Применительно к рассмотренной модели это может быть сделано за счет придания большего веса компоненту модели $F_3(t,m,w)$, а также переходу к модели авторегресии – скользящего среднего [5].

Заключение

В результате обработки экспериментальных данных было установлено, что предложенная модель позволяет получать приемлемые прогнозы в случае, если обучающая выборка содержит как минимум 60 базовых периодов (т.е. продолжительность мониторинга составляет порядка двух месяцев). Использование данной модели в IDS обеспечивает надежное распознавание атак типа «отказ в обслуживании» и ситуаций выхода оборудования из строя.

Обеспечение информационной безопасности – одна из наиболее актуальных и сложных проблем в современных сетях передачи данных [6]. Разработка средств предотвращения вторжений требует применения статистических методов анализа, позволяющих обнаруживать ранее неизвестные типы атак. В рассмотренном подходе многошаговые прогнозы, построенные на основе анализа временных рядов, используются в качестве базовой модели для обнаружения нештатных ситуаций. Основные усилия должны быть сосредоточены на повышении точности модели и уменьшении количества ложных срабатываний.

Литература

1. Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 года.
2. Гирик А.В. Инструментирование клиент-серверных приложений // Научно-технический вестник СПбГУ ИТМО. Выпуск 19. Программирование, управление и информационные технологии / Главный редактор д.т.н., проф. В.Н. Васильев. – 2005. – № 19. – С. 150–154.
3. Гирик А.В. Многокритериальное прогнозирование в задачах обнаружения сетевых аномалий // Труды XII международной научно-технической конференции «Теория и технология программирования и защиты информации». – 2008. – С. 66 – 70.
4. Papadopouli M., Shen H., Raftopoulos E., Ploumidis M., Hernandez-Campos F. Short-term traffic forecasting in a campus-wide wireless network. – 16th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications, Berlin, 2005. – PP. 165 – 179.
5. Barford P., Plonka D. Characteristics of Network Traffic Flow Anomalies. – Proceedings of ACM SIGCOMM Internet Measurement Workshop, San Francisco, 2001. – PP. 271 – 293.
6. Markoff J. Do we need a new Internet? – New York Times, 2009. – Режим доступа: http://www.nytimes.com/2009/02/15/weekinreview/15markoff.html, свободный.

УДК 681.7.06:681.327.8

РАЗРАБОТКА ВЕРОЯТНОСТНОЙ МОДЕЛИ ФОРМИРОВАНИЯ КЛЮЧЕЙ В СИСТЕМАХ КВАНТОВОЙ КРИПТОГРАФИИ

Д.М. Голубчиков
(Технологический институт «Южного федерального университета» в г. Таганроге)
Научный руководитель – д.т.н., профессор К.Е. Румянцев
(Технологический институт «Южного федерального университета» в г. Таганроге)

Предложена вероятностная модель формирования ключей в системах квантовой криптографии, позволяющая проводить анализ влияния отдельных компонентов на эффективность работы системы в целом. Предложены новые критерии эффективности формирования ключевой последовательности. Построено дерево вероятностей событий для систем квантовой криптографии. Выведены аналитические выражения влияния характеристик модулей системы на качество формируемой ключевой последовательности.

Ключевые слова: вероятностная модель, квантовая криптография, системы распределения ключей

Введение

Квантовая криптография – новое направление развития систем защищенной передачи информации. Системы квантового распределения ключей позволяют двум пользователям гарантированно сформировать общий секретный ключ, который не будет не известен злоумышленнику. Процесс формирования ключей основан на кодировании информации с помощью состояний одиночных фотонов. Основы теории квантового распределения ключей заложили учёные Чарльз Беннет (Charles Bennett) из фирмы IBM и Жиль Брассард (Gilles Brassard) из Монреальского университета, которые 1984 году первыми разработали способ кодирования и передачи сообщений с помощью квантовых состояний [1]. На сегодняшний день ни одна из компаний производящих системы квантового распределения ключей не вышла на уровень серийного производства. При разработке и изготовлении коммерческих реализаций систем квантовой криптографии производители сталкиваются с множеством различных задач. Одной из них является предсказания характеристик изготавливаемой системы. Невозможность точного анализа комплексных характеристик системы является следствием не идентичности применяемых оптических компонентов.

Основной задачей работы является выявление узлов оказывающих наиболее значительное влияние на характеристики систем. Для решения поставленной задачи требуется выбрать и обосновать основные характеристики систем. Компании разработчики систем квантовой криптографии при рекламе своих систем преподносят в качестве основных характеристик систем следующие данные: скорость формирования «сырой» ключевой последовательности и максимальную длину линии связи [2].

В работе предложено в качестве критериев эффективности систем квантовой криптографии использовать вероятностные параметры: вероятность формирования бита ключа и вероятность формирования ошибочного бита. Исходя из приведенных критериев и при известных характеристиках компонентов системы можно скорость формирования просеянной ключевой последовательности и максимальную протяженность квантового канала, а при известном алгоритме «коррекции ошибок» появляется возможность рассчитать скорость формирования итоговой ключевой последовательности.

Дерево вероятностей

В результате анализа структур и принципов функционирования систем квантового распределения ключей [3] было построено дерево возможных исходов при формировании ключевой последовательности системами квантовой криптографии для расчета вероятности формирования бита ключа и вероятности формирования ошибочного бита.

Отображенное на рисунке дерево вероятностей позволяет рассчитать вероятность появления каждого события, влияющего на характеристики системы.

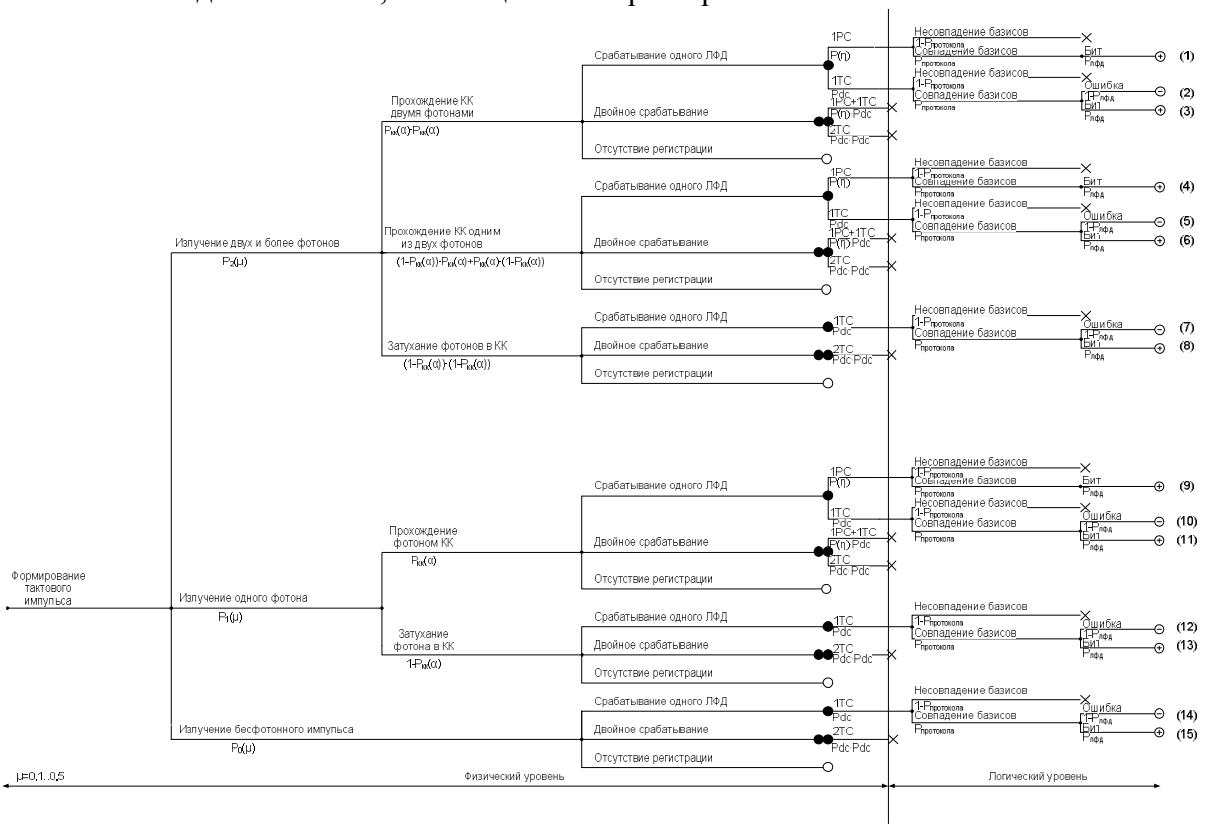


Рисунок. Дерево возможных исходов

Описание ветвей дерева вероятностей

Дерево разбито на две части: одна часть описывает физический уровень работы систем квантового распределения ключей, вторая – логический уровень. Рассмотрим допустимые исходы в вероятностном дереве. Все ветви оканчивающиеся событием формирования бита или ошибки, пронумерованы от 1 до 15.

Ветви с номерами 1, 3, 4, 6, 8, 9, 11, 13, 15, обозначенные «+», приводят к появлению правильного бита в «просеянной» ключевой последовательности. Ветви с номерами 2, 5, 7, 10, 12, 14, имеющие обозначение «–», приводят к формированию ошибочного бита в «просеянной» ключевой последовательности, который должен быть обнаружен и удален на этапе коррекции ошибок.

В соответствии с построенным деревом вероятностей определены возможные исходы работы системы:

(1) формирование ошибочного бита ключа в результате темнового отсчета на выходе однофотонного детектора;

(2) формирование бита ключа в результате темнового отсчета на выходе однофотонного детектора;

(3) формирование бита в результате срабатывания однофотонного детектора вследствие приема однофотонного излучения.

Введем обозначения, которые использованы при подписи ветвей и при расчетах вероятностных характеристик систем квантовой криптографии.

$p_n(\mu)$ – вероятность излучения n фотонов при среднем количестве фотонов на импульс равном μ. Распределение вероятностей описывается законом Пуассона.

$p\left(f_{dc}, \frac{\tau}{T}\right)$ – вероятность появления темнового отсчета на выходе однофотонного детектора, характеризуется частотой темнового счета детектора f_{dc}, длительностью импульсов вольтодобавки τ и период следования импульсов синхронизации T.

$p_{протокола}$ – вероятность совпадения базисов, зависит от выбранного протокола обмена квантовыми ключами.

$p_{лфд}$ – вероятность попадания фотонов на правильный фотодиод.

$p_{кк}(\alpha)$ – вероятность прохождения фотоном квантового канала, зависит от ослабления в квантовом канале α, которое, в свою очередь, является функцией от протяженности квантового канала, погонного затухания на километр оптического волокна и качества прокладки волоконно-оптической линии связи.

$p_n(\eta)$ – вероятность регистрации n фотонов однофотонным детектором, характеризуется квантовой эффективностью фотодетектора η.

В результате анализа событий приводящих к появлению ошибочных битов (события 2, 5, 7, 10, 12, 14) можно заметить, что каждое из них в отдельности зависит от множества параметров:

$$p_{2ош}(\mu, \alpha, f_{dc}, \frac{\tau}{T}) = p_2(\mu) \cdot p^2{}_{кк}(\alpha) \cdot p\left(f_{dc}, \frac{\tau}{T}\right) \cdot p_{протокола} \cdot p_{лфд},$$

$$p_{5ош}(\mu, \alpha, f_{dc}, \frac{\tau}{T}) = p_2(\mu) \cdot 2 \cdot (1 - p_{кк}(\alpha)) \cdot p_{кк}(\alpha) \cdot p\left(f_{dc}, \frac{\tau}{T}\right) \cdot p_{протокола} \cdot p_{лфд},$$

$$p_{7ош}(\mu, \alpha, f_{dc}, \frac{\tau}{T}) = p_2(\mu) \cdot (1 - p_{кк}(\alpha))^2 \cdot p\left(f_{dc}, \frac{\tau}{T}\right) \cdot p_{протокола} \cdot p_{лфд},$$

$$p_{10ош}(\mu, \alpha, f_{dc}, \frac{\tau}{T}) = p_1(\mu) \cdot p_{кк}(\alpha) \cdot p\left(f_{dc}, \frac{\tau}{T}\right) \cdot p_{протокола} \cdot p_{лфд},$$

$$p_{12ош}(\mu, \alpha, f_{dc}, \frac{\tau}{T}) = p_1(\mu) \cdot (1 - p_{кк}(\alpha)) \cdot p\left(f_{dc}, \frac{\tau}{T}\right) \cdot p_{протокола} \cdot p_{лфд},$$

$$p_{14ош}(\mu, f_{dc}, \frac{\tau}{T}) = p_0(\mu) \cdot p\left(f_{dc}, \frac{\tau}{T}\right) \cdot p_{протокола} \cdot p_{лфд}.$$

Все функции вероятности появления ошибочного бита за исключением последней зависят от параметров $\mu, \alpha, f_{dc}, \frac{\tau}{T}$. Параметры $\mu, f_{dc}, \frac{\tau}{T}$ – являются индивидуальными для каждой системы и не зависят от внешних факторов; α – величина ослабления в квантовом канале для каждой системы является параметром внешним и переменным; μ – среднее количество фотонов в импульсе, является собственным параметром излучающего модуля и суммарного ослабления в системе. Частота следования импульсов темнового счета на выходе детектора f_{dc} – собственный параметр детектирующего модуля; $\frac{\tau}{T}$ – собственный параметр системы, зависящий от характеристик детекторного модуля и системы синхронизации.

Для вычисления общей вероятности появления ошибочного бита просуммируем все вероятностные исходы, в результате которых на выходе системы будет продетектировано ошибочное значение бита. После преобразований, вероятность формирования ошибочного бита примет вид:

$$p_{\Sigma ош}(f_{dc},\frac{\tau}{T}) = p\left(f_{dc},\frac{\tau}{T}\right)\cdot p_{протокола}\cdot p_{лфд}\cdot$$

В полученном выражении отсутствуют функциональная зависимость от среднего количества фотонов и от ослабления в квантовом канале, таким образом, суммарная вероятность появления ошибочного бита является собственной функцией системы и её параметры взаимосвязаны с параметрами работы детекторов систем квантовой криптографии и параметрами подсистемы синхронизации.

Анализ вероятности появления ошибочного бита показал необходимость учета параметра τ – длительность импульса вольтодобавки, который связан с длительностью излучаемых импульсов и с дисперсионной характеристикой квантового канала, и параметра T – период следования импульсов вольтодобавки. Так как T для каждой системы квантовой криптографии является фиксированным параметром, то целесообразно провести анализ влияния τ на вероятность появления ошибочных битов при различных длительностях импульсов и протяженностях квантового канала.

Шесть описанных событий приводят к появлению в просеянных ключах ошибок. Полученная зависимость определяет минимальный порог вероятности появления ошибочных битов в просеянной ключевой последовательности.

Однако вследствие срабатывания детекторов из-за появления импульсов темнового счета формируются не только ошибочные биты, но и правильные биты ключевой последовательности.

Суммарная вероятность событий 3, 6, 8, 11, 13, 15, приводящих к появлению корректных битов ключей при регистрации импульсов темнового счета, при условии идентичности характеристик фотодетектирующих модулей, будет равна суммарной вероятности событий регистрации ошибочных битов ключевой последовательности:

$$p_{\Sigma бит.т.с.}(f_{dc},\frac{\tau}{T}) = p\left(f_{dc},\frac{\tau}{T}\right)\cdot p_{протокола}\cdot p_{лфд}\cdot$$

Из полученных данных можно сделать вывод о возможности формирования ключевой последовательности в отсутствии излучения. Однако из сформированной последовательность не возможно будет получить общий секретный ключ, так как процент ошибочных битов в ней составит 50%.

Проанализируем события, приводящие к формированию корректных битов ключевой последовательности, в результате регистрации импульсов содержащих фотоны. Данные события соответствуют ветвям с номерами 1, 4 и 9.

$$p_{1рс}(\mu,\alpha,\eta) = p_2(\mu)\cdot p^2{}_{кк}(\alpha)\cdot p_2(\eta)\cdot p_{протокола},$$

$$p_{4рс}(\mu,\alpha,\eta) = p_2(\mu)\cdot 2\cdot p_{кк}(\alpha)\cdot(1-p_{кк}(\alpha))\cdot p_1(\eta)\cdot p_{протокола},$$

$$p_{9рс}(\mu,\alpha,\eta) = p_1(\mu)\cdot p_{кк}(\alpha)\cdot p_1(\eta)\cdot p_{протокола}\cdot$$

Каждое событие зависит от α – величина ослабления в квантовом канале, для каждой системы является параметром внешним и меняющимся в зависимости от протяжности квантового канала, μ – среднего числа фотонов в импульсе, является собственным параметром излучающего модуля и суммарного ослабления в системе. И η – квантовой эффективности фотодетектора.

Формула суммарной вероятность формирования правильного бита в результате регистрации однофотонного излучения будет включать зависимости от величин α, μ, η:

$$p_{\Sigma бит}(\mu,\alpha,\eta) = p_{протокола} \cdot (p_2(\mu) \cdot p^2{}_{кк}(\alpha) \cdot p_2(\eta) + p_2(\mu) \cdot 2 \cdot p_{кк}(\alpha) \times$$
$$\times (1 - p_{кк}(\alpha)) \cdot p_1(\eta) + p_1(\mu) \cdot p_{кк}(\alpha) \cdot p_1(\eta)).$$

Скорость формирования просеянной ключевой последовательности будет равна суммарной вероятности формирования ошибочного бита ключа в результате темнового отсчета на выходе однофотонного детектора и формирование бита ключа в результате темнового отсчета на выходе однофотонного детектора и формирование бита в результате срабатывания однофотонного детектора вследствие приема однофотонного излучения умноженной на частоту появления оптических импульсов на выходе передающего модуля.

$$\nu_\Sigma(\mu,\alpha,\eta,f_{dc},\frac{\tau}{T}) = \upsilon \cdot (p_{\Sigma ош}(f_{dc},\frac{\tau}{T}) + p_{\Sigma бит.т.с.}(f_{dc},\frac{\tau}{T}) + p_{\Sigma бит}(\mu,\alpha,\eta)),$$

где υ – частота появления оптических импульсов на выходе передающего модуля.

Заключение

При выполнении работы были проанализированы все допустимые события при функционировании систем квантового распределения ключей до этапов коррекции ошибок и усиления секретности. Предложена оценка характеристик систем квантовой криптографии на основе вероятностной модели. По данным анализа построено дерево возможных событий, позволяющее проводить анализ влияния отдельных компонентов системы квантовой криптографии на характеристики всей системы. Получены аналитические выражения взаимосвязи характеристик системы с характеристиками компонентов, а также выражение для расчета скорости формирования просеянной ключевой последовательности.

На следующих этапах работы планируется вывести выражение для расчета максимальной протяженности квантового канала. Провести анализ влияния физических параметров лазерного и фотодетектирующего модулей на характеристики систем. Провести экспериментальную проверку результатов работы на двух квантово-криптографических системах QPN5505, производства фирмы MagiQ Technologies Inc. и Id3100 Clavis, производства компании IdQuantique Inc.

Литература

1. Bennett C., Brassard G. Quantum cryptography: Public key distribution and coin tossing. // Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (Institute of Electrical and Electronics Engineers, New York, 1984). – P. 175–179.
2. Румянцев К.Е., Хайров И.Е. Эффективность волоконно-оптической системы передачи информации. // Научно-практический журнал «Информационное противодействие угрозам терроризма» . – 2004. – №2. – С. 50–52.
3. Голубчиков Д.М. Структура и принципы функционирования системы квантового распределения ключей Id 3000 Clavis. // Известия ЮФУ. Технические науки. Тематический выпуск «Безопасность телекоммуникационных систем». Таганрог: Изд-во ТТИ ЮФУ. – 2008. – №3(80). – С. 149–157.

УДК 681.3.067:621.396.2

КЛАССИФИКАЦИЯ АТАК НА КАНАЛЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧЕЙ

Я.С. Розова
(Технологический институт «Южного федерального университета» в г. Таганроге)
Научный руководитель – д.т.н., профессор К.Е. Румянцев
(Технологический институт «Южного федерального университета» в г. Таганроге)

В работе приведена классификация атак на каналы квантового распределения ключей. Выделено два больших класса методов съема информации: атаки на кубиты и атаки, использующие не идеальность компонентов систем. Приведен анализ основных схем, позволяющих получить информацию о битах ключа. Дана оценка уровня появления ошибочных бит в ключе в случае реализации атак на системы квантовой криптографии.

Ключевые слова: квантовая криптография, классификация, схемы атак

Введение

Одним из наиболее значимых применений принципов квантовой механики является их использование в процессе распределения ключевых последовательностей, необходимых для шифрования конфиденциальной информации. При этом безопасность передаваемой информации гарантируется не математической стойкостью алгоритмов, как это имеет место в классической криптографии, а фундаментальными законами физики. В таком случае, попытка любой третьей стороны осуществить несанкционированный доступ к информации о ключах, приведет к ее разрушению. Такой вывод следует из принципа неопределенности Гейзенберга, применимого к одиночным квантовым объектам, которые являются носителями информации о битах ключей.

Тем не менее, все чаще появляются работы, доказывающие возможность съема информации с квантовых каналов связи. Описано множество теоретических методов несанкционированного доступа к битам ключевых последовательностей в процессе их передачи.

В работе приведена классификация известных стратегий поведения злоумышленника, дано краткое описание схем осуществления атак и оценка вносимых ими ошибок.

1. Классификация методов съема информации

Известные стратегии съема информации можно разделить на две большие группы: атаки на состояния фотонов и атаки, использующие не идеальность компонентов оборудования квантовой криптографии [1].

Первый класс атак состоит в измерении состояния фотонов, что ведет к увеличению числа ошибок. Рассматриваемый класс методов съема информации включает в себя три подкласса: когерентные, некогерентные и комбинированные атаки. Некогерентные атаки подразумевают собой такое действие злоумышленника, при котором для осуществления съема информации происходит взаимодействие с каждым кубитом (фотоном переносящим информацию о бите ключа). К группе некогерентных атак относятся перехватчик-ретранслятор, симметричные атаки и атаки, использующие процесс квантового клонирования [2]. При использовании схем для когерентных атак, Ева использует взаимодействие с массивом кубитов. Комбинированные атаки представляет собой промежуточный подкласс атак, использующий взаимодействие с каждым отдельным кубитом, а измерение проводится над их массивом.

Второй класс атак использует неидеальности оборудования, которое участвует в процессе квантового распределения ключей и состоит из двух подклассов: атаки с по-

мощью светоделителя и атаки мощным импульсом. Реализация атак с помощью светоделителя возможна вследствие применения в схемах квантовой криптографии мультифотонных источников излучения. Стратегии, в которых применяются мощные импульсы, позволяют получить информацию о битах ключа с помощью сканирования состояния оборудования (атаки типа «Троянский конь») или используя аномальное поведение узлов системы (атаки подложными состояниями).

В общем виде, классификация атак приведена на рис. 1.

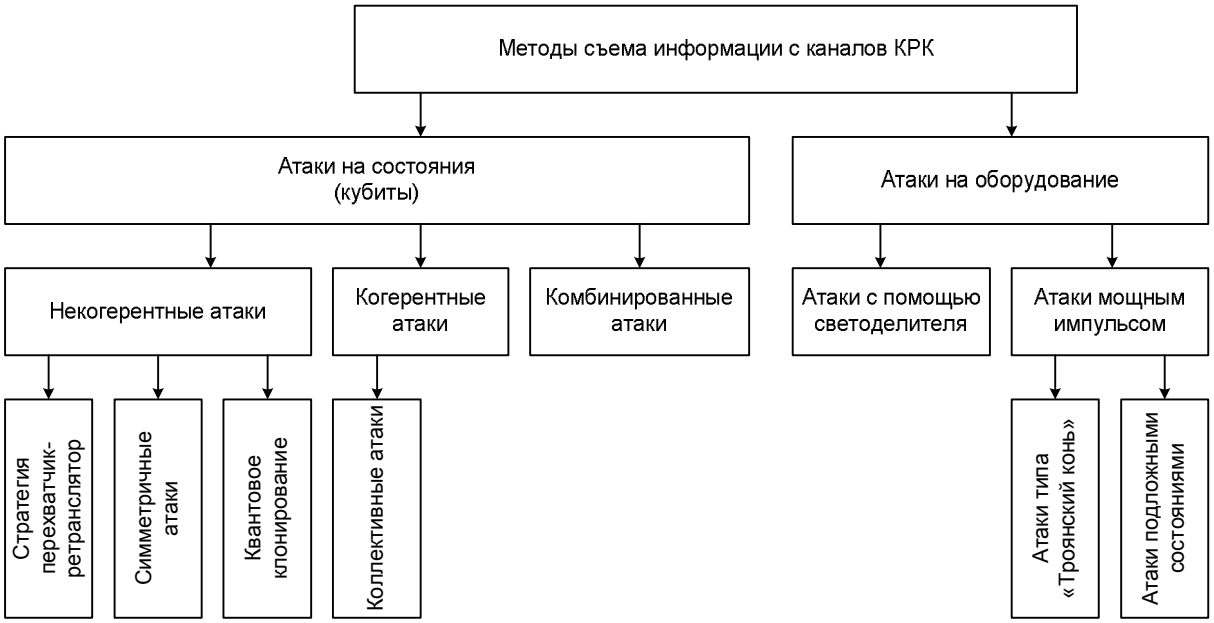


Рис. 1. Классификация атак на каналы квантового распределения ключей

Далее проведен анализ основных схем, позволяющих производить съем информации с каналов квантового распределения ключей.

2. Атаки на состояние

2.1. Стратегия перехватчик-ретранслятор

Стратегия перехватчик-ретранслятор представляет собой наиболее простой и реализуемый на практике метод съема информации (рис. 2).

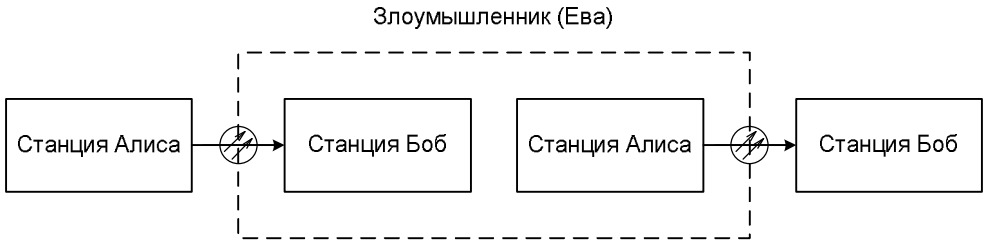


Рис. 2. Схема проведения атаки перехватчик-ретранслятор

Атака состоит в измерении злоумышленником (Евой) каждого кубита в одном из двух базисов, подобно тому, как это происходит в станции Боб. Затем Ева пересылает другой кубит в состоянии согласно своим измерениям по направлению к приемной станции. В половине случаев, она осуществит выбор базиса, который совпадает с базисом, используемым при передаче. В этом случае она пересылает кубит в корректном состоянии и присутствие злоумышленника не будет обнаружено. В остальных 50% случаев, используемый Евой базис несопоставим с состоянием передаваемых кубит и ее присутствие будет замечено по возросшему числу ошибок. Такая ситуация имеет

место по причине отсутствия у злоумышленника какой-либо информации о генераторе случайных состояний станции Алиса (при условии что генератор вырабатывает действительно случайные состояния). Если Ева использует стратегию перехватчик-ретранслятор, она получает 50% информации, в то время как законные пользователи получают около 25% ошибок в просеянном ключе.

2.2. Симметричные атаки

Идея съема информации с квантовых каналов с использованием симметричных атак заключается в использовании произвольных вспомогательных состояний (проб). Структурная схема атаки приведена на рис. 3.

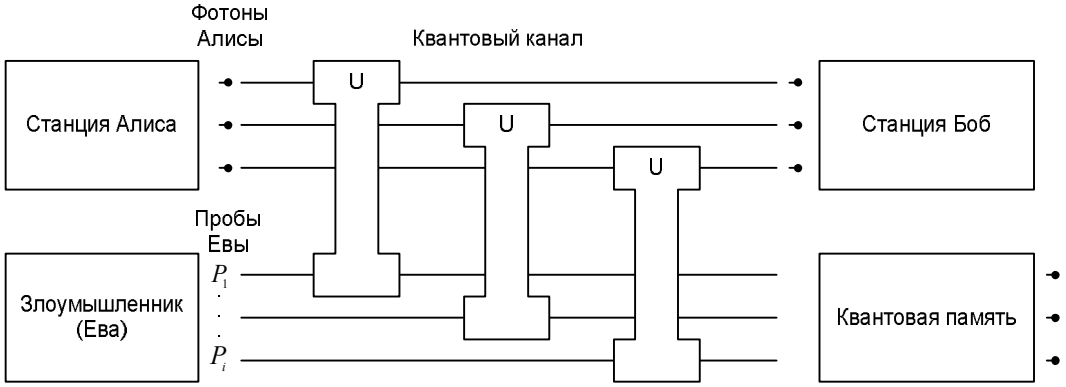


Рис. 3. Схема проведения симметричной атаки

Используемая система проб должна подчиняться законам квантовой механики, т.е. описываться с помощью некоторого Гильбертова пространства. В процессе передачи, злоумышленник осуществляет взаимодействие проб с потоком кубит. Используемое взаимодействие не должно вносить большого числа ошибок в формируемую ключевую последовательность, но при этом быть независимым от состояния кубита и описываться унитарным оператором. После взаимодействия, кубит пересылается по направлению к станции Боб, а пробы сохраняются в квантовой памяти оборудования Евы. Для получения наибольшего количества информации о ключе, злоумышленник должен измерить состояния своих проб после окончания процедуры согласования базисов между законными пользователями. Величина вносимых ошибок при использовании описанной стратегии составляет 15% от длины ключевой последовательности.

2.3. Когерентные атаки

Реализация когерентных атак аналогична случаю симметричных атак, но Ева осуществляет перепутывание пробы произвольной размерности и в любом состоянии со всей последовательностью передаваемых кубит, а не с каждым отдельным кубитом. Она сохраняет пробу большого объема и проводит над ней измерения только после окончания процесса согласования базисов между законными пользователями. Общая схема когерентной атаки приведена на рис. 4.

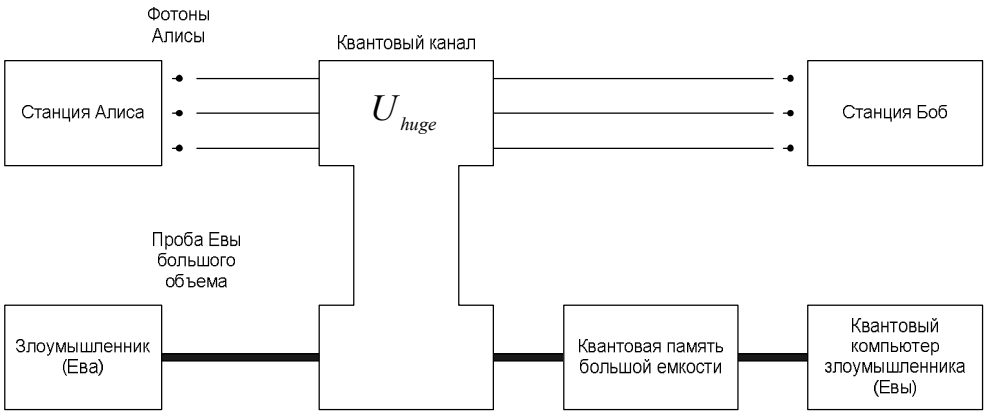


Рис. 4. Схема проведения когерентной атаки

При использовании когерентных атак для съема информации, величина вносимых ошибок составляет 11% от длины ключевой последовательности.

3. Атаки на оборудование

3.1. Атаки с помощью светоделителя

При осуществлении атак на светоделитель, Ева расщепляет все импульсы на две части и анализирует каждую половину в одном из двух базисов (рис. 5), используя устройства счета фотонов, способные различать импульсы с содержанием 0, 1 и 2 фотонов.

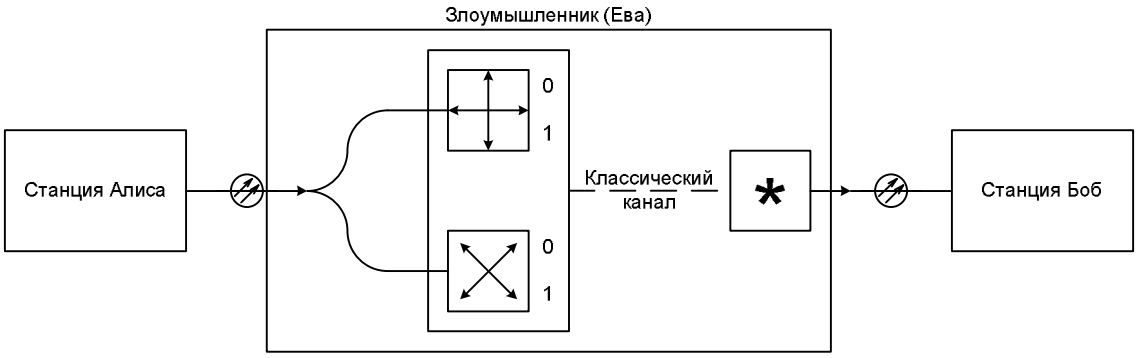


Рис. 5. Схема проведения атаки с помощью светоделителя

Практически эта стратегия может быть реализована при использовании большого числа соединенных параллельно счетчиков одиночных фотонов.

3.2. Атаки типа «Троянский конь»

При осуществлении атак типа «Троянский конь», световые импульсы, излучаемые лазером злоумышленника, разделяются на сканирующий и опорный с помощью разветвителя [3]. Сканирующий импульс распространяется по направлению к станции Алиса или станции Боб через оптический мультиплексор. При отражении от компонентов системы, импульс модулируется в соответствие с их состоянием и поступает на схему детектирования. При этом введено допущение, что Ева использует наиболее чувствительный метод детектирования, который требует наличия опорных импульсов.

Вторая половина разделенного импульса и выступает в качестве опорного сигнала. Она задерживается в опорной схеме детектирования для того чтобы приходить на схему детектирования синхронно со сканирующим. Параметры отраженного импульса определяют ту информацию, которую получит злоумышленник в результате проведения атаки. Оптический мультиплексор необходим для неискажающей передачи фото-

нов от станции Алиса к Станции Боб. Схема осуществления атаки мощным импульсом приведена на рис. 6.

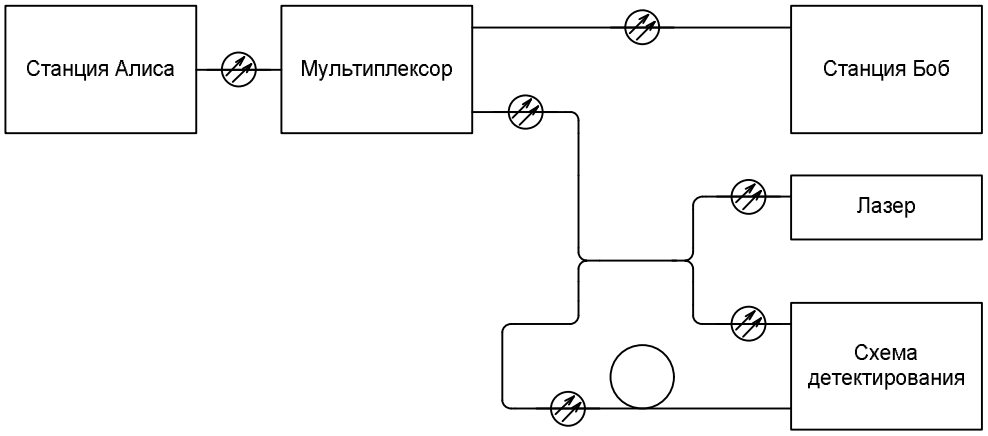


Рис. 6. Схема проведения атаки типа «Троянский конь»

3.3. Атаки подложными состояниями

Один из новых методов взлома систем квантовой криптографии, представляющий собой атаку подложными состояниями был экспериментально продемонстрирован группой исследователей под руководством Вадима Макарова [4–5]. Общая схема эксперимента приведена на рис. 7.

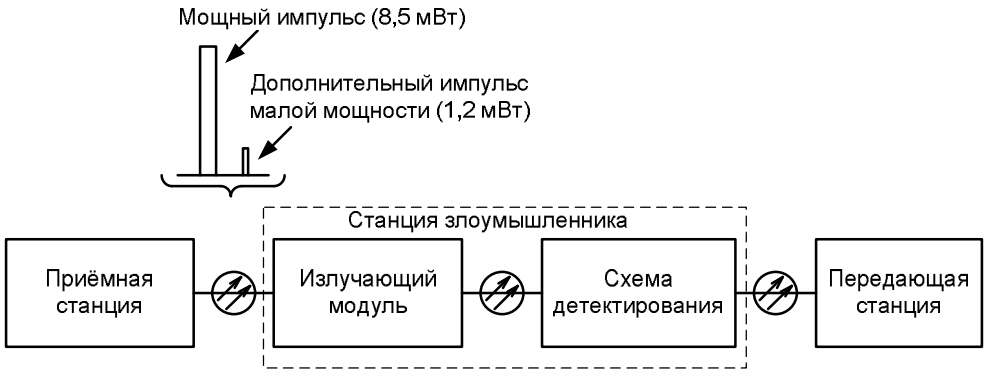


Рис. 7. Структурная схема атаки подложными состояниями

Технология съема информации основана на аномальном поведении приемных модулей SPCM-AQR производства фирмы PerkinElmer, построенных на кремниевых детекторах и используемых в некоторых коммерческих реализациях систем квантовой криптографии.

Злоумышленник может получить полный контроль над процессом формирования ключевых последовательностей, используя световые импульсы с пиковой мощностью порядка 1–10 мВт и длиной волны 780 нм. Воздействие на детекторы системы излучения с приведенными параметрами приведет к появлению тока, величина которого значительно выше по сравнению со штатным режимом работы приёмного модуля. Процессы протекающие в электронной схеме детектора приведут к появлению скачков напряжения смещения, составляющие порядка 12–14 В, что вызывает абсолютную нечувствительность фотодиодов к приходящим одиночным фотонам и темновому току. Детекторы будут регистрировать только подаваемые мощные импульсы.

Таким образом, при использовании в системах квантового распределения ключей протокола BB84, использующего четыре состояния фотона [6, 7], злоумышленник мо-

жет осуществить атаку с помощью пересылки импульсов на определенный детектор. Как только злоумышленник получает контроль над работой приемного модуля системы, он может осуществить атаку перехватчик-ретранслятор и получить полную информацию о формируемых ключевых последовательностях, оставаясь при этом незамеченным.

Взломщика косвенно будет выдавать только приход на приемный детектор паразитных световых импульсов с частотой повторения около 70 кГц.

Заключение

В заключение необходимо отметить, что из всех представленных атак практически в реальных условиях могут быть реализованы стратегия перехватчик-ретранслятор и атаки с использованием мощных импульсов. Но они не обладают высокой эффективностью. Первая вносит большое число ошибок и легко обнаруживается. Предотвратить вторую атаку можно используя специальные схемы детектирования (фотодетектор в токовом режиме с компараторами) или уменьшая интенсивность отраженного импульса. Когерентные, некогерентные и комбинированные атаки не могут быть реализованы на сегодняшний день, так как для их реализации необходимо наличие больших объемов квантовой памяти.

Литература

1. Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden Quantum cryptography //Reviews of Modern Physics. – 2007. – April 1. – 57 p.
2. Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin Quantum cloning //Quantum physic. – 2005. – November 9. – 33 p.
3. Artem Vakhitov, Vadim Mkarov, Dag R. Hjelme Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography //Journal of modern optics. – 2001. – Vol. 48. – No. 13. – PP. 2023–2038.
4. V. Makarov, A. Anisimov, S. Sauge Can Eve control PerkinElmer actively-quenched single-photon detector?: http://arxiv.org/ftp/arxiv/papers/0809/0809.3408.pdf
5. V. Makarov, J. Scaar, A. Anisimov Faked states attack exploiting detector efficiency mismatch on BB84, phase-time, DPSK, and Ekert protocols – Poster on XI International Conference on Quantum Optics. – 2006. – May 26. – PP. 31–30.
6. Слепов Н. Квантовая криптография: передача квантового ключа. Проблемы и решения. Электроника: Наука, Технология, Бизнес №2. – 2006. – С. 54–60.
7. Квантовый протокол BB84: http://qcrypto.by.ru/bb84.html

УДК 681.3.067

ПРОБЛЕМА ПОДГОТОВКИ ПРОФЕССИОНАЛЬНЫХ КАДРОВ ДЛЯ СФЕРЫ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

А.Е. Дудина
(Южно-Уральский государственный университет)
Научный руководитель – д.п.н., профессор Л.В. Астахова
(Южно-Уральский государственный университет)

В настоящее время всевозрастающая значимость аспекта безопасности в каждой без исключения сфере человеческой жизнедеятельности очевидна и особенно проявляется в кризисный период. Данная статья о том, каких специалистов готовит российское государство для обеспечения безопасности в разных сферах жизнедеятельности. Система подготовки профессиональных кадров такого уровня находится на стадии своего становления, поскольку по совокупности причин образовательный процесс пока не охватил все виды безопасности, что и составляет одну из приоритетных задач в области обеспечения внутренней и внешней безопасности государства. А решению поставленной задачи предшествует колоссальная по объему, времени и ресурсам работа.

Ключевые слова: безопасность, кадры, специальности

Введение

Рубеж XIX–XX веков и все последующее XX столетие ознаменовались переходом на революционно новый уровень осознания человеком своего места и роли в природе. Мировые тенденции данного исторического периода – мировые войны, стремительный научно-технический прогресс, экстремизм и терроризм, как крайняя его форма, создание и распространение оружия массового поражения, и многие другие, – заставили человека обратить внимание на такую сторону своей жизнедеятельности как «безопасность», причем в комплексном его понимании, а не только в ее традиционном аспекте – физическая безопасность. Разновекторное развитие человечества приводит к тому, что понятие «безопасность» становится ключевым понятием современной жизнедеятельности и приобретает всевозрастающую значимость на всех уровнях – глобальном, национальном и региональном. Обеспечение безопасности становится в ряд приоритетных задач государственной политики любой страны. Это зафиксировано и в основополагающих нормативно-правовых документах Российской Федерации, с опорой на которые выстраивается курс поступательного развития российского общества.

Основная часть

«В настоящее время Совет Безопасности РФ осуществляет разработку проекта Стратегии национальной безопасности РФ до 2020 года. Последняя, являясь системообразующим документом стратегического планирования обеспечения национальной безопасности, в котором определяются направления функционирования системы обеспечения национальной безопасности, призвана увязать деятельность органов государственной власти, государственных, корпоративных и общественных организаций по защите национальных интересов РФ и обеспечению безопасности личности, общества и государства» [1]. В частности, это касается взаимодействия российского правительства и системы образования.

В уже действующей «Концепции национальной безопасности Российской Федерации» (2000) в Главе II «Национальные интересы» выделены сферы национальных интересов: экономика, внутренняя политика, социальная сфера, духовная сфера, международная сфера, информационная сфера пограничная сфера, военная сфера, экология. В Главе III «Угрозы национальной безопасности Российской Федерации» выявлены угро-

зы в этих сферах. На основе этого, как мы предполагаем, должна выстраиваться и система подготовки кадров.

В системе российского высшего образования создан и функционирует комплекс образовательных учреждений осуществляющих подготовку кадров для сферы безопасности. В Общероссийском классификаторе специальностей по образованию (ОКСО) мы выявили специальности, которые имеют непосредственную связь с понятием «безопасность». Деятельность выпускников этих специальностей направлена на выстраивание и функционирование системы ее обеспечения, а само понятие безопасность содержится в названии специальности и в содержательной ее части, то есть в дисциплинах (см. табл. 1).

Код специальности	Наименование специальности	Наименование квалификации
050000 Образование и педагогика		
050104	Безопасность жизнедеятельности	Учитель безопасности жизнедеятельности
090000 Информационная безопасность		
090101	Криптография	Математик
090102	Компьютерная безопасность	Математик
090103	Организация и технология защиты информации	Специалист по защите информации
090104	Комплексная защита объектов информатизации	Специалист по защите информации
090105	Комплексное обеспечение информационной безопасности автоматизированных систем	Специалист по защите информации
090106	Информационная безопасность телекоммуникационных систем	Специалист по защите информации
090107	Противодействие техническим разведкам	Специалист по защите информации
140000 Энергетика, энергетическое машиностроение и электротехника		
140307	Радиационная безопасность человека и окружающей среды	Инженер-физик
140309	Безопасность и нераспространение ядерных материалов	Инженер-физик
190000 Транспортные средства		
190702	Организация и безопасность движения	Инженер по организации и управлению на транспорте Инженер путей сообщения
280000 Безопасность жизнедеятельности, природообустройство и защита окружающей среды		
280101	Безопасность жизнедеятельности в техносфере	Инженер
280102	Безопасность технологических процессов и производств	Инженер
280103	Защита в чрезвычайных ситуациях	Инженер
280104	Пожарная безопасность	Инженер
280200	Защита окружающей среды	Бакалавр техники и технологии
280200	Защита окружающей среды	Магистр техники и технологии
280201	Охрана окружающей среды и рациональное использование природных ресурсов	Инженер-эколог

280102	Инженерная защита окружающей среды	Инженер-эколог
280302	Комплексное использование и охрана водных ресурсов	Инженер
280402	Природоохранное обустройство территорий	Инженер

Таблица 1. Специальности, имеющие непосредственную связь с понятием безопасность и ее обеспечением

Анализ приведенной выше таблицы указывает на трудности установления соответствия между специальностями подготовки в рамках групп ОКСО и сферами жизнедеятельности, а соответственно и сферы безопасности, которые представлены в «Концепции…». Например, специальность «Организация и безопасность движения» в рамках группы специальностей 190000 «Транспортные средства» и «Безопасность жизнедеятельности» в рамках группы специальностей 050000 «Образование и педагогика» сложно отнести к какой-либо сфере безопасности. Вместе с тем, для других специальностей это соответствие очевидно: «Информационная безопасность телекоммуникационных систем» и «Компьютерная безопасность» – информационная сфера; «Радиационная безопасность человека и окружающей среды», «Безопасность и нераспространение ядерных материалов», «Безопасность жизнедеятельности, природообустройство и защита окружающей среды», «Пожарная безопасность», «Безопасность жизнедеятельности в техносфере» и «Безопасность технологических процессов и производств» – экология.

Выявив специальности, которые непосредственно связаны с определенным видом безопасности и его обеспечением, мы задаемся вопросом, а выпускники каких специальностей призваны обеспечивать безопасность в других сферах жизнедеятельности, выделены в «Концепции …». Вероятно, таковые существуют, однако в названии специальностей понятие безопасность не отражено. Поиск таких специальностей усложняется ввиду прежде обозначенного несоответствия классификаций сфера обеспечения безопасности нормативного документа и ОКСО.

В «Концепции … » подчеркивается, что устойчивое развитие экономики является главным условием для минимизации и ликвидации угроз национальной безопасности, а значит, и реализации национальных интересов российского государства. В этой связи **экономическая безопасность** образует ключевой элемент в системе национальной безопасности государства. Обучение на специальностях группы 080000 «Экономика и управление», как мы предполагаем, направлено на подготовку кадров по созданию и совершенствованию системы обеспечения экономической безопасности в том числе. Однако в результате проведенного анализа государственных стандартов высшего профессионального образования 2 поколения группы специальностей 080000 «Экономика и управление» на предмет наличия дисциплин по безопасности, мы обнаружили, что только 2 специальности из 24, а именно «Налоги и налогообложение» и «Таможенное дело» содержат такой курс как «Экономическая безопасность». При этом на других экономических специальностях изучают такие дисциплины, которые неразрывно связаны с понятием безопасность. Например, «Прогнозирование национальной экономики», «Антикризисное управление», «Товароведение и экспертиза товаров», «Комплексный экономический анализ».

«Во **внутриполитической сфере** национальные интересы России состоят в сохранении стабильности конституционного строя, институтов государственной власти, в обеспечении гражданского мира и национального согласия, территориальной целостности, единства правового пространства, правопорядка и в завершении процесса становления демократического общества, а также в нейтрализации причин и условий, способствующих возникновению политического и религиозного экстремизма, этносепара-

тизма и их последствий – социальных, межэтнических и религиозных конфликтов, терроризма» [2]. Кадры готовят в рамках групп специальностей 030000 «Гуманитарные науки» – «Политология», «История», «Юриспруденция», «Философия», «Религиоведение», «Теология», «Правоохранительная деятельность», «Связи с общественностью», – и 040000 «Социальные науки» «Конфликтология», «Социальная работа». Однако, изучая государственные образовательные стандарты указанных специальностей, самого понятия «политическая безопасность» мы не встретили. Тем не менее, в образовательных программах включены многие дисциплины, которые затрагивают понятие внутренней безопасности государства. Например, «Современные нетрадиционные религиозные движения и культы», «Конфессиональное право», «Политический анализ и прогнозирование», «Прокурорский надзор», «Конфликтология».

В социальной сфере главная конечная цель государства заключаются в достижении высокого уровня жизни народа. Обеспечение **социальной безопасности** должно быть, на наш взгляд, одной из приоритетных задач выпускников следующих групп специальностей 040000 «Социальные науки»: «Социальная работа», «Организация работы с молодежью», «Конфликтология»; 070000 «Культура и искусство»: «Социально-культурная деятельность». А анализ государственных образовательных стандартов указанных групп направлений подготовки не подтверждает, что выпускаемые специалисты готовы к деятельности по обеспечению безопасности в социальной сфере. Только направление «Социальная работа» (бакалавриат) содержит единственную дисциплину в блоке дисциплин специализации «Социальная безопасность». Дополняет эту дисциплину, на наш взгляд, курсы «Основы социальной медицины», «Конфликтология в социальной работе», «Опыт социальной работы с различными группами населения».

Особое место в данном случае занимает группа специальностей 060000 «Здравоохранение» («Лечебное дело», «Педиатрия», «Медико-профилактическое дело», «Стоматология», «Фармация», «Сестринское дело», «Медицинская биохимия», «Медицинская биофизика», «Медицинская кибернетика»). Специалисты названных направлений подготовки призваны стоять на страже здоровья нации, противодействуя многочисленным угрозам национальной безопасности в социальной сфере, например, – «росту потребления алкоголя и наркотических веществ, резкому сокращению рождаемости и средней продолжительности жизни в стране, деформации демографического и социального состава общества и т.д.» [2].

К деятельности по обеспечению безопасности в **духовной сфере** имеют прямое отношение выпускники группы направлений подготовки 030000 «Гуманитарные науки» («Философия», «История», «Культурология» «Искусствоведение», «Религиоведение», «Теология»), а также практически вся группа направлений подготовки 070000 «Культура и искусство». Это обусловлено тем, что профессиональная деятельность этих специалистов направлена, главным образом, на сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны. Рассуждать, таким образом, позволяет анализ государственных образовательных стандартов.

Наряду с обеспечением внутренней безопасности личности общества и государства Российская Федерация в равной степени озабочено и обеспечением своей внешней безопасности. В **международной сфере** наше государство нацелено на «обеспечение суверенитета, упрочение позиций России как великой державы - одного из влиятельных центров многополярного мира, в развитии равноправных и взаимовыгодных отношений со всеми странами и интеграционными объединениями, прежде всего с государствами - участниками СНГ и традиционными партнерами России, повсеместное соблюдение прав и свобод человека и недопустимости применения при этом двойных стандартов» [2]. В этой связи российская система образования осуществляет подготовку кадров по группе специальностей 030000 «Гуманитарные науки», а именно «Междуна-

родные отношения» и «Регионоведение». В образовательном стандарте последней содержится дисциплина «Национальная и региональная безопасность», в образовательный стандарт специальности «Международные отношения» включен курс «Проблемы национальной безопасности и контроль над вооружениями». Другие специальности этой же группы, например, «Востоковедение, африканистика», «Религиоведение», «Теология», «Юриспруденция» «Конфликтология» в своих образовательных стандартах содержат смежные дисциплины по своему содержанию с понятием безопасность. Например, «Конфликтология международных отношений», «Правоохранительные органы», «Государственное законодательство о религии», «Диалог религиозных т нерелигиозных мировоззрений», «Международные экономические отношения».

Приведенная Таблица 1 дает четкое представление о том, каких специалистов готовят для обеспечения **информационной безопасности.**

«Национальные интересы России **в военной сфере и пограничной сфере**, как ее составляющей, заключаются в защите ее независимости, суверенитета, государственной и территориальной целостности, в предотвращении военной агрессии против России и ее союзников, в обеспечении условий для мирного, демократического развития государства» [2]. Специалистов такого уровня готовят в военных и силовых высших учебных заведениях, которые являются специализированными образовательными учреждениями определенных государственных военных и силовых структур Российской Федерации: «(а) Министерства внутренних дел (институты, университеты, академии, а также сеть юридических институтов); (б) Министерства Обороны (Военный институт физической культуры, Военный университет Министерства обороны РФ, Военно-воздушная инженерная орденов Ленина и Октябрьской Революции Краснознаменная академия имени профессора Н.Е. Жуковского Военно-транспортный университет Железнодорожных войск); (в) Министерства Чрезвычайных Ситуаций (Академия Государственной противопожарной службы МЧС России, Академия гражданской защиты МЧС РФ); (г) Федеральной Службы Безопасности (Академия Федеральной службы безопасности РФ, Голицынский военный институт ФПС РФ, Хабаровский Пограничный Институт ФСБ РФ, Московский военный институт Пограничной службы ФСБ России); (д) Федеральной Службы Охраны (Академия Федеральной службы охраны РФ)» [3].

Специалистами по обеспечению безопасности в военной и пограничной сферах являются выпускники групп специальностей 160000 «Авиационная и ракетно-космическая техника», 170000 «Оружие и системы вооружения», 180000 «Морская техника», а также некоторых специальностей группы направлений подготовки 030000 «Гуманитарные науки», например, «Юриспруденция», «Судебная экспертиза», «Правоохранительная деятельность». Очевидно, что в названных специализированных образовательных учреждениях готовят кадры для обеспечения безопасности личности, общества и государства, специальности которых по объективным причинам имеет доступ ограниченного характера.

Кроме выявленных специальностей в группе специальностей и направлений подготовки 280000 «Безопасность жизнедеятельности, природообустройство и защита окружающей среды» (см. Таблица 1), существует ряд специальностей, в рамках которых затронут аспект **экологической безопасности**. Например, это специальности из разных групп 020000 «Естественные науки» («Океанология», «Экология и природопользование», «Экология», «Биоэкология»), 110000 «Сельское и рыбное хозяйство» («Водные биоресурсы и аквакультура», «Защита растений», «Ветеринария») и 190000 «Транспортные средства» («Машины и оборудование природообустройства и защиты окружающей»). Подтверждением тому стало изучение государственных образовательных стандартов.

Анализ государственных образовательных стандартов показал, что выпускники практически всех специальностей выступают объектами обеспечения *собственной* безопасности. Такой курс как «Безопасность жизнедеятельности» или «Основы безопасности жизнедеятельности» содержится в образовательных программах многих рассмотренных специальностей. А предпочтительнее в данном случае было бы, чтобы будущий специалист был субъектом обеспечения определенного вида безопасности или безопасности в одной из сфер человеческой жизнедеятельности. Выполнять роль субъекта подготовлены специалисты групп направлений 090000 «Информационная безопасность», 280000 «Безопасность жизнедеятельности, природообустройство и защита окружающей среды» и специальностей для военной и пограничной сфер.

В результате проведенного исследования по вопросу подготовки государством кадров для обеспечения безопасности в различных сферах жизнедеятельности, классификация которых приведена в «Концепции …» мы можем сделать некоторые выводы. Все рассмотренные специальности можно условно разделить на две группы. К первой мы относим те, которые в своем названии и содержании имеют понятие «безопасность». Это специальности группы 090000 «Информационная безопасность», 280000 «Безопасность жизнедеятельности, природообустройство и защита окружающей среды» и специальностей для военной и пограничной сфер. Ко второй группе относятся все остальные.

Для первой группы характерна насыщенность дисциплинами по безопасности в федеральном компоненте государственных образовательных стандартов. Вторая группа отличается фактическим отсутствием дисциплин такого содержания.

Специалисты первой группы специальностей, исходя из содержания подготовки, выполняют функции субъектов обеспечения безопасности, а второй – субъектов обеспечения собственной безопасности.

Заключение

Анализ специальностей показал, что в большей степени кадрами для безопасности обеспечены такие сферы как информационная, экологическая и военная (пограничная как составная ее часть). Вследствие такой расстановки акцентов на современном этапе увеличивается уязвимость других сфер безопасности. Во многом это обусловлено мировыми тенденциями. Однако есть и специфические проблемы системы отечественного образования (например, отсутствие или неудовлетворительное кадровое обеспечение образовательного процесса), которые требуют безотлагательного разрешения, что в противном случае неминуемо отбрасывает государство на десятки лет назад в отношении уровня подготовки профессиональных кадров.

В соответствии с полученными выводами мы предлагаем следующие пути решения проблем. Во-первых, посредством национально-регионального (вузовского) компонента и дисциплин по выбору студента для второй группы специальностей (выделенной нами) дополнить образовательные программы комплексом дисциплин, которые бы раскрывали понятия «безопасность», «защита», «угроза безопасности» определенный вид безопасности (по отрасли), описывали построение и функционирование системы обеспечения безопасности с учетом специфики субъекта РФ. Это мера призвана придать системе подготовки кадров комплексный характер, то есть будет способствовать движению к единой цели – обеспечению безопасности – с позиций объекта и субъекта. Во-вторых, декларируемую в нормативных документах РФ равнозначность сфер безопасности показать на практике. Это предполагает разработку новых курсов дисциплин в рамках второй группы специальностей, расширение номенклатуры специальностей.

Литература

1. О проекте Стратегии национальной безопасности Российской Федерации до 2020 года [Электронный ресурс]. – Режим доступа: http://www.scrf.gov.ru/news/367.html – Загл. с экрана. – Яз. Рус.
2. Концепция национальной безопасности Российской Федерации [Текст]: от 10.01.00 // КонсультантПлюс. Технология 3000: Версия Проф [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М. – 2008. – (Серия 300).
3. Военные и силовые вузы [Электронный ресурс]. – Режим доступа: http://www.5ballov.ru/universities.city=%C2%F1%E5&type=10013&spec=&find=%C8%F1%EA%E0%F2%FC – Загл. с экрана. – Яз. Рус.

УДК 004.056

ПОИСК УЯЗВИМОСТЕЙ В WEB-ПРИЛОЖЕНИЯХ НА ОСНОВЕ АНАЛИЗА ИСХОДНЫХ ТЕКСТОВ

А.В. Миноженко

Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В данной статье описан метод поиска уязвимостей в Web-приложениях основанный на ручном анализе исходного кода. Приведена статистика по эффективности этого метода в сравнение с автоматизированным поиском. Также рассмотрены основные принципы при анализе исходного кода.

Ключевые слова: уязвимости, web-приложения, анализ, угрозы

Введение

Согласно статистики уязвимостей Web-приложений за 2008 год от компании Positive Technologies среди 10459 Web-приложении в 83% были обнаружены критичные уязвимости, и в 78% случаев из ста в программном обеспечении Web-приложения содержатся уязвимости средней степени риска. Причиной этого является то, что при разработке Web-приложений не достаточно вниманию уделяется вопросам, связанным с защищенность этих систем [1].

Цель этой статьи описать основные принципы поиска уязвимостей в web-приложениях.

Методы тестирования приложений

Существует два метода тестирования приложении «черный ящик» и «белый ящик». К «белому ящику» относится также поиск уязвимостей на основе анализа исходного кода.

Анализ исходно кода может быть произведен вручную или при помощи автоматизированных средств. Разделяют два подхода к анализу автоматизированными средствами — динамический анализ и статический. Динамические анализаторы более эффективны, однако менее распространены, чем статистические из-за своей сложности. Статистические анализаторы более просты в реализации и вследствие чего более распространены, и их можно найти под все распространенные языки. Однако такие средства применяются как вспомогательные средства при ручном анализе из-за множества ложных срабатываний и низкой эффективности. Среди таких средств можно выделить анализаторы кода RATS, ITS4, RATS, PScan, Flawfinder

По данным статистике от компании Positive Technologies вероятность обнаружения уязвимостей в одном Web-приложении (т.е. эффективность оценки защищенности) при его детальном анализе выше, чем при автоматическом сканировании на 26%. Такое соотношение обусловлено, прежде всего, тем, что анализ исходного кода и выполнение ручных проверок позволяет добиться лучших результатов, чем при автоматизированном сканировании. Кроме того, в работах по исследованию Web-приложений ручным способом применяются методы проверки приложений на основе системных журналов, исходных кодов, что увеличивает охват API системы, и как следствие, позволяет получить более объективную оценку защищенности исследуемых систем [1].

Вероятность обнаружения уязвимости различными методами их поиска.

Следовательно, ручной анализ исходных кодов более эффективен, однако не может быть применен при значительных объемах исходных кодов в связи с большими затратами времени.

Проект OWASP занимается вопросами безопасности в web-приложениях. Разра-

батывает документацию и программное обеспечение для анализа безопасности web-приложении. Среди его проектов есть проект «OWASP Code Review Guide», в котором описывается методология поиска уязвимостей в исходном коде. Ниже приведены основные принципы, изложенные в этом руководстве.

Анализ транзакции

Главная часть анализа исходного кода состоит в выполнение анализа транзакции. Приложение получает некие исходные данные и выдаёт другие выходные данные. Прежде всего, нужно определить все входные данные. Например такие как:

- Данные полученные с браузера (Http);
- Cookies;
- Файлы;
- Другие источники.

Так как входные данные изменяют состояние приложения, то с помощью входных данных атакуют web-приложения. Анализ транзакции включает в себя не только данные полученные от пользователя, а так же данные передаваемые между клиентом и сервером [3].

Основные принципы. Что нужно проверять при анализе исходных кодов

Аутентификация:

- убедиться, что все внешние соединения проходят через соответствующие и достаточную форму аутентификации;
- убедиться что все страницы подтверждены требованиям аутентификации;
- убедиться, что вся принимаемая идентификационная информация проходит через метод HTTP «POST» а не HTTP «GET»;
- любая страница находящиеся вне границ аутентификации должна быть проверена на возможность взлома;
- убедиться, что верительные данные не передаются в открытой форме.

Авторизация:

- убедиться, что присутствует механизм авторизации;
- убедиться, что приложение имеет четко определенные типы пользователей;
- убедиться, что используются наименьшие привилегии в операциях;
- убедиться, что механизм авторизации работает должным образом, падает безопасно и не может быть обманут;
- убедиться, что авторизация проверяется на каждый запрос.

Управление Cookies:

- убедиться, что неавторизованная активность не может быть выполнена через манипуляцию с cookie;
- убедиться, что используется надежное шифрование;
- убедиться, что установлен флаг безопасности, чтобы предотвратить передачу через небезопасный канал;
- проверить, что все транзакции в коде проверяют cookie и используют их;
- убедить, что все данные сессии проверяются на валидность;
- убедиться то cookie содержат минимальное количество персональной информации;
- определить все используемые приложением cookie, их имена и необходимость.

Проверка валидности входных данных:

- убедиться, что присутствует механизм проверки валидности данных;

- убедиться что все входные данные, которые могут быть изменены ненадежным пользователем такие как: заголовки http, cookie, скрытые поля, поля ввода – надежно проверяются;
- убедиться, что есть проверка на длину ввода;
- убедиться, что проверка данных происходит на стороне сервера;
- проверить где происходит проверка данных;
- все входящие данные должны проверяться.

Сообщения об ошибках:

- убедиться, что никакие системные ошибки не показываются пользователю;
- убедиться, что ресурсы освобождаются, если происходит ошибка.

Аудит журналов:

- убедиться, что записываются удачные и неудачные попытки авторизации;
- убедиться, что все ошибки записываются в журнал;
- убедить, что никакие важные данные не будут записаны в журнал, такие как: cookie, идентификационные данные.

Криптография:

- убедиться, что важные данные не передаются в чистом виде;
- убедиться, что приложение использует надежные криптографические методы.

Безопасность среды кода:

- проверить приложение на уязвимость к SQL injection;
- проверить, что приложение правильно выделяет память;
- проверить, не содержится ли в коде закомментированной важной информации;
- проверить на возможность ошибки любые вызовы системных функции или открытии файлов.

Управление сессиями:

- проверить где и когда сессия создаётся для авторизованного пользователя и неавторизованного;
- проверить стойкость идентификатора сессии;
- проверить, как хранятся сессии;
- проверить, как приложение отслеживает сессии;
- определить, что приложение делает, если идентификатор сессии неправильный;
- проверить, как сессия завершается.

Заключение

В данной статье были рассмотрены основные методы и принципы при поиске уязвимостей методом анализа исходного кода. Ручной метод анализа исходных текстов является более эффективным по сравнению с автоматизированными средствами при небольших объемах исходных текстов. В дальнейшем возможно создание методики поиска уязвимостей основанной на анализе исходного кода с применением автоматизированных средств.

Литература

1. Дмитрий Евтеев. Статистика уязвимостей Web приложений за 2008 год [Электронный ресурс] http://www.securitylab.ru/analytics/368513.php
2. Web Application Security Consortium, Web Security Threat Classification [Электронный ресурс] http://webappsec.org/projects/threat
3. The Open Web Application Security Project.[Электронный ресурс]

https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project

УДК 004.771

МЕТОДЫ ЗАЩИТЫ СЕТИ ОТ ЕЕ ПЕРЕПРОФИЛИРОВАНИЯ В БОТСЕТЬ СТОРОННИМ ЗЛОУМЫШЛЕННИКОМ. ОБЗОР МЕТОДИК ЗАЩИТЫ И ПРЕДОТВРАЩЕНИЯ DDoS-АТАК

А.Ю. Соломатин
Научный руководитель – д.т.н., профессор Л.Г. Осовецкий

В данной статье кратко описывается актуальность рассматриваемой темы на текущий 2009 г. В статье изложены основные возможности, доступные для преступных групп с использованием ботсети. Методы защиты локальной сети и методы выявления автономно работающего программного обеспечения на клиентских машинных. Представлен обзор аппаратных, программных комплексов и методов защиты по предотвращению DDoS-атак в реальном времени. Предложен возможный путь по искоренению данного вида информационной атаки и повышению защищенности компьютерных сетей.
Ключевые слова: DDoS-атака, информационная безопасность, ботсеть, Cisco

Важность рассматриваемой проблемы на текущий 2009 год

Актуальность рассмотрения проблемы ботсетей в области информационной безопасности на текущий 2009 году заключается в том, что прошедший 2008 год прошел в мире информационной безопасности под знаком ботнетов. Специалисты ведущих фирм в области информационной безопасности концентрировали свое внимание на способах обнаружения и предотвращения заражения компьютера-жертвы. Компания WatchGuard Technologies, одна из ведущих фирм в области решений для обеспечения и построения защищенных компьютерных сетей, анонсировала пятерку ключевых тенденций информационных угроз в компьютерных сетях в 2009 году. Четвертое место в этой пятерке занимает проблема компьютерных ботов и построенных с их помощью ботсетей. Специалисты компании WatchGuard Technologies считают, что в этом году разработчики ботнетов попытаются приложить максимум усилий, для того чтобы их продукт стал более незаметным, более опасным и непредсказуемым [1]. Данные стремления злоумышленников будут способствовать укреплению мощи зомби-сетей и распространению ботов. Создание и владение ботсетями станет еще более прибыльном делом. Единственный способ борьбы и противодействия мощным преступным зомби-сетям должен будет включать в себя широкий спектр средств и методов защиты, и потребует высокого уровня подготовки администраторов сети и специалистов в области информационной безопасности для проведения профилактических и оборонительных мероприятий по обеспечению сохранности данных и устойчивости информационных систем.

Что такое ботсеть?

Ботсеть это компьютерная сеть, которая состоит из N-ого количества хостов. На каждом хосте установлено и запущенно автономно работающее программное обеспечение, на профессиональном языке именуемое ботом. Это программное обеспечение служит для выполнения неких действий с использованием аппаратных ресурсов зараженного компьютера не анонсированных пользователем машины. Боты, чаще всего, создаются и распространяются на компьютеры жертв для осуществления неправомерных действий в области рассылки спама, кражи конфиденциальной информации с зараженного компьютера, а также для организации точечных атак на информационные системы с целью обеспечения их отказа в обслуживании. Отказ в облуживании информационной системы происходит в результате истощения аппаратных ресурсов атакуемой системы избыточными многократными запросами со

стороны распределенного количества клиентов. Данный вид атаки называется DDoS (Distributed Denial of Service) и последние несколько лет получил репутацию наиболее страшного кибернетического оружия интернет-злоумышленников.

Возможности ботсети для преступных групп

Ботсети организуются злоумышленниками для проведения массивных атак на информационные системы крупных предприятий, чья деятельность непосредственно связанна с работай в сети Интернет и предоставлением для пользователей онлайн-ресурсов. Неработоспособность, недоступность этих ресурсов влечет для компании серьезные финансовые потери и открывает для злоумышленников возможность шантажа руководства организации с целью получения финансового откупа от преступных группировок. В качестве примера можно привести информационные структуры банков, веб-ресурсов и приложений.

Методы защиты локальной сети и выявления автономно работающего программного обеспечения на клиентских машинах

Наиболее современные методики проверки, используемые антивирусными средствами для выявления вредоносного ПО, зачастую, не способны обнаружить и искоренить бота злоумышленника на зараженном компьютере. Одна из причин заключается в том, что должно пройти определенное количество времени, прежде чем ботсеть даст о себе знать и заработает в полную силу, предоставив специалистам в области компьютерной безопасности возможность локализации и последующего анализа активированного бота и занесения его в антивирусные базы.

При написании ботов, злоумышленники зачастую используют модульную систему в основе построения его функциональных возможностей, что позволяет дописывать и без труда распространять обновления для уже существующих ботов. Авторы данного вредоносного программного обеспечения зачастую используют механизмы защиты от удаления, аналогичные большинству вирусов и руткитов. Применяются методики маскировки ботов под системные процессы, используется подмена системных файлов для самомаскировки, а также организуются самоперезапускающиеся процессы, которые направлены на перезапуск друг друга. Такие процессы довольно сложно и практически нереально завершить, так как они вызывают следующий процесс и завершают сами себя намного быстрее, чем их успевают завершить принудительно. Существует еще масса различных алгоритмов, и появление новых алгоритмов постоянно растет, делая борьбу с ними, мягко говоря, затруднительной.

Для организации безопасности локальной сети и выявления автономно работающих ботов существуют несколько рекомендаций, направленных на устранение данной проблемы. Заражению вредоносным ПО подвержены не только домашние компьютеры пользователей, но и компьютеры больших организаций. Администраторы сетей порой не считают своим долгом уделять должное внимание очистки собственных сетей от такого рода программного обеспечения, полагаясь полностью на установленные антивирусные решения.

Существует несколько рекомендованных методов и стратегий по защите корпоративной локальной сети от ботов и перепрофилирования ее в зомби-сеть. Первое, что необходимо сделать, это начать с правильной настройки межсетевого экрана, с помощью которого необходимо постоянно отслеживать все попытки генерации мусорного трафика клиентскими компьютерами. Необходимо держать открытыми только те порты на межсетевом экране, которые необходимы для правильной работы установленных приложений. Нельзя пренебрегать анализом

проходящего через сеть трафика и подвергать тщательному анализу немотивированные всплески сетевой активности. Также имеет смысл периодически проверять отдельные компьютеры сети на наличие несанкционнированного подсоединения по IRC каналу с их стороны. Если при просмотре активных соединений хоста результат выполнения команды netstat подтвердит активное соединение, то вероятен шанс того, что данный хост заражен зловредным ботом. Рекомендуется также периодически проверять следующий путь в реестре HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run на наличие подозрительных ключей. При нахождении таких ключей следует их удалять и соответственно удалять выполняющийся файл.

Различными компаниями в области информационной безопасности ведутся довольно успешные программные разработки систем раннего обнаружения ботов в локальных сетях. К таким системам можно отнести такие программные продукты как BotHunter, BotMiner, BotProbe и BotSniffer. Все они действуют с помощью своих уникальных алгоритмов. Но большинство подобных программных продуктов нацелено на анализ сетевой активности отдельных компьютеров в сети. Дело в том, что все боты в один момент демонстрирует одинаковую поведенческую особенность. В один и тот же момент они одновременно начинают опрашивать один заданный ресурс, передавать информацию, сканировать сеть или выполнять другие действия, связанные с передачей пакетов по сети. При этих условиях алгоритмы поведенческого анализа демонстрируют себя с наибольшей эффективностью.

Обзор аппаратных, программных комплексов и методов защиты, способствующих предотвращению DDoS-атак в реальном времени

Попасть под удар DDoS-атаки – один из самых кошмарных сценариев для любого специалиста в области компьютерной безопасности. Распознать DDoS-атаку на свою сеть довольно просто, она влечет за собой замедление работы самой сети и серверов в целом. На сегодняшний день специалистами в области компьютерной безопасности разработаны весьма неплохие методы борьбы с DDoS-атаками. Но все равно, независимо от типа атаки DDoS, разработанные и активно применяемые методы борьбы с ними не обеспечивают требуемое устранение угрозы и непрерывную и надежную работу всех систем.

Специалисты компании Cisco заявляют, что сумели создать полнофункциональное решение по защите от атак DDoS, как указано на официальном сайте компании, и это решение основано на принципах «выявления, переориентации, верификации и пересылки, применение которых гарантирует полную защиту» [2]. Сотрудники компании считают, что их решение защитит наиболее критичные к простою системы от DDoS атак любого типа, включая, что немаловажно, совершенно новые разновидности атак этого типа. «Активные ресурсы устранения позволяют быстро выявить атаку и отделить злоумышленный трафик от легитимного. Поэтому решение Cisco обеспечивает оперативную реакцию на атаки DDoS, скорость которой измеряется секундами, а не часами. Решение Cisco можно легко развернуть рядом с важными маршрутизаторами и коммутаторами, его можно масштабировать, благодаря чему устраняются любые точки возможного сбоя, и не ухудшается быстродействие и надежность существующих сетевых компонентов».

В решении Cisco System по защите от DDoS атак важнейшую роль играют два компонента Cisco – Traffic Anomaly Detector и компонент Cisco Guard.

Рисунок. Аппаратный комплекс Cisco Traffic Anomaly Detector

Первый компонент действует как система пассивного контроля по мониторингу сетевого трафика, направленная на выявление аномалий от базового поведения для заданной сети. Если система считает, что интенсивность IP-пакетов, передаваемых из одного источника, превышает допустимые значения, то она перенаправляет трафик компоненту Cisco Guard. Этот компонент представляет высокопроизводительное устройство для устранения вышеупомянутых атак [2]. Cisco Guard подвергает тщательному пятиступенчатому анализу весь проходящий трафик и выявляет весь злоумышленный трафик для его удаления. В результате удаляется ненужный, мусорный трафик и пропускаются хорошие пакеты, благодаря чему достигается стабильность работы всех сетевых систем и компонентов.

Cisco Guard основан на уникальной патентуемой архитектуре процесса мульти-верификации. Эта архитектура включает в себя 5 стадий по выявлению неблагонадежного сетевого трафика. Первая стадия – это фильтрация трафика, модуль основан на статических и динамических фильтрах DDoS. Статические методы блокируют второстепенный трафик и могут быть настроены системным администратором. Динамические методы вводятся в действие другими модулями на основе проведенного анализа сетевого трафика другими модулями. При этом в реальном времени динамические методы корректируются и изменяются на основе новых данных. Второй модуль системы – это модуль активной верификации, который поверяет на спуфинг все пакеты сети. Третий модуль – распознавание аномалий. Этот модуль выполняет мониторинг трафика, который не был остановлен двумя предыдущими модулями и сопоставляет его с базовым поведением, зафиксированным за определенный период времени. Четвертый модуль, анализ протоколов, который обрабатывает те потоки данных, которые на третьем этапе были признаны подозрительными. Последний модуль системы – это модуль нормирования, в котором заложены ответные меры. Он не допускает, чтобы потоки с аномальным поведением бомбардировали защищаемый объект. Формируется трафик по каждому конкретному потоку и применяет особые меры к источникам, которые потребляют чрезмерный объем ресурсов на протяжении длительного времени [2]. Уникальность системы Cisco Guard заключается еще и в том, что в перерыве между атаками система находится в режиме обучения. Таким способом формируется отчет о нормальном поведении систем и составляется базовый профиль.

Разрушительная сила от DDoS атак продолжает расти, постоянно применяются все более мощные инструменты атаки, поскольку в сети Интернет достаточно уязвимых точек. Требуется постоянная работа в этой области с целью поиска новых инновационных подходов и путей решения этой очень важной проблемы информационной безопасности нашего дня.

Абстрактные пути по искоренению данного вида информационной атаки и повышению защищенности компьютерных сетей

На мой взгляд, проблемы многих информационных угроз существуют в связи с существующей монополизацией рынка программного обеспечения. Большинство компаний работают под операционной системой Windows, и на это нацелены злоумышленники. Существует альтернатива операционной системе Windows – это операционная система Linux. Переход на заявленную операционную систему Linux существенно снизит риски и повысит защищенность информационных и аналитических систем, обеспечит надежную работу аппаратных и программных средств, как в личном секторе, так и в коммерческом. Открытость исходных кодов, модульность и разграниченность операционной системы Linux определяет ее как операционную систем, непригодную для маштабного распростронения жизнедеятельности вредоносных программ. Я не буду вдаваться в подробности этой операционной системы и рассказывать о ее плюсах и минусах, разжигать священную войну между пользователями Linux и Windows, поскольку эта тема уже другой дискуссии.

В настоящем изложении я описал важность проблемы DDoS-атак на текущий 2009 год, рассказал про ботсети и о вредоносных возможностях, которые они представляют для преступных групп, систематизировал основные рекомендации, направленные на обеспечение защиты компьютерных сетей от их перепрофилирования злоумышленником в ботсеть. И с другой стороны, рассказал про активные аппаратные и программные меры, используемые для профилактики и устранения DDoS-атак.

Надеюсь, что вышесказанное найдет своего слушателя и достойное применение.

Литература

1. Информационная безопасность 2009: откуда ждать угрозы? [Электронный ресурс] / Журнал Хакер; Режим доступа: http://www.xakep.ru/post/47084/default.asp, свободный. – Статья. – яз. рус.
2. Предотвращение атак с распределенным отказом в обслуживании (DDoS) [Электронный ресурс] / Сайт компании Cisco, Аналитический материал; Режим доступа: http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900aecd 8011e927_.html, свободный. – Статья. – яз. рус.

ИНФОРМАЦИОННО-ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ (ПЕДАГОГИКА)

УДК 37:004

МОДУЛЬ ДЛЯ ПРОВЕДЕНИЯ ГОЛОСОВЫХ КОНФЕРЕНЦИЙ В СРЕДЕ MOODLE

А.А. Першин
Научный руководитель – д.т.н., профессор Л.С. Лисицына

В работе рассмотрены технологии реализации систем голосовых конференций, приведены принципы разработки и описаны особенности реализации модуля для проведения голосовых конференций в среде Moodle, определены направления работ по усовершенствованию модуля. Особый акцент делается на использовании открытого программного обеспечения для реализации модуля.

Ключевые слова: голосовая конференция, синхронное дистанционное обучение, открытое программное обеспечение

Введение

Интерес к системам синхронного дистанционного обучения в мире постоянно растет [1]. В корпоративном секторе этот интерес вызван необходимостью повышения эффективности обучения и снижения издержек, связанных с обучением персонала. Одним из способов повышения эффективности обучения является смешивание онлайнового и оффлайнового обучения, синхронного и асинхронного обучения [1].

В западных компаниях все чаще проводятся так называемые «вебинары» – занятия в реальном времени, когда преподаватель и обучаемые сотрудники находятся не в одном помещении, а на своих рабочих местах у компьютеров, подключенных к интернету или локальной сети. Общение происходит посредством видео- и аудиотехнологий. Такой способ проведения занятий максимально приближен по условиям общения к традиционным занятиям в классе. Однако, он позволяет сделать занятия более интерактивными и эффективными. Самую важную роль при общении пользователей на таких онлайн-сессиях играет голосовое общение [2, 3].

Для России данная технология является достаточно новой и пока еще широко не применялась в образовательном процессе. Этому препятствовала неразвитость инфраструктуры, недостаточное количество широкополосных каналов доступа в интернет. Однако, можно с уверенностью сказать, что в очень скором времени проблема нехватки быстрого интернета исчезнет.

Уже сейчас в сфере образования осознается востребованность технологий голосового синхронного дистанционного обучения.

Говорить об этом можно, основываясь на опыте подготовки сетевых преподавателей в Ставропольском крае, Калужской области и республики Карелия в 2005-2008 гг. В итоговом отчете о результатах дополнительной подготовки педагогов говорится о том, что возможностей, предоставляемых асинхронными технологиями, такими как форумы, не всегда достаточно для организации эффективного процесса обучения. Также делается вывод о востребованности голосовых технологий и возможности их применения для дистанционного обучения сетевых преподавателей из различных регионов РФ.

Данная технология предоставляет новые возможности для людей с ограниченными физическими способностями, которые по тем, или иным причинам не могут присутствовать на занятиях. Они смогут не только прослушивать выступления лектора, но и задавать вопросы.

Можно сделать вывод, что существует потребность общества в системах дистанционного обучения, предоставляющих возможность проведения голосовых конференций.

Система дистанционного обучения Moodle широко распространена, бесплатна и открыта, используется множеством организаций. Однако, Moodle не предоставляет возможностей для организации и проведения голосовых конференций. Такую функциональность можно добавить в Moodle, если создать специальный программный модуль. И этот модуль был создан.

В данной статье описаны технологии реализации систем проведения голосовых конференций, принципы разработки и особенности реализации модуля для проведения голосовых конференций в среде Moodle.

Подход к разработке модуля

При разработке модуля было решено придерживаться принципов, описанных ниже.

Бесплатность и открытость. Модуль разрабатывается для бесплатной и открытой системы Moodle, также он должен быть доступен для использования и модификации всем желающим без каких либо ограничений. Из этого вытекает, что для разработки модуля необходимо использовать только бесплатные и открытые программные компоненты.

Возможность работы только через браузер без необходимости установки дополнительного программного обеспечения. Модуль должен быть максимально прост в установке, настройке и использовании. Идеальная ситуация, когда обычный пользователь даже не задумывается о необходимости что-то устанавливать и настраивать, он просто заходит в систему Moodle, видит, что в его курсе появилась голосовая конференция, щелкает по ссылке и начинает общаться с остальными.

Кроссплатформенность, возможность работы в разных ОС. В связи с этим принципом предполагается использовать технологию Java.

Доступность для конечного пользователя и простота. В связи с этим предполагается использовать минимальное и достаточное для реализации модуля количество разнородных технологий. Для реализации клиентской части предполагается по максимуму использовать HTML, CSS и JavaScript, так как эти технологии поддерживает любой современный браузер. Компоненты, которые нельзя реализовать с помощью HTML, CSS и JavaScript, реализовывать при помощи какой-либо одной технологии: например Java.

Использование стандартизованных протоколов для связи голосового сервера и голосового клиента. Благодаря использованию стандартизованного протокола появляется возможность использовать любой сервер, который поддерживает данный протокол. Таким образом, модуль избавляется от привязанности к какому-либо конкретному ПО голосовых конференций.

Технологии реализации систем голосовых конференций

В общем случае системы голосовых конференций реализуются по клиент-серверной технологии.

Сервер голосовых конференций решает следующие задачи:

- организация обмена голосовыми сообщениями между участниками конференции;
- декодирование и кодирование голосовых данных;
- микширование голосовых данных;
- управление составом участников конференции;
- объединение участников конференции в группы (комнаты);
- управление этими группами [4].

Голосовой клиент – приложение, которое соединяется с голосовым сервером и обменивается с ним голосовыми сообщениями. Голосовой клиент обеспечивает выполнение следующих функций:

- запись речи участника с микрофона;
- воспроизведение речи участников;
- кодирование и декодирование речи;
- выбор приоритетного кодека;
- отправка и прием данных [4].

Обмен сообщениями между клиентами и сервером обычно происходит с использованием таких стандартизованных протоколов, как Session Initiation Protocol (SIP) или H.323, но могут использоваться и другие протоколы.

Существует несколько подходов к реализации голосового клиента.

Первый вариант – это отдельное приложение, которое пользователь самостоятельно скачивает, устанавливает и настраивает. К недостаткам такого подхода можно отнести отсутствие кроссплатформенности и зависимость от операционной системы, что означает, что для каждой операционной системы и платформы необходимо создавать свою версию данного приложения. Возрастает сложность и стоимость поддержки и обновления такого приложения, также могут возникать трудности с установкой и настройкой.

Другой вариант – так называемый, «web-based» или браузерный голосовой клиент – компонент, который запускается прямо в браузере пользователя, причем настройки соединения берутся этим компонентом прямо из HTML-кода страницы. Таким образом, стадии установки и настройки исчезают. Такой компонент можно реализовать с использованием таких технологий как Adobe Flash и Java.

Описание разработанного модуля

Созданный модуль позволяет организовывать и проводить голосовые конференции, а также управлять конференцией во время ее проведения. Для участия в конференции необходим только браузер с Java-плагином, наушники и микрофон.

Ведущий заносит информацию о предстоящей конференции в систему, затем формирует список участников и в оговоренное время начинает конференцию. Участники конференции щелкают по специальной ссылке и попадают в виртуальный конференц-зал, где могут общаться с помощью голоса, а также обычного текстового чата.

На рис. 1 представлен интерфейс виртуального конференц-зала с точки зрения ведущего. На рисунке можно увидеть список участников с индикаторами присутствия, а также управляющими ссылками для блокировки и отключения участника.

Все события, происходящие во время конференции, заносятся в лог. Также логируется и текстовый чат. В дальнейшем предполагается добавить функцию записи конференции на голосовом сервере, чтобы каждый участник мог скачать её и прослушать. Лог событий конференции, текстового чата и звуковая запись конференции с одной стороны нужны ведущему для оценивания работы участников, если за конференцию предполагается выставлять оценки, а с другой стороны могут пригодиться самим участникам, а также тем, кто не участвовал в конференции.

Модуль состоит из следующих компонентов, представленных на рис. 2:

- серверной PHP-части, относящейся к системе Moodle, ответственной за организацию конференции и управление участниками во время ее проведения;
- браузерного голосового клиента, обеспечивающего возможность обмена голосовыми данными с сервером голосовых конференций;
- сервера голосовых конференций, обеспечивающего обмен голосовыми сообщениями между участниками конференции;
- браузерного приложения, реализованного с помощью JavaScript, работающего в

связке с серверной частью, обеспечивающего возможность управления конференцией в реальном времени, а также дополнительные возможности для участников конференции, такие как текстовый чат.

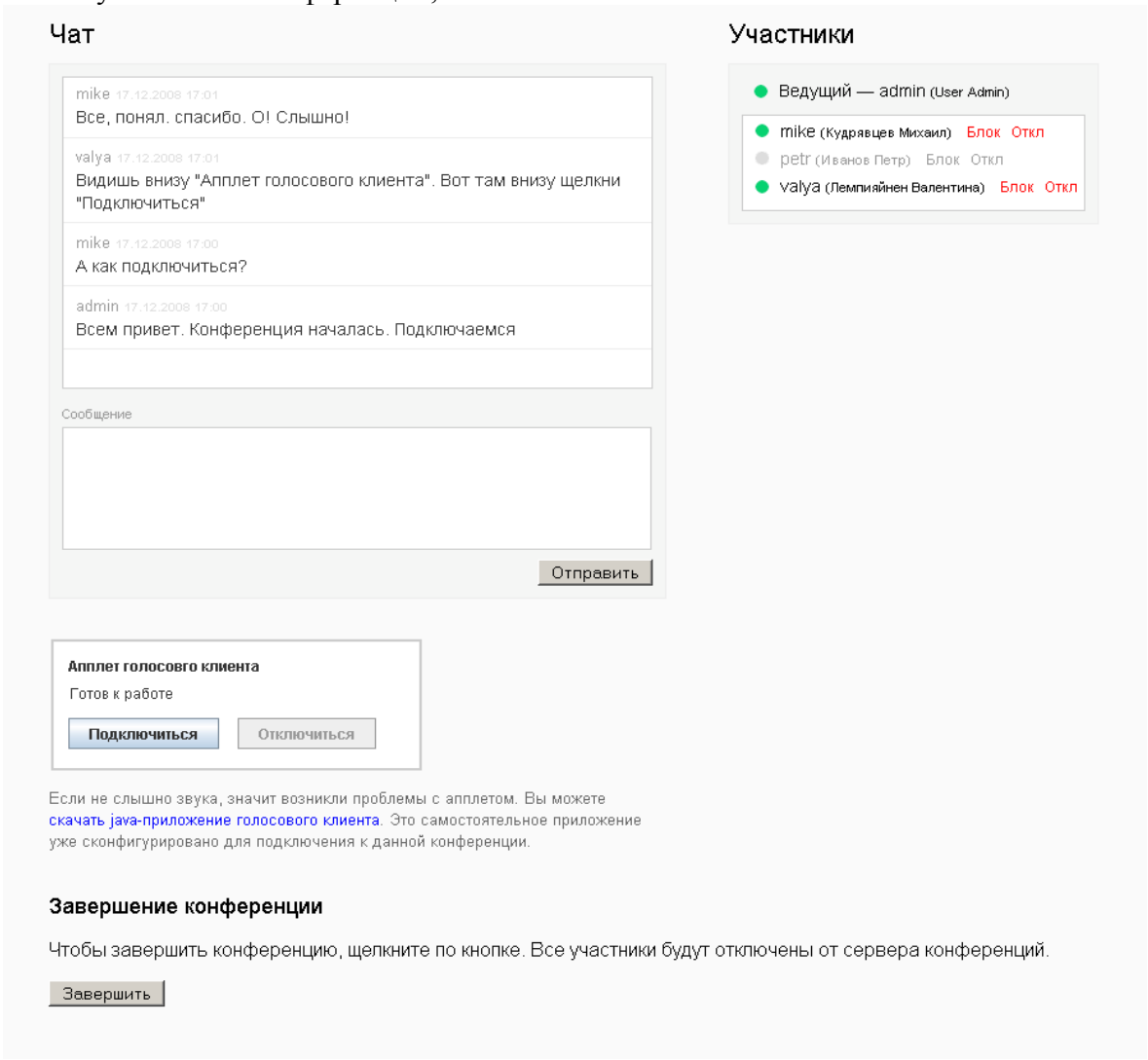


Рис. 1. Интерфейс виртуального конференц-зала

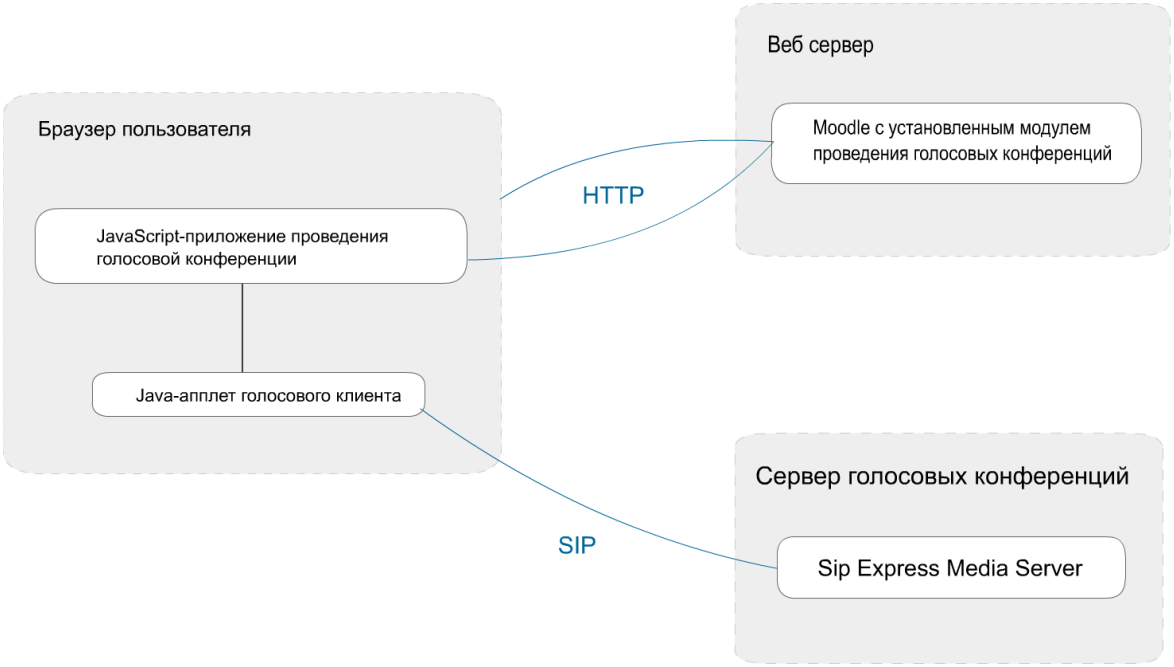


Рис. 2. Компоненты модуля

Модуль разработан в соответствии с требованиям Moodle по разработке модулей, такими как структура файлов и папок, объектно-ориентированный подход к разработке, наличие XML-описания структуры базы данных и другими [5].

Особенностью реализации модуля является использование шаблонизатора для формирования HTML-кода страниц, что является огромной редкостью в модулях Moodle. Использование шаблонизатора позволило отделить программный код на PHP от шаблонов, содержащих HTML-код и специальную разметку. Таким образом, появилась возможность изменять внешний вид приложения, не изменяя программный код, что привело к повышению гибкости системы, уменьшению вероятности возникновения ошибок, повышению скорости разработки.

Для реализации клиентской части использовался открытая JavaScript библиотека jQuery.

Апплет голосового клиента создан на базе открытого голосового клиента MjSip UA. MjSip UA использует открытую библиотеку MjSip, которая является реализацией стека протоколов SIP на Java. Апплет конфигурируется с помощью параметров соединения, заданных в HTML-тэгах <param>. При нажатии на кнопку «Подключиться» апплет присоединяется к заданной конференции на заданном сервере.

В качестве сервера голосовых конференций был выбран SIP Express Media Server или SEMS. Это открытый сервер для Voice over IP-приложений на базе протокола SIP, поддерживающий возможность проведения голосовых конференций. Сервер был выбран благодаря его простоте, а также благодаря тому, что есть возможность протестировать функцию проведения голосовых конференций прямо на сайте производителя.

Заключение

В работе были рассмотрены технологии реализации систем голосовых конференций, принципы разработки и особенности реализации модуля для проведения голосовых конференций в среде Moodle.

Данный модуль можно использовать в учебном процессе кафедры КОТ, как для проведения занятий с использованием голосовых технологий, так и просто для неформального общения учеников.

Работа над модулем продолжается. Усовершенствование модуля планируется вести по следующим направлениям:

- наращивание дополнительных возможностей, например, запись в mp3 голосовых конференций;
- совершенствование кодеков, используемых для передачи аудиоданных;
- добавление возможности использовать видео.

Планируется разместить модуль вместе со специально подготовленной документацией в репозитории модулей Moodle и постепенно совершенствовать, основываясь на отзывах пользователей.

Литература

1. Смешанное обучение: смешивание методов [Электронный ресурс] – Режим доступа: http://www.distance-learning.ru/db/el/960DE7EBAAEA091CC325737C002E2918/doc.html, свободный. – Загл. с экрана.
2. Мифы и реальность синхронного обучения [Электронный ресурс] – Режим доступа: http://www.distance-learning.ru/db/el/97398A007D535B12C32572FD0031072E/doc.html,

свободный. – Загл. с экрана.
3. Системы компьютерной видеоконференцсвязи [Электронный ресурс] – Режим доступа: http://masters.donntu.edu.ua/2007/ggeo/kulinchenko/library/book2.htm, свободный. – Загл. с экрана.
4. Голосовые коммуникации в виртуальных образовательных средах [Электронный ресурс] – Режим доступа: http://ifets.ieee.org/russian/depository/v10_i4/html/2.htm, свободный. – Загл. с экрана.
5. Development:Developer documentation – MoodleDocs [Электронный ресурс]: документация для разработчиков Moodle – Режим доступа: http://docs.moodle.org/en/Developer_documentation, свободный. – Загл. с экрана.

УДК65.050.2

ИСПОЛЬЗОВАНИЕ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ-ДОКУМЕНТОВЕДОВ

П.В. Беспалова
(Южно-Уральский государственный университет)
Научный руководитель – д.п.н., профессор Л.В. Астахова
(Южно-Уральский государственный университет)

Одним из современных подходов российского образования сегодня можно считать компетентностный подход, который предполагает формирование необходимых компетентностей специалистов. Одной из них является информационно-технологическая компетентность, формирование которой возможно при практико-ориентированном обучении. Одним из важных направлений в современном документационном обеспечении управления является внедрение новых информационных технологий: систем автоматизации делопроизводства и электронного документооборота. Поэтому в подготовке специалистов-документоведов необходимо использовать названные программные продукты для формирования жизненно важной информационно-технологической компетентности.

Ключевые слова: информационно-технологическая компетентность, компетентностный подход, система электронного документооборота, информационные технологии, документационное обеспечение управления

Введение

Вхождение России в современное информационное общество сопровождается коренными изменениями в различных сферах деятельности. В связи с этим определяется актуальная проблема, связанная с модернизацией профессионального образования. Современные реалии предъявляют новые требования для высшей школы – подготовка специалистов, обладающих профессиональной компетентностью. Особое место в образовании сегодня занимает компетентностный подход, акцентирующий внимание на результате образования, причем в качестве результат рассматривается не сумма усвоенной информации, а способность человека действовать в различных проблемных ситуациях [1].

Основная часть

В условиях глобальной информатизации общества информационно-технологическая компетентность является одной из жизненно необходимых компетентностей для социальной и профессиональной деятельности человека.

Необходимость формирования IT-компетентности у будущих специалистов-документоведов обусловлена рядом факторов:

- наличие информационно-документационной базы в любой организации;
- активное использование и внедрение новых информационных технологий, в том числе систем автоматизации делопроизводства и электронного документооборота (СЭД), в различных сферах деятельности;
- формирование информационного пространства на уровне предприятия.

Современный работодатель отчетливо понимает, что переход от бумажных технологий управления к электронным жизненно необходим. При этом ему требуется специалист, выполняющий функции системного технолога при использовании и внедрении систем автоматизации делопроизводства и электронного документооборота. Разработчики соответствующих программных продуктов в роли системного технолога видят именно специалиста по документационному обеспечению управления.

Системный технолог настраивает систему электронного документооборота в соответствии с бумажным, описывает маршруты движения и виды документов, обеспечивает работу остальных пользователей системы, настраивает систему на текущие изменения в структуре и документообороте организации. Во многом его функции переплетаются с функциями начальника службы документационного обеспечения управления организации.

Системным технологом должен быть работник предприятия, знающий принятый для данного предприятия порядок документооборота и обладающий навыками работы с компьютером [2]. К сожалению, уровень IT-компетентности такого работника не всегда позволяет выполнять подобные функции, и руководителям предприятий часто приходится место системного технолога занимать IT-специалистом, хотя это в корне является неверным решением.

Одним из основных аспектов реализации компетентностного подхода в образовании является усиление прикладного (практического) характера образования [3]. В данном случае практическим аспектм будет использование СЭД в управлении документацией предприятия.

Основной упор на изучение систем электронного документооборота при подготовке по специальности «Документоведение и документационное обеспечение управление» делается на дисциплине «Компьютерные информационные технологии документационного обеспечения управления», которая входит в федеральный компонент. Соотношение лекционных занятий и практических часов по учебному плану 1:3. Во время изучения курса студенты получают знания по классификации СЭД, защите информации в таких системах, оценке эффективности внедрения систем автоматизации управления, по анализу рынка соответствующих программных продуктов. Однако при формировании информационно-технологической компетентности необходимы в большей степени практические занятия. Для этого необходимо внедрять учебные версии систем электронного документооборота. Причем, необходимо использовать максимально возможное количество таких программных продуктов. Организацию практических занятий целесообразно проводить с использованием активных форм обучения. Примером может быть деловая игра «Электронный офис», в которой студенческая группа является аналогом организации. При этом с заданной периодичностью необходимо менять роли в игре: от системных технологов до технических исполнителей.

Бесспорным лидером рынка систем автоматизации делопроизводства и электронного документооборота сегодня является система «ДЕЛО» компании «Электронные офисные системы», которая занимает около 50% российского рынка. Кроме того, именно эта компания первой начала активное сотрудничество с российскими вузами по программе «Электронный документооборот со студенческой скамьи». На сегодняшний день компании-разработчики СЭД по примеру «ЕОС» предоставляют учебные версии бесплатно, или по льготным условиям для вузов (системы «Летограф», «Евфрат», Lotus-Notes и т.д.). Как правило, функции системы в учебных версиях несколько ограничены, однако их бывает достаточно для практико-ориентированного обучения.

Еще одной особенностью сотрудничества с компаниями-разработчиками СЭД является их готовность бесплатно обучить преподавателей работе в системе. Для этого организуются семинары, деловые игры и т.д.

Кроме того, одним из принципов российского образования является преемственность. Этот принцип можно использовать в рамках подготовки по отдельной специальности. Например, в учебном плане по специальности «Документоведение и документационное обеспечение управления» дисциплины по формированию информационно-технологической компетентности распределены с 1-го

по 5-й курс дисциплины: «Информатика», «Информационные системы», «Глобальные сети», «Вычислительная техника и программирование», «Компьютерные информационные технологии в ДОУ», «Автоматизация деятельности кадровой службы». Этот принцип преемственности также может быть реализован при выполнении сквозных курсовых проектов, переходящих в выпускную квалификационную работу.

Заключение

Исследования, проводимые на базе кафедры «Информационная безопасность» Южно-Уральского государственного университета, показали, что использование в учебном процессе систем электронного документооборота при подготовке документоведов существенно повышает уровень информационно-технологической компетентности. Кроме того, это является необходимым условием для качественной подготовки по специальности «Документоведение и документационное обеспечение управления», а выполнение этого условия ускорит процесс профессиональной адаптации выпускников и увеличит их конкурентоспособность на рынке труда.

Литература

1. Никитина Е.Ю., Афанасьева О.Ю. Педагогическое управление коммуникативным образованием студентов вузов: перспективные подходы [Текст]: монография/ Е.Ю. Никитина, О.Ю. Афанасьева. – Москва: МАНПО, 2006. – 154 с.
2. Система автоматизации делопроизводства и электронного документооборота «ДЕЛО. Версия 8.8». Руководство пользователя. Том 1.
3. Иванов Д.А., Митрофнов К.Г., Соколова О.В. Компетентностный подход в образовании. Проблемы, понятия, инструментарий: Учебно-метод. пособие. – М.: АПКиПРО, 2003. – 101 с.

УДК 681.3.067

ОСОБЕННОСТИ ФОРМИРОВАНИЯ КУЛЬТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ФЕДЕРАЛЬНЫХ ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ

А.Е. Кулемина
(Южно-Уральский государственный университет)
Научный руководитель – д.п.н., профессор Л.В. Астахова
(Южно-Уральский государственный университет)

В статье рассматриваются проблема понятия «культура информационной безопасности», а также особенности процесса формирования культуры информационной безопасности в федеральных органах государственной власти. Кроме того, в статье выделены и сформулированы мероприятия по повышению уровня культуры информационной безопасности в федеральных органах государственной власти.
Ключевые слова: Информационная безопасность, культура, органы государственной власти

Введение

Одним из наиболее важных факторов, определяющих развитие современного общества, является информационная революция. Во многом благодаря ее результатам существенно расширились возможности реализации права человека на свободу информационной деятельности как в каждой отдельной стране, так и во всем мире. Возникли качественные изменения в содержании национальных интересов, национальной и международной безопасности, в методах их обеспечения. Национальные интересы многих стран мира стали включать в себя активное участие в формировании информационного общества и связываться с развитием глобальной информационной инфраструктуры, с созданием и использованием современных информационных технологий в целях обеспечения устойчивого экономического роста, поддержания национального согласия, укрепления демократии и стабильности в международных отношениях.

В современных условиях наблюдается растущая зависимость государственных органов, предприятий, других организаций и индивидуальных пользователей от информационных технологий в плане осуществления своих функций, ведения дел, обмена информацией, предоставления товаров и услуг. Информация стала ценным активом для физических лиц, предприятий, организаций и государств. Когда важные данные не удаётся эффективно защищать, под угрозой находится личная безопасность людей, безопасность бизнеса и, что ещё важнее, национальная безопасность государств [1].

Следовательно, становится важной проблема защиты ценной информации. Однако не всегда еще приходит четкое понимание того, что информационная безопасность – это комплексная проблема. Подходить к ней необходимо с нескольких сторон и рассматривать в разных аспектах. Многие до сих пор считают, что достаточно построить только мощную программную или техническую защиту ценной коммерческой информации. Однако это не так. По мере всё большего вовлечения стран в процесс развития глобального информационного общества происходит осознание того, что информационную безопасность нельзя обеспечить с помощью одной только техники. Эффективное решение возникающих проблем зависит не только от действий государственных или правоохранительных органов, но и от превентивных мер и поддержки во всем обществе. Государственные органы, предприятия, организации, индивидуальные владельцы и пользователи продуктов ИТ-индустрии должны знать о факторах, угрожающих информационной безопасности, и возможных превентивных действиях, должны сознавать свою ответственность и принимать меры для повышения

безопасности информационных технологий. Именно с этой целью в современном обществе должна быть сформирована культура информационной безопасности [1].

Определение понятия культура ИБ

Определим понятие «культура информационной безопасности», которое связано с понятиями информационной и корпоративной культуры. Направление это новое, ещё не исследованное, но, судя по публикациям, активно развивающееся.

Приведем несколько определений понятия «культура», хотя это понятие очень многогранно. Культура (лат. cultura, от корня colere – «возделывать») – обобщающее понятие для форм жизнедеятельности человека, созданных и создаваемых человеком в процессе эволюции. Культура – это нравственные, моральные и материальные ценности, умения, знания, обычаи, традиции. Таким образом, культура- это определённая форма деятельности, результатом которой являются ценности (нравственные, моральные, материальные и т.д.) [2]. Можно сказать, что культура – это своего рода процесс создания. Процесс создания информационной безопасности. Что же такое информационная безопасность?

В последнее время возрастает внимание государства к информационным технологиям и, особенно к информационной безопасности.

Информационная безопасность – понятие более широкое, чем просто безопасность информации или защита информации. Информационная безопасность- это вообще состояние защищённости интересов личности, общества, государства в информационной сфере. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений (Доктрина информационной безопасности РФ) [3]. С другой стороны информационная безопасность – это состояние защищенности субъектов информационных отношений, включающее в себя качественную информационную среду (защищенность субъектов от негативных информационных воздействий) (Информационно-психологическая безопасность) и защищенность их информации (Безопасность информации) и обеспечивающее полное удовлетворение информационных потребностей субъектов (Деятельностный подход). Т.е. ИБ включает в себя два аспекта: ИПБ и БИ.

Культура ИПБ непосредственно близка к понятию корпоративной культуры. Понятие «корпоративная культура» на сегодняшний день имеет несколько формулировок. Оно включает в себя множество взаимосвязанных элементов, которые дополняют друг друга и составляют основу для успешного функционирования компании. Корпоративная культура состоит из идей, взглядов, основополагающих ценностей, которые разделяются членами организации. Однако нам необходимо рассматривать корпоративную культуру в рамках федеральных органов государственной власти. Государственная служба опирается на систему ценностей, которые должны способствовать развитию духовной культуры государства и общества в целом. Сами по себе культурные ценности не могут быть ни хорошими, ни плохими, однако они могут способствовать или препятствовать реализации определенных целей и задач, решаемых обществом. И если исходить из того, что целью является кардинальное повышение эффективности государственной службы в интересах развития гражданского общества и укрепления государства и его информационной безопасности, то с этих позиций нужно подходить к изучению культурных факторов [4].

Опыт развитых демократических государств показывает, что корпоративная культура, обеспечивающая эффективность и управляемость системы государственной службы, должна включать служение общественному благу, профессиональную

компетентность, стабильность, гласность в осуществлении профессиональной деятельности, социальную ответственность за свои действия, дисциплинированность [4].

Повышение уровня корпоративной культуры российской государственной службы, формирование в ней целесообразных ценностных ориентации, установок, норм, отношений является важным условием эффективного функционирования государственной службы на благо общества, в том числе формирования информационной безопасности.

Ценностную основу государственной службы составляет не только динамично развивающаяся совокупность нормативных ценностей Конституции Российской Федерации, ценностей российской ментальности, но и корпоративные ценности, ориентированные на цели и стратегии демократического и правового государства и информационного общества.

Корпоративные ценности являются внутренним стержнем корпоративной культуры государственной службы, действенной стороной «коллективного сознания». Поэтому, формирование внутри государственной службы адекватной ее предназначению и роли этической среды, превращается в важное средство оздоровления общества и формирования позитивной ценностной ориентации нового поколения чиновников. Формирование корпоративной культуры в органах государственной власти заставляет чиновников более серьёзно и осмысленно относится к своим обязанностям и существенно повышает информационную безопасность личности [4].

Формирование корпоративной культуры в органах государственной власти как составной части культуры ИБ должно способствовать повышению внутреннего взаимодействия государственных служащих. Каждый служащий какого-либо ведомства должен осознавать свою ответственность за сохранность информации ограниченного доступа, с которой он работает. Особенностью формирования корпоративной культуры в органах государственной власти является тот факт, что она призвана повышать устойчивость государственных служащих к вредным психологическим воздействиям со стороны общества (например, коррупция, превышение должностных полномочий). Теперь рассмотрим вторую составляющую понятия культуры информационной безопасности.

Она, на взгляд автора, связана с информационной культурой. Что же это такое? Проблема изучения информационной культуры очень актуальна в наш век технологий и информационных потоков. В широком социокультурном контексте рассматриваются такие феномены, как информационное общество, информатизация, информационное образование и др. Проблема формирования информационной культуры личности и изучение специфики информационного поведения, как отдельных людей, так и социальных групп, в этих условиях приобретает особое значение. Понятие информационной культуры в настоящее время достаточно четко оформлено институционально. При Международной Академии Информатизации (МАИ) существует Отделение информационной культуры. Понятие информационная культура состоит из двух трудноопределимых терминов «культура» и «информация». Исходя из этого, можно выделить «культурологический» и «информационный» подходы к трактовке понятия информационная культура. В рамках культурологического подхода информационная культура рассматривается как способ жизнедеятельности человека в информационном обществе, как составляющая процесса формирования культуры человечества. В рамках информационного подхода большинство определений подразумевает совокупность знаний, умений и навыков поиска, отбора, анализа информации, то есть всего того, что включается в информационную деятельность. В современных исследованиях информационной культуры преобладает информационный подход, поскольку данная проблематика пришла в науку из информационной сферы. Информационная культура – это совокупность системных сведений об: (а) основных методах представления и добывания знаний; (б) умениях и навыках применять их на практике. Эти пункты

реализуются с использованием современных информационных технологий. Иными словами информационная культура – это культура обращения со знаниями, данными и информацией, которые сосредоточены на компьютерах сети Интернет [5].

Спецификой формирования информационной культуры в федеральных органах государственной власти является курс на построение информационного общества в Российской Федерации и внедрение информационных технологий в систему государственного управления. При этом вопрос обеспечения информационной безопасности встаёт достаточно остро.

Информатизация российского общества помимо явных плюсов имеет свои минусы. В рамках информатизации в федеральных органах государственной власти можно отметить широкое распространение использования информационно-телекоммуникационных технологий, формирование электронного правительства и т. д.

Особенность обеспечения информационной безопасности в органах государственной власти заключается в том, что при необходимости сохранять конфиденциальность информации ограниченного доступа, циркулирующей в данных структурах, нужно не забывать о конституционном праве граждан «свободно искать, получать, передавать, производить и распространять информацию любым законным способом» (п. 4 ст. 29 Конституции Российской Федерации). С этой точки зрения информационная культура в органах государственной власти играет важную роль. Процесс информатизации в федеральных органах государственной власти закреплен в определенных правовых документах, одними из них являются Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года (одобрена распоряжением Правительства РФ от 27 сентября 2004 г. N 1244-р) и Стратегия развития информационного общества в Российской Федерации (Утверждена Президентом Российской Федерации В.Путиным 7 февраля 2008 г., № Пр-212) [6].

Согласно Стратегии развития информационного общества в РФ основной целью является использование информационных технологий в деятельности федеральных органов государственной власти для повышения эффективности государственного управления на основе создания общей информационно-технологической инфраструктуры, включающей государственные информационные системы и ресурсы, а также средства, обеспечивающие их функционирование, взаимодействие между собой, населением и организациями в рамках предоставления государственных услуг [7]. В рамках реализации Программы до 2010 г. ожидается: утверждение основных стандартов использования информационных технологий в деятельности органов государственной власти; внедрение информационных технологий, обеспечивающих для органов государственной власти возможность интерактивного информационного обслуживания граждан и организаций; подключение федеральных органов государственной власти к единой защищенной телекоммуникационной инфраструктуре, обеспечение эффективного и защищенного информационного обмена и электронного взаимодействия федеральных органов государственной власти между собой, с населением и организациями; внедрение систем электронного документооборота с использованием электронной цифровой подписи в органах государственной власти; внедрение в органах государственной власти комплексных информационных систем управления кадровыми, финансовыми и материально-техническими ресурсами; повышение квалификации пользователей и обслуживающего персонала по использованию информационных технологий; формирование основных государственных информационных ресурсов и обеспечение доступа к ним; обеспечение доступа граждан к информации о деятельности федеральных органов государственной власти; применение Интернета в деятельности органов

государственной власти. Безусловно, на федеральном уровне наблюдается значительное продвижение в выполнении поставленных задач [8].

К аспектам формирования информационной культуры органов государственной власти из перечисленного выше можно отнести в первую очередь повышение квалификации пользователей и обслуживающего персонала по использованию информационных технологий, создание правил использования ИКТ и Интернета. В условиях формирующегося российского информационного общества, обеспечение открытости и прозрачности государственной службы невозможно без должной квалификации государственных служащих в области ИКТ (компьютерной грамотности, информационной культуры). Государственный служащий является информационным посредником между обществом и институтами государственной власти и должен обладать необходимыми навыками и знаниями при использовании современной техники. Соответствие квалификационных требований к государственным служащим современным реалиям является важной гарантией реализации основных прав и свобод человека и гражданина при взаимодействии с органами государственной власти [9].

Формирование культуры ИБ в органах государственной власти

Таким образом, мы выяснили, как понимать две составляющие термина «культура ИБ» в рамках федеральных органов государственной власти, теперь необходимо определить, как формируется на основе этих составляющих культура ИБ в данных структурах.

Понятие культуры информационной безопасности находится как раз на стыке информационной и корпоративной культур. Культура ИБ – это совокупность сведений о том, как создать и сохранить информационную безопасность личности, т.е. состояние защищённости индивида от вредных воздействий (информационно-психологическая безопасность) и как создать состояние защищенности информации, принадлежащей индивиду (безопасность информации). Также культура ИБ – процесс создания и сохранения состояния защищенности индивида и его информации от вредных воздействий на основе имеющихся знаний, навыков и умений, а также постоянное их совершенствование, приводящее к полному удовлетворению информационных потребностей. Исходя из определения данного понятия, можно сказать, что процесс формирования культуры ИБ в федеральных органах государственной власти складывается из процессов создания и повышения корпоративной и информационной культур. Однако не все мероприятия относятся к этому процессу, а только те, которые касаются информационной безопасности. Формирование культуры информационной безопасности в органах государственной власти относится к гуманитарным проблемам информационной безопасности.

Подход к формированию культуры ИБ в федеральных органах власти должен быть комплексным, должны быть задействованы все механизмы обеспечения данного процесса.

Так как это направление новое, то, конечно, существует ещё множество недостатков, тормозящих процесс формирования культуры ИБ в органах государственно власти. К ним можно отнести недостаточное развитие нормативно-правовой базы в данной сфере, неопределенность режима служебной тайны, недостаточная активность федеральных органов государственной власти в информировании общества о своей деятельности, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан.

Федеральными органами государственной власти прилагаются определённые усилия для преодоления трудностей и недостатков, мешающих формированию культуры ИБ. Однако предстоит еще многое сделать.

К мероприятиям по формированию и повышению культуры ИБ в федеральных органах власти можно отнести следующие:

- совершенствование законодательства Российской Федерации, регулирующего отношения в области взаимодействия федеральных органов государственной власти в целях обеспечения информационной безопасности;
- создание и чёткая эксплуатация правил формирования и использования федеральных информационных ресурсов;
- создание организационной, кадровой и ресурсной базы системы мониторинга угроз информационной безопасности федеральных органов государственной власти, использование его результатов при оценке информационной безопасности для государственных структур;
- развитие системы контроля действий государственных служащих по работе с информацией;
- совершенствование нормативной правовой и методической базы в области защиты государственных информационных систем и ресурсов, формирование единого порядка согласования технических заданий на обеспечение информационной безопасности государственных информационных систем и ресурсов;
- повышение квалификации и организация обучения государственных служащих, разработка специальных образовательных программ по вопросам информационной безопасности;

На наш взгляд, одним из наиболее важных механизмов повышения компетентности и формирования культуры ИБ все-таки является обучение госслужащих тому, как ценить безопасность, ответственно использовать компьютерные технологии, как реагировать на инциденты, связанные с нарушением информационной безопасности, как и кому, сообщать об инцидентах нарушения ИБ.

Заключение

Таким образом, нами сформулированы особенности формирования культуры информационной безопасности в федеральных органах государственной власти:

– при необходимости сохранять конфиденциальность информации ограниченного доступа, циркулирующей в органах государственной власти, нужно не забывать о конституционном праве граждан на получение открытой информации;

– государственным служащим в отличие от сотрудников не государственных организаций необходимо формировать более высокую устойчивость к вредным информационно- психологическим воздействиям;

– в органах государственной власти создана благоприятная почва для формирования культуры ИБ в связи с тем, что некоторые её элементы уже созданы, наработаны за прошедшее время.

В статье мы также выделили мероприятия, необходимые для решения проблем в области формирования культуры ИБ в органах государственной власти.

Полагаем, что реализация названных мероприятий будет способствовать повышению уровня культуры информационной безопасности государственных служащих. Одним из ключевых субъектов решения этих непростых задач является специалист по защите информации, получивший профессиональное образование по специальности «Организация и технология защиты информации».

Литература

1. Герасименко В.А. Обеспечение информационной безопасности как составная часть информационных проблем современного общества [Текст] // Безопасность информационных технологий. – 1998. – № 2. – С. 41–50.
2. Соционика, психология и межличностные отношения: человек, коллектив, общество [Текст]: информ.-аналит. журн. / учредитель ЗАО "Паруса". – 2001, июнь. – М.: Паруса, 2001. – Двухмес. – ISSN 1684-8152.
3. Доктрина информационной безопасности Российской Федерации [Электронный ресурс] / Российская газета; ред. Фронин В.А. – Режим доступа: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm, свободный. – Загл. с экрана.
4. Гендина Н.И. Информационная культура личности [Текст]: учеб-метод. пособие в 2-х частях / Н.И. Гендина, Н.И. Колкова, Г.А. Стародубова. – Кемерово: Сибирский писатель. – 1999.
5. Антонова С.Г. Информационная культура личности [Текст]: вопросы формирования. // Высшее образование в России – 1994. — № 1. – С. 82 –87.
6. Райков А.Н. Развитие России и единое информационное пространство [Текст] / Росийский фонд фундаментальных исследований. // «Вестник РФФИ». – 1999. – № 3. – С. 29–34.
7. Стратегия развития информационного общества в Российской Федерации [Электронный ресурс] / Российская газета; ред. Фронин В.А. – Режим доступа: http://www.rg.ru/2008/02/16/informacia-strategia-dok.html, свободный. – Загл. с экрана.
8. Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года [Электронный ресурс] / Российская газета; ред. Фронин В.А. – Режим доступа: http://www.rg.ru/2004/10/07/konzepciya-it-doc.html, свободный. – Загл. с экрана.
9. Стрельцов А.А. Региональные проблемы обеспечения информационной безопасности России [Текст] // Информационное общество. – 2003. – № 4. – С. 7–9.

УДК 004.418

ИНТЕГРАЦИЯ ОБРАЗОВАТЕЛЬНЫХ И СОЦИАЛЬНЫХ ФУНКЦИЙ ШКОЛЫ В WEB-СИСТЕМЕ JUNIOR U

А.В. Беляев, М.И. Гаврилов, А.Н. Ситников
Научный руководитель – к.т.н., доцент Э.В. Денисова

В статье рассматриваются типы социальных сетей: сетей общего назначения и нишевых сетей. Дано обоснование целесообразности создания школьной социально-образовательной сети. Рассмотрены функциональные особенности и аспекты реализации подобной сети Junior U – WEB-сайта, являющегося социальной сетью с образовательным уклоном.
Ключевые слова: web, социальная сеть, дистанционное обучение

Введение

Современные наиболее популярные социальные сети рассчитаны на широкую аудиторию и объединение людей по интересам в них происходит с помощью механизма групп. Подобные социальные сети общего назначения обладают схожей функциональностью:

- группы (круги, сообщества);
- блоги (заметки, журналы);
- сообщения;
- медиа (фотографии, видео, аудио).

Одновременно развиваются так называемые нишевые социальные сети, которые рассчитаны на более узкую целевую аудиторию, предоставляя некоторые специализированные сервисы для данной аудитории:

- подбор персонала;
- сервисы знакомств;
- коллективные блоги.

Нишевые социальные сети обеспечивают удобное взаимодействие пользователей с учетом специфики их деятельности. Образовательные сайты для учебных заведений и для дистанционного обучения обычно предоставляют следующие функции:

- разделение ролей (учитель, ученик);
- дневники;
- расписания занятий;
- журнал оценок;
- система раздачи заданий и сбора выполненных заданий;
- коллекция материалов (библиотека).

Идея объединить социальную сеть общего назначения с образовательным сайтом, т.е. создать специализированную (нишевую) социальную сеть для образования появилась относительно недавно. Если, скажем, для системы высшего образования польза подобного объединения сомнительна, то для школы есть некоторые очевидные и неочевидные плюсы.

Концепция безопасности

Для детей школьного возраста критическим аспектом работы в Интернете и в социальной сети в частности является безопасность:

- ограничения на контент;
- ограничение возможностей третьих лиц на общение с детьми;
- отсутствие анонимных угроз.

Данные аспекты безопасности сложно обеспечить в социальной сети общего назначения, т.к. регистрация открыта для всех. Сложно также обеспечить верификацию возраста и идентифицировать регистрируемого.

Концепция Junior U, объединяя в себе функции социальной сети и образовательного сайта, позволяет решить проблему безопасности школьников. Для этого вводятся следующие роли:

- ученик;
- учитель;
- родитель ученика.

Для пользователей действуют правила регистрации:

- учитель регистрируется на сайте, указывая свою школу;
- его учетная запись активизируется администратором сайта по звонку в школу;
- учитель может регистрировать учеников и их родителей.

Таким образом, учетные записи учителей связаны с конкретными учителями. Учителя подписывают на сайт учеников и родителей, также обеспечивая соответствие пользователя типу учетной записи.

Ограничения на контент работают автоматически, т.к. учителя и родители имеют возможность контролировать контент, созданный учениками. Более того, коль скоро каждая учетная запись связана с конкретным человеком, он несет ответственность за созданный контент в полной мере. Нежелательные элементы не могут зарегистрироваться на сайте ни в качестве учителей (из-за верификации), ни в качестве школьников или родителей (последних регистрирует учитель). Анонимные угрозы отсутствуют, т.к. за каждой учетной записью стоит конкретный человек.

Функциональность

Как уже было сказано, на сайте есть три типа пользователя: ученик, учитель, родитель. Часть функций доступна всем типам пользователей, часть функций могут выполнять лишь определенные типы пользователей. Социальные функции, разумеется, доступны всем:

- заметки с возможностью комментирования;
- фотографии с возможностью комментирования;
- сообщения;
- профайлы (странички, где пользователь может указать различные данные о себе: имя, возраст, фото и т.д.).

Важным аспектом сайта является сущность школы. Для всех школ автоматически создаются профайлы, с указанием контактных данных школы и ее директора. Пользователи-ученики и пользователи-учителя при регистрации ассоциируются с одной из школ. Учителям доступны следующие функции:

- регистрация учеников школы и их родителей;
- создание классов из учеников школы;
- рассылка заданий в классе;
- ведение журнала оценок класса.

Ученики, как основные (по количеству) пользователи системы, имеют следующие возможности:

- доступ к персональному расписанию;
- просмотр своих оценок;
- просмотр своих классов и их свойств;
- возможность загрузить файл выполненного задания к заданию учителя;
- доступ к профайлам своих родителей.

Родители, помимо общего контроля за контентом, могут делать следующее:

- смотреть профайлы своих детей;
- контролировать успеваемость своих детей, просматривая их расписание и оценки.

Реализация

Описанная функциональность была реализована с использованием современных WEB-технологий: Взаимодействие этих технологий в виде компонентов представлено на рис. 1.

Технология	Назначение
Python	Основной язык программирования серверной логики [1]
PostgreSQL	Сервер баз данных [2]
JuniORM	Собственная библиотека для организации ORM с кэшированием в Memcache
Memcache	Распределенный кэш для объектов ORM и отрендереных страниц [3]
Nginx	Фронт WEB-сервер и балансировщик нагрузки [4]
CherryPy	WSGI-сервер для бекэнда [5]
Mako	Рендерер HTML, XML страничек [6]
PIL	Библиотека обработки графических файлов
SimpleJson	Сериализатор JSON
FormEncode	Верификатор данных форм
Psycopg2	Библиотека доступа к PostgreSQL из Python

Таблица 1. Используемые технологии

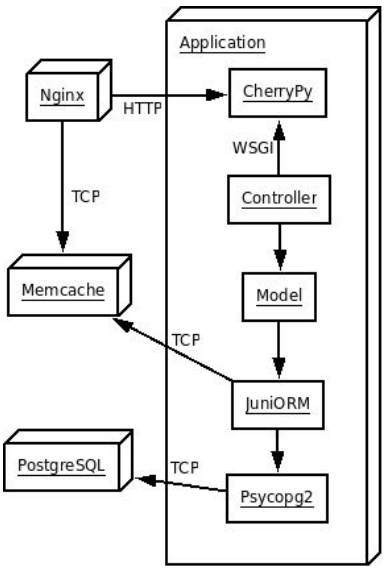


Рис. 1. Взаимодействие технологий и компонентов

Параллелепипедами на диаграмме обозначены процессы, а прямоугольниками – компоненты и библиотеки. HTTP запрос поступает на WEB-сервер Nginx, который, в свою очередь, смотрит, есть ли нужный прокэшированный запрос в распределенном кэше Memcache. Если есть, то выдает результат оттуда, если нет, то передает запрос в процесс приложения по протоколу HTTP. Внутри процесса приложения WEB-сервер CherryPy по протоколу WSGI вызывает методы контроллера, который, обрабатывая параметры запросов и используя модель, генерирует ответ. Модель для хранения данных в базе данных использует ORM (Object-Relational Mapper) JuniORM. JuniORM использует распределенный кэш Memcache для кэширования объектов базы данных. Тем самым облегчается нагрузка на базу данных и увеличивается общая производительность приложения. JuniORM использует библиотеку Psycopg2 для взаимодействия с сервером базы данных PostgreSQL. Подобная архитектура позволяет масштабировать приложение на несколько физических машин, как показано на рис. 2.

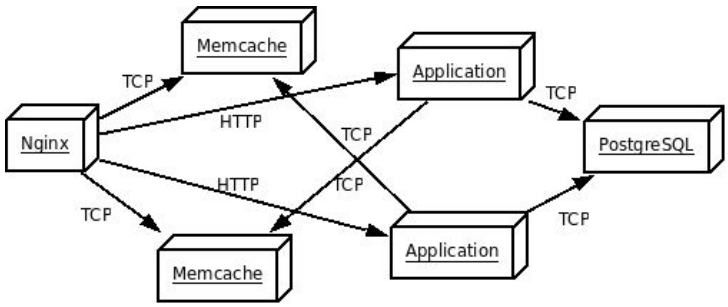


Рис. 2. Масштабирование

Процессы Application и Memcache присутствуют в нескольких экземплярах. Распределение процессов по физическим машинам может быть, например, следующим. Первая машина – балансировщик нагрузки с Nginx. Вторая и третья машины – серверы приложений и распределенного кэша. Каждая из них содержит процессы Memcache и Application. Четвертая машина – сервер базы данных с процессом PostgreSQL. Подобная схема масштабирования называется горизонтальным масштабированием, поскольку позволяет увеличивать производительность системы, просто добавляя машины. Горизонтальное масштабирование хорошо освещено в статьях [7].

Заключение

В статье дано обоснование наличия ниши для школьных социальных сетей. На примере проекта Junior U рассмотрены функциональные особенности таких сетей. Описана архитектура Junior U, как машстабируемого WEB-сервиса.

Литература

1. Python Porgramming Language [Электронный ресурс] / Python Software Foundation, 2009. – Режим доступа: http://python.org, свободный – Загл. с экрана. – Яз. англ.
2. Postgresql [Электронный ресурс] / Postgresql Global Development Group, 2009. – Режим доступа: http://postgresql.org, свободный – Загл. с экрана. – Яз. англ.
3. Memcached Distributed Cache [Электронный ресурс] / Livejournal LLC, 2009. – Режим доступа: http://danga.com/memcached, свободный – Загл. с экрана. – Яз. англ.
4. Nginx [Электронный ресурс] / И. Сысоев, 2009. – Режим доступа: http://sysoev.ru/nginx, свободный – Загл. с экрана. – Яз. англ.
5. CherryPy [Электронный ресурс] / Python Software Founation, 2009. – Режим доступа: http://cherrypy.org, свободный – Загл. с экрана. – Яз. англ.
6. Mako Templates for Python [Электронный ресурс] / M. Bayer, 2009. – Режим доступа: http://makotemplates.org, свободный – Загл. с экрана. – Яз. англ.
7. HighScalability [Электронный ресурс] / T. Hoff, 2009. – Режим доступа: http://highscalability.com, свободный – Загл. с экрана. – Яз. англ.

УДК 7967012.68

ПРОГРАММНОЕ СРЕДСТВО ДЛЯ ПОДДЕРЖКИ ГРАФИЧЕСКОГО ЯЗЫКА ОПИСАНИЯ ИГРОВЫХ ЭПИЗОДОВ В ФУТБОЛЕ

М.Н. Царев, Ф.Н. Царев, Ю.К. Чеботарева
Научный руководитель – д.т.н., профессор А.А. Шалыто

В статье развивается идея применения графического языка описания игровых эпизодов для описания поведения футболиста во время футбольного матча. Применение графического языка позволяет значительно повысить эффективность тактической подготовки игроков. Приведено описание программного средства, позволяющего применять графический язык на этапах изучения тактики и корректировки ошибок.

Ключевые слова: графический язык, игровой эпизод, футбол

Введение

При подготовке юных футболистов перед тренерами неизменно встает вопрос: как передать своим воспитанникам необходимые знания? Особенно трудно обучить игроков тактике футбола. Объяснить понятно и доходчиво, что и в какой ситуации надо делать, довольно сложно. В традиционных футбольных учебниках [1–5] для описания поведения игроков в различных ситуациях применяются рисунки (рис. 1). Часто они бывают, непонятны и могут по-разному трактоваться.

Рис. 1. Пример описания поведения игроков из [4]

Для решения указанной проблемы в работе [6] при участии авторов был предложен графический язык описания игровых эпизодов в футболе. Концепция подхода основана на теории систем [7] – футбольный матч можно разделить на множество взаимосвязанных между собой игровых эпизодов. В каждом игровом эпизоде могут быть определены роли игроков и их взаимные связи.

Таким образом, игру команды можно рассматривать, как «большой» алгоритм, состоящий из множества частных алгоритмов, увиденных и реализованных игроками команды. В идеальном случае все игроки команды должны видеть игровой эпизод одинаково и действовать в его рамках по одинаковому алгоритму, свойственному данному игровому эпизоду.

Для описания игровых эпизодов вводится 5 типов блоков:

1. Начало игрового эпизода;
2. Игровое действие;
3. Результат игрового действия;

4. Отрицательный исход игрового эпизода;
5. Положительный исход игрового эпизода.

Этими пятью элементами можно схематично описать любой игровой эпизод. Рисовать схемы, состоящие из этих блоков вручную или с использованием существующих программных средств достаточно утомительно. Поэтому для поддержки описанного подхода и облегчения его интеграции в образовательный процесс, авторами начата работа над программным средством, включающим в себя систему описательного моделирования игровых эпизодов и систему их визуализации.

Система описательного моделирования поведения игроков в игровых эпизодах

Система описательного моделирования поведения игрока в игровых эпизодах позволяет создавать, хранить и редактировать алгоритмы, описанные средствами графического языка описания игровых эпизодов в футболе. Общий вид системы описательного поведения игроков в игровых эпизодах представлен на рис. 2. На рис. 3 приведен фрагмент алгоритма поведения игрока в игровом эпизоде.

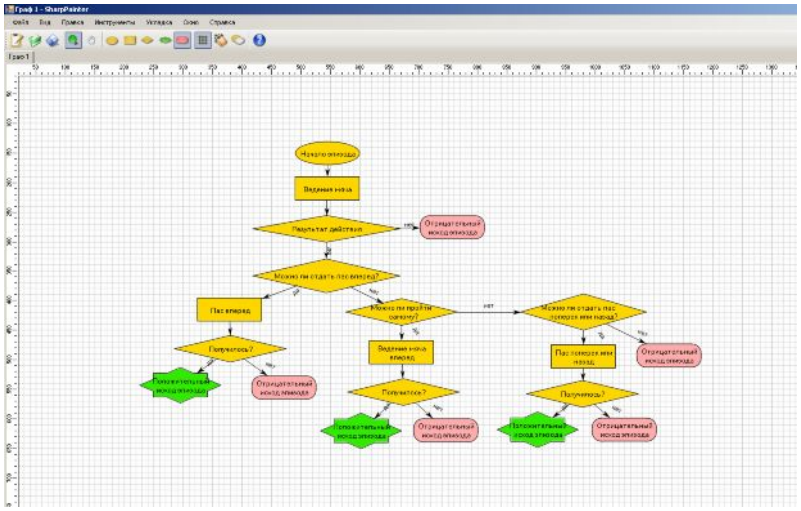


Рис. 2. Общий вид системы описательного моделирования поведения игроков в игровых эпизодах

Рис. 3. Фрагмент алгоритма поведения игрока

Система визуализации алгоритмов

Для визуализации игрового эпизода необходимо описать участок поля, на котором проходит игровой эпизод, участников игрового эпизода, алгоритмы действий игроков и начальные положениям игроков и мяча. Если заданы все эти параметры, то поведение

игроков может быть визуализировано. Игровой эпизод может развиваться по различным сценариям. На рис. 4 представлены три возможных сценария развития игрового эпизода «вбрасывание мяча в ситуации два нападающих против одного защитника».

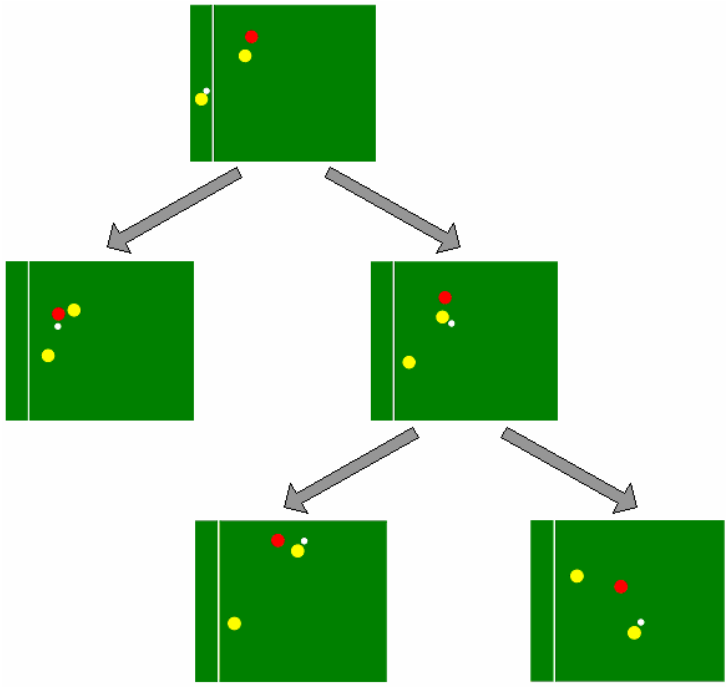


Рис. 4. Визуализация трех сценариев развития игрового эпизода «вбрасывание мяча из-за боковой линии в ситуации 2 нападающих против 1 защитника»

За счет возможности «проигрывания» различных сценариев, тренер сможет донести до игроков более полную информацию об игровом эпизоде.

Применение программного средства для поддержки графического языка описания игровых эпизодов в учебно-тренировочном процессе

Процесс изучения игровых эпизодов состоит из 5 этапов (рис. 5). На первых двух этапах тренер производит выбор игрового эпизода и разработку его описательной модели. Для разработки описательной модели тренер использует систему описательного моделирования поведения игроков в игровых эпизодах. Далее следует этап изучение модели игрового эпизода. В рамках этого этапа тренер при помощи программного комплекса для поддержки графического языка описания игровых эпизодов в футболе объясняет игрокам, что и как им необходимо делать. Главную роль тут играет система визуализации игровых эпизодов, которая позволит «проиграть» разные сценарии развития игрового эпизода и покажет игрокам какие действия и когда им необходимо выполнять. На двух последних этапах игроки применяют полученные знания и переводят их в навык. На этих двух этапах использование разрабатываемого программного средства целесообразно при корректировке ошибок.

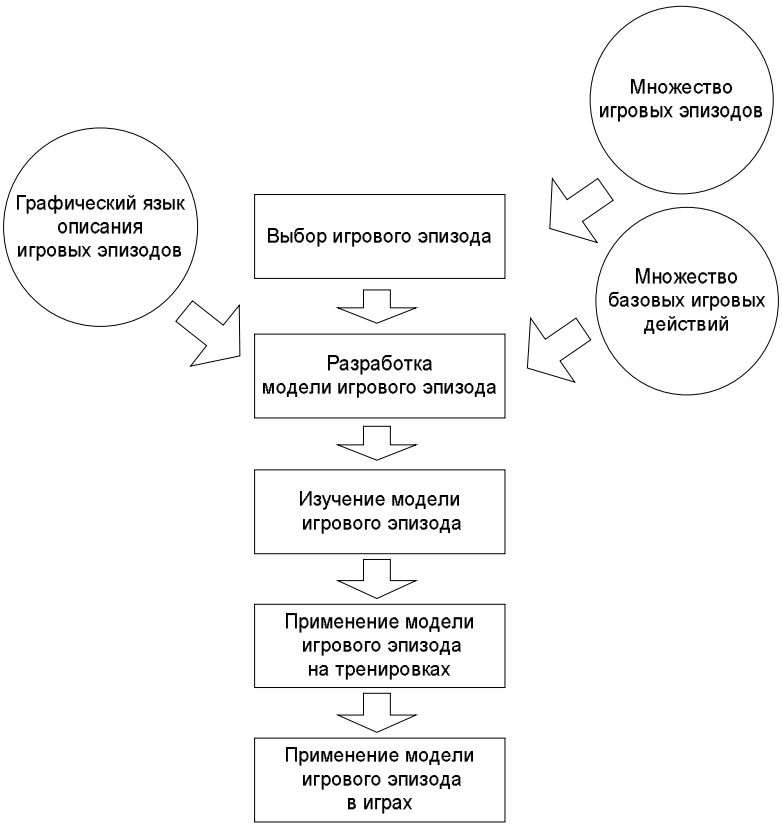


Рис. 5. Система изучения игровых эпизодов

Заключение

Из изложенного следует, что описанное программное средство позволит применять графический язык описания игровых эпизодов в учебно-тренировочном процессе на этапах изучения тактики и корректировки ошибок. Это программное средство позволит совместить точность схем алгоритмов с наглядностью их визуализации.

Литература

1. Козловский В.И. (ред.) Подготовка футболистов. М. Физкультура и Спорт, 1977.
2. Андреев С.Н. Играй в мини-футбол. – М.: Советский спорт, 1989. – 47 с.
3. Кук М. 101 упражнение для юных футболистов 7–11 лет/ Пер. с англ. Л. Захаровича. – М.: ООО издательство АСТ, ООО издательство Астрель, 2001. – 128 с.
4. Кук М. 101 упражнение для юных футболистов 12-16 лет./ Пер. с англ. Л. Захаровича. – М.: ООО издательство АСТ, ООО издательство Астрель, 2001. – 128 с.
5. Гил Харви и др. Футбол для начинающих: Практический курс./ Пер. с англ. В. Гаппарова – М.: ООО издательство АСТ, ООО издательство Астрель, 2001. – 128 с.
6. Царев М.Н., Царев Ф.Н., Румянцев Н.А. Графический язык описания игровых эпизодов в футболе /Тезисы научно-практической конференции «Спорт и занятость». СПбГУ ФК им. П.Ф. Лесгафта. 2008.
7. Ван Гиг Дж. Прикладная общая теория систем /Дж. ван Гиг. – М.: МИР, 1981. – 730 с.
8. Гойдановский В. 800 вопросов и ответов о правилах футбола. Издательство ЦК КП Грузии, Тбилиси, 1987.
9. Футбол (Правила соревнований). М.: Терра-Спорт, 2000. – 72 с.

УДК 004.588

МЕТОДИКА ПОДГОТОВКИ ЭТАЛОННЫХ НАБОРОВ ДАННЫХ ДЛЯ АВТОМАТИЗИРОВАННОЙ ПРОВЕРКИ ВИРТУАЛЬНЫХ ЛАБОРАТОРНЫХ РАБОТ

О.Е. Вашенков

Научный руководитель – к.т.н., доцент А.В. Лямин

В работе представлена структура системы AcademicNT, роль и функции виртуальных лабораторий и методы разработки эталонных наборов для качественной оценки результатов виртуального эксперимента. Исследование проводилось для виртуальной лаборатории по информатике, но такой подход может быть использован для любых виртуальных лабораторий.

Ключевые слова: виртуальная лаборатория, информационно-образовательная среда, электронное обучение

Введение

В рамках информационно-образовательной среды виртуальные лаборатории необходимы для формирования и проверки креативных навыков. В отличие от электронных тестов, задания виртуальных лабораторий имеют неразрешимое множество правильных ответов. Для таких заданий нельзя описать правильный ответ конечным множеством или формальным выражением, например, в виде регулярных выражений. Электронные задания, выполненные по технологии виртуальных лабораторий, используются в различных дисциплинах, позволяя проводить эксперименты и контролировать методику их выполнения [1, 2]. Ярким примером использования данной технологии стал многостилевой редактор кода, который предназначен для проверки навыков реализации алгоритмов с возможностью кодирования на наиболее распространенных языках программирования [2–4].

Следует различать виртуальные лаборатории от тренажеров и интерактивных демонстраций. Виртуальная лаборатория позволяет организовать автоматическую проверку. Тренажеры и демонстрации не предназначены для проверки заданий средствами информационно-образовательной среды.

Структура системы AcademicNT

Реализация виртуальной лаборатории предусматривает взаимодействие между различными модулями информационно-образовательной среды AcademicNT. При запросе задания клиенту передается интерактивный элемент лаборатории – аплет. После взаимодействия с аплетом пользователь отправляет ответ на сервер с помощью управляющих элементов HTML-страницы. При этом используется язык сценариев JavaScript для получения данных из аплета. Взаимодействие между клиентом и сервером организовано по протоколу HTTP, что накладывает ограничение на символы, используемые в ответе пользователя. Поэтому задача аплета – корректное экранирование ответа пользователя перед отправкой. Сервер перенаправляет HTTP-запрос веб-приложению, выполненному по технологии Java Servlets. Сервлет организует вызов хранимой процедуры на стороне системы управления базами данных (СУБД) и передает ей ответ пользователя. Процедура вызывает команду на стороне сервлета для отправки XML-сообщения на проверяющий сервер. Сообщение содержит ответ пользователя и эталонные данные. Вместе с командой на проверку сервлету передается ряд дополнительных переменных и список процедур, которые требуется вызвать после проверки. Проверяющий сервер осуществляет проверку для каждой пары эталонных наборов и возвращает результат сервлету в форме XML-сообщения. Взаимодействие между сервлетом и проверяющим сервером происходит по протоколу RLCP (Remote

Laboratory Control Protocol – протокол управления удаленной лабораторией) [4]. После получения ответа, сервлет разбирает XML-ответ и последовательно вызывает хранимые процедуры для занесения результатов проверки. Связи между модулями представлены на рис. 1.

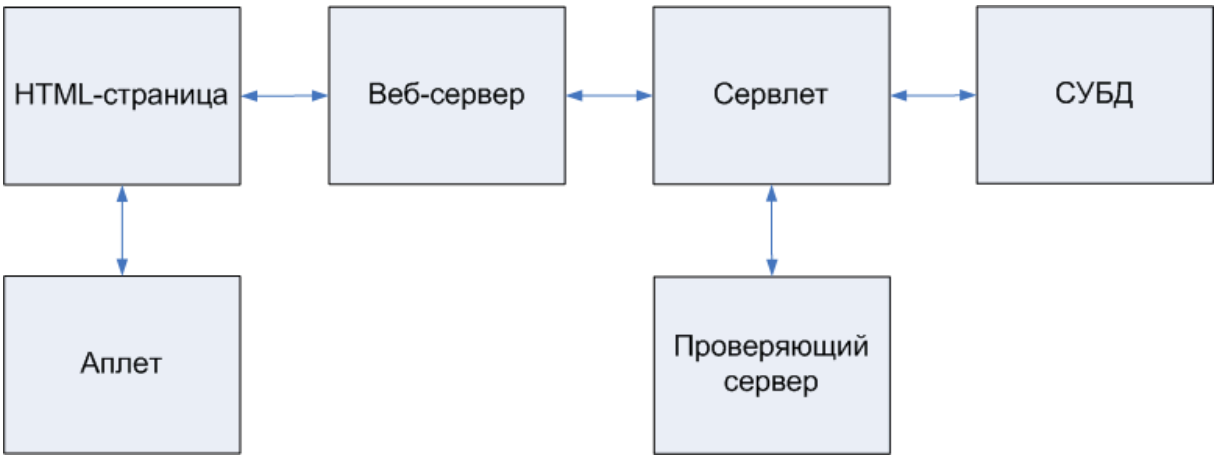


Рис. 1. Схема взаимодействия модулей информационно-образовательной среды

Технология виртуальных лабораторных работ

В общем случае, ответ на задание виртуальной лаборатории содержит описание некоторой системы с определенным набором входов и выходов. Эта система конструируется в соответствии с заданием на специализированном виртуальном стенде из объектов и отношений предметной области. Знание о правильном ответе может быть представлено в виде пар эталонных наборов входных и выходных данных. Для оценки правильности ответа необходимо получить реакцию описанной системы на заданном наборе входных данных и сравнить ее с соответствующим эталонным набором выходных данных. Совпадение реакции системы с эталонным набором выходных данных будет свидетельствовать о правильности ответа. Для получения реакции системы, описанной в ответе, на заданном наборе входных данных используется специализированная виртуальная машина.

Организация взаимодействия виртуального стенда и виртуальной машины, входящих в состав лаборатории, формирование заданий, эталонных наборов входных и выходных данных, протоколирование выполненных действий и полученных результатов – функции информационно-образовательной среды.

Основные требования для авторов виртуальных лабораторий:

- подготовка интерактивного элемента – аплета;
- разработка алгоритмов проверки и реализация проверяющего сервера;
- подготовка эталонных входных и выходных данных;
- описание сценария, заданий и установки в формате XML.

При разработке интерактивного элемента требуется соблюдение лишь одного ограничения – реализация метода для получения ответа испытуемого в текстовом виде.

При разработке модуля проверки, автор может взять за основу каркас для разработки проверяющих серверов виртуальных лабораторий. Его использование позволяет абстрагироваться от низкоуровневой сетевой передачи и протокола RLCP, фокусируя внимание только на алгоритмах проверки.

С помощью эталонных наборов, автор описывает соответствие между заданными входными и выходными данными. Задача проверяющего сервера – установить перед выполнением работы эталонные входные данные, а после выполнения сверить эталонные выходные данные с данными, полученными в ходе автоматического

эксперимента. Эталонные наборы должны быть описаны для каждого задания отдельной виртуальной лабораторной работы. Автор может разработать один и более наборов. Итоговая оценка за задание устанавливается системой, как процент успешно пройденных наборов.

Единственное требование при оформлении эталонных наборов – оформление набора, как строки символов. Например, если требуется перечислить последовательность целых чисел, набор может выглядеть следующим образом: «0 1 12 15 3 4 5 8». Программный модуль проверяющего сервера получает эту строку, а её интерпретация – задача автора лаборатории.

Например, в виртуальной лаборатории «Многостилевой редактор кода» допустимыми являются следующие эталонные наборы:

- целочисленный массив: a=[0, 1, 2, 3, 4, 5];
- строковая переменная: b="answer";
- вещественная переменная с допустимой ошибкой – 10%: c{10%}="1.2E+3".

Проверяющий сервер производит разбор таких наборов и сверяет значения переменных со значениями, полученными в результате выполнения программы испытуемого.

Методика разработки оптимальных наборов

В качестве примера будет рассмотрена виртуальная лаборатория по информатике, которая используется для проверки навыка испытуемых в разработке алгоритмов решения стандартных задач. Сложности в составлении эталонных наборов заключаются в выборе данных. Например, при наличии одного эталонного набора, оценка работы сводится к двоичному «правильно»/«неправильно», при необходимости более детальной дифференциации оценки, требуется провести анализ влияния входных данных на выполнение программы, разработанной испытуемым.

Рассмотрим, для примера, типовые задачи по информатике: поиск минимума в массиве и сортировка массива. Первая задача звучит следующим образом: найти индекс последнего минимального элемента в целочисленном массиве из десяти элементов.

На рис. 2 представлен интерфейс виртуальной лаборатории по информатике с решением задачи и использованием стиля кодирования аналогичного языку "C".

В приведенных ниже примерах переменная **a** принадлежит набору входных данных, а **b** – эталонным выходным данным. В самом простом случае, проверка может быть организована на основе одного набора:

a=[10, 10, 10, 10, 10, 1, 10, 10, 10, 10] b=5

В таком случае не учитывается вариант, когда программа некорректно обрабатывает граничные случаи. Такие случаи могут быть связаны с ошибками в операторах управления (условия, циклы). В данной программе таких оператора два.

В инварианте цикла может быть допущена ошибка в условии или при инициализации переменной цикла. В таком случае может возникнуть исключение времени выполнения (выход за границы массива) или пропуск крайних элементов. Исключение времени выполнения в данной работе может быть обнаружено при локальной отладке программы в среде редактора кода. Пропуск крайних элементов найти сложнее, и программа, в таком случае, может считаться "частично" рабочей. Для проверки можно добавить два дополнительных набора:

a=[0, 1, 2, 3, 4, 5, 6, 7, 8, 9] b=0

a=[1, 2, 3, 4, 5, 6, 7, 8, 9, 0] b=9.

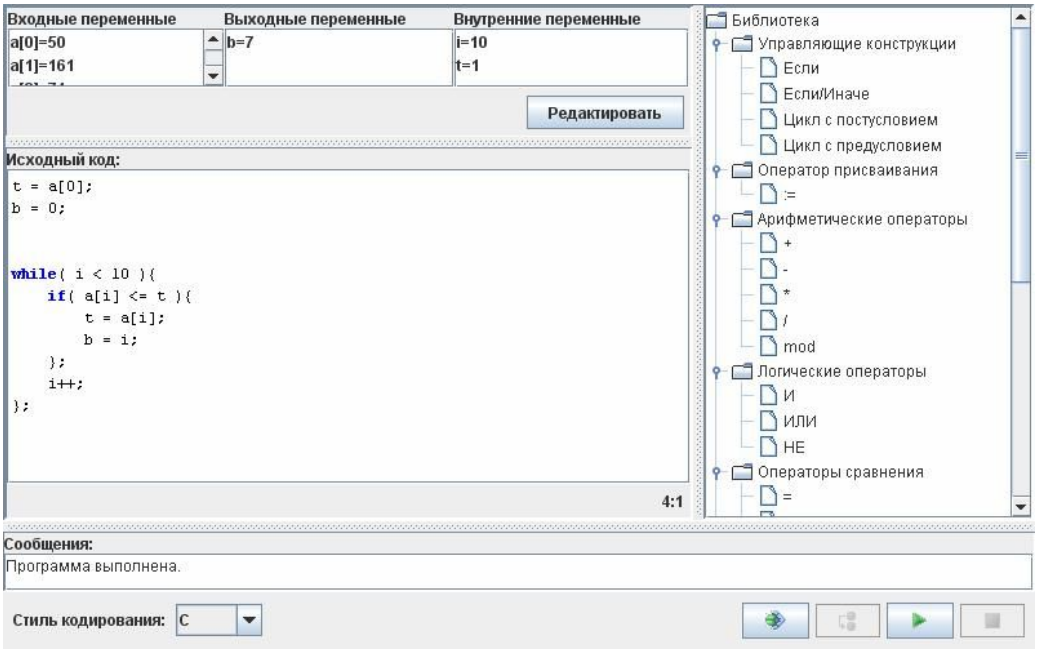


Рис. 2. Решение задачи о поиске минимума в массиве

По заданию, требовалось найти последний минимальный элемент. Ошибка в операторе условия может привести к нахождению первого из минимальных элементов. Для проверки этого условия требуется добавить следующий набор:

a=[0, 1, 2, 3, 4, 5, 6, 7, 8, 0] b=9.

Таким образом, вместо двоичной оценки было получено четыре критерия для проверки.

Вторая задача звучит следующим образом: отсортировать целочисленный массив из десяти элементов по возрастанию. Решение задачи с использованием стиля языка "C" можно записать следующим образом:

```
i = 0; j = 0;
while( i < 10 ){
 j = j + 1;
 while( j < 10 ){
      if( b[j] < b[i] ){
           t = b[j];
           b[j] = b[i];
           b[i] = t;
      }
      j++;
 }
 i++;
}
```

Наиболее простой случай проверки можно описать одним набором:

a=[0, 1, 2, 4, 3, 5, 6, 7, 8, 9] b=[0, 1, 2, 3, 4, 5, 6, 7, 8, 9].

Данная программа содержит три оператора управления, следовательно, дополнительные эталонные наборы позволят обнаружить ошибки, связанные с этими операторами. Первый оператор – цикл с предусловием. Ошибка в инициализации переменной цикла или в операторе условия может привести к пропуску граничных элементов массива. Второй оператор также представляет собой цикл с предусловием, и инвариант цикла может сказаться на пропуске граничных элементов. Ошибка в записи третьего оператора условия может привести к обратному порядку сортировки или к лишним операциям обмена. Последнее сложно проверить, т.к. для таких простых программ разница во времени будет не значительной.

Для проверки инварианта первого цикла можно использовать следующий набор:

a=[1, 0, 2, 3, 4, 5, 6, 7, 8, 9] b=[0, 1, 2, 3, 4, 5, 6, 7, 8, 9].

Инвариант второго цикла влияет на обработку граничных элементов справа. Для проверки требуется следующий набор:

a=[0, 1, 2, 3, 9, 4, 5, 6, 7, 8] b=[0, 1, 2, 3, 4, 5, 6, 7, 8, 9].

Если автор лаборатории примет решение, что сортировка в порядке, обратном заданию также является верным решением, можно добавить набор для проверки оператора условия:

a=[0, 1, 2, 3, 4, 5, 6, 7, 8, 9] b=[9, 8, 7, 6, 5, 4, 3, 2, 1, 0].

Таким образом, для дифференцирования оценки, можно использовать четыре эталонных набора вместо одного для выявления некритических ошибок в алгоритмах.

Заключение

Одним из основных достоинств среды AcademicNT является наличие встроенного механизма для построения виртуальных лабораторий, которые необходимы для формирования и проверки навыков. В данной статье приведены схема взаимодействия модулей информационно-образовательной среды, принципы функционирования виртуальных лабораторий, требования к оформлению эталонных наборов данных и методика разработки эталонных наборов для наиболее точного оценивания результатов виртуальных экспериментов. Основные результаты статьи проиллюстрированы на примере виртуальной лаборатории «Многостилевой редактор кода», которая предназначена для проверки навыков реализации алгоритмов с возможностью кодирования на наиболее распространенных языках программирования.

Представленные в статье результаты прошли апробацию и продемонстрировали свою эффективность в ходе реализации следующих проектов:

- система дистанционного обучения СПбГУ ИТМО (http://de.ifmo.ru);
- система для проведения Интернет-олимпиад и экзаменов (http://de.ifmo.ru/exam).

Рассмотренный подход к разработке проверяющих наборов и виртуальная лаборатория используются в электронном курсе «Информатика». Использование дополнительных эталонных наборов позволило более точно оценить навыки студентов.

Литература

1. Вашенков О.Е., Лямин А.В., Тарлыков В.А. Оценивание результатов обучения в среде электронного учебно-методического комплекса по дисциплине «Когерентная оптика» // Конференция «Оптика и образование-2006» / СПбГУ ИТМО. – СПб. – 2006. – С. 70–71.
2. Васильев В.Н., Лисицына Л.С., Лямин А.В. Технология проведения ЕГЭ по инфоратике в компьютерной форме // Научно-технический вестник СПбГУ ИТМО. – 2007. – Выпуск 45. – С. 126–143.
3. Васильев В.Н., Лисицына Л.С., Лямин А.В. Сетевая технология проведения вступительных испытаний по информатике в режиме on-line // Сборник научных трудов «Использование информационно-коммуникационных технологий в процессе оценки качества образования». – СПб. – 2008. – С. 55–70.
4. Вашенков О.Е., Лямин А.В. Технология разработки виртуальных лабораторий в информационно-образовательной среде AcademicNT на примере работы по информатике // Материалы межвузовской научно-методической конференции «Проблемы разработки учебно-методического обеспечения перехода на двухуровневую систему в инженерном образовании» / МИСиС. – М. – 2008. – С. 239–249.

УДК 53.05

РАЗРАБОТКА КОМПЬЮТЕРНОГО ЛАБОРАТОРНОГО КОМПЛЕКСА ДЛЯ КОЛИЧЕСТВЕННОГО ИЗУЧЕНИЯ ФИЗИЧЕСКИХ ЯВЛЕНИЙ

К.В. Панков
(Российский государственный педагогический университет им. А.И. Герцена)
Научный руководитель – д.ф.-м.н., профессор В.М. Грабов
(Российский государственный педагогический университет им. А.И. Герцена)

В данной работе рассматриваются возможности разработанного компьютерного лабораторного комплекса, основанного на фотографическом методе исследования физических явлений и призванного показать рациональное использование ИКТ в рамках курса преподавания физики, как в школе, так и в ВУЗе при организации демонстраций, лабораторных и исследовательских работ.
Ключевые слова: физика, демонстрация, эксперимент, ИКТ

Введение. Постановка цели

В настоящее время информационные технологии применяются повсеместно, не стало исключением и преподавание физики. Однако, вопрос рационального использования ИКТ, а в частности ЦОР, в рамках данной дисциплины является актуальным и на данный момент. Прежде всего, это связано с чрезмерным использованием виртуальных лабораторий, что может свести такое понятие как физический эксперимент к изучению компьютерной модели и привести к ликвидации экспериментального метода познания физических явлений и процессов. Основными недостатками данных лабораторий является то, что все эксперименты идеальны; учителя и преподаватели лишены возможности давать задания по экспериментальной обработке данных; учащиеся школ и студенты ограничены на этапе построения хода эксперимента; лишены возможности самостоятельно работать с физическими приборами, полученными данными и самое главное на их основе строить, опровергать или подтверждать теорию. Все эти факторы могут привести к снижению общих знаний по курсу физики и вместе с тем уменьшить интерес к самому предмету. В связи с этим целью работы стала разработка такого цифрового образовательного ресурса, с помощью которого стало бы возможным решение изложенных проблем, интеграция физико-математических дисциплин, а также осуществление исследовательской деятельности учащихся и студентов не только в рамках учебного заведения, но и в домашних условиях.

Главная идея. Принцип работы

На начальном этапе работы был создан комплекс программного обеспечения, предназначенный для количественного изучения физических явлений. Построен комплекс был по принципу, что компьютер в совокупности с подключенными периферийными устройствами, такими как веб-камера и микрофон, прежде всего, должен использоваться в качестве регистрирующей части лабораторной установки, а в дальнейшем как инструмент обработки полученных данных. Помимо этого используемые аппаратные средства должны быть широко распространены не только в пределах образовательных учреждений, но и быть доступны в домашних условиях, что позволяет организовать исследовательскую деятельность на дому [1].

Именно поэтому основу комплекса составил фотографический метод исследования физических явлений, заключающийся в запечатлении изучаемых процессов с помощью веб-камеры и последующем анализе полученных снимков с помощью компьютера, посредством сравнения с фоновым кадром, в результате чего исследователь полу-

чает таблицу значений координат тела и значения, соответствующих им, моментов времени, по которым можно напрямую или косвенно изучать сами явления. Пример изучения затухающих колебаний представлен на рис. 1.

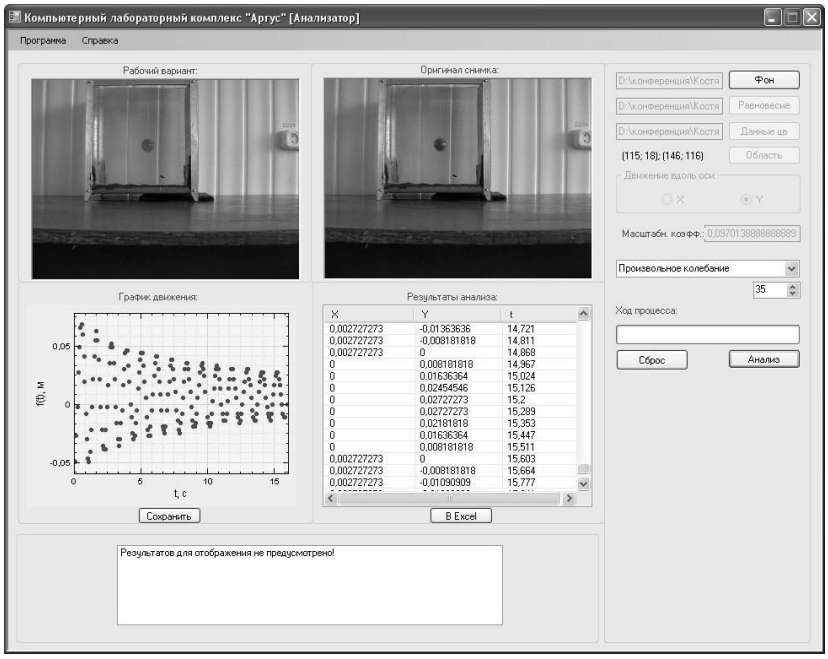


Рис. 1. Результат изучения колебаний пружинного маятника

В ходе проведения процедуры анализа снимков программа демонстрирует весь снятый материал и сразу же воспроизводит на графике точки, характеризующие положение тела в текущий момент времени записи, что, безусловно, является весьма наглядным. В дальнейшем таблицу данных для проведения обработки можно экспортировать в табличные процессоры, такие как MS Excel и OpenOffice Calc, а затем по мере необходимости в специальные математические пакеты, такие как MathCAD. Примером простейшей процедуры обработки данных полученных в результате изучения затухающих колебаний пружинного маятника, представленных на рис. 1, служит рис. 2.

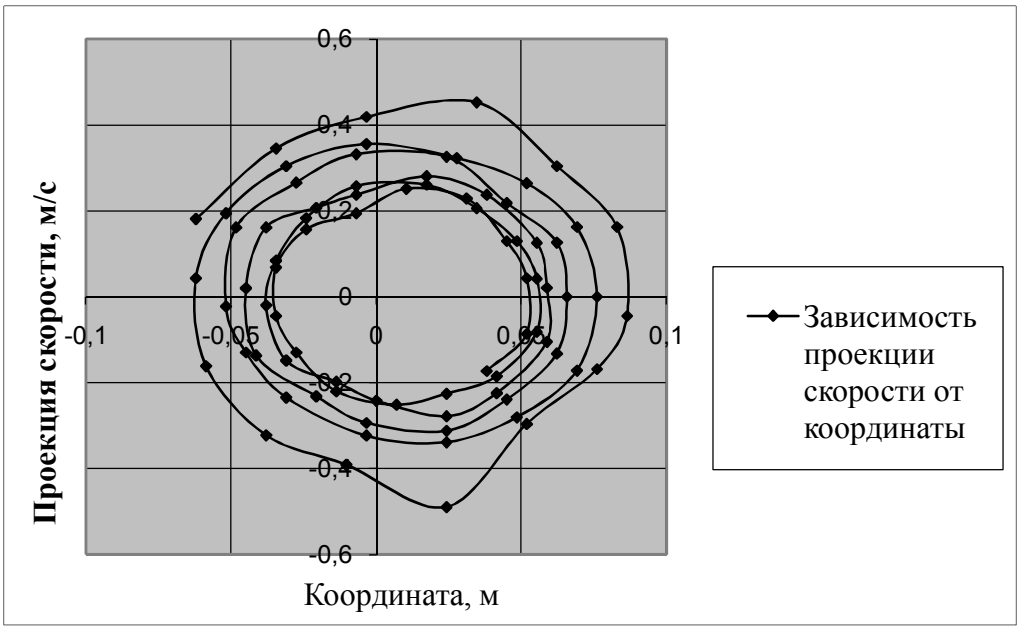


Рис. 2. Фазовая траектория затухающих колебаний пружинного маятника

Некоторые возможности комплекса

Указанная выше возможность позволяет преподавателю давать задания по обработке экспериментальных данных, а использование специальных программных средств позволяет связать физико-математические дисциплины, что безусловно сказывается на качестве подготовки студентов и выпускников школ. Помимо этого можно использовать комплекс для организации исследовательской деятельности в рамках лабораторных или факультативных занятий. Этому способствует хорошая точность данных, обеспечиваемая программным обеспечением и аппаратными средствами персонального компьютера, что, конечно же, важно для подтверждения и построения теории. Результаты всех экспериментов: таблицы данных, графики, стробоскопические фотографии, снимки экспериментов, – можно сохранять, чтобы в дальнейшем использовать для составления отчетов о проделанной работе и формирования экспериментальной базы, которая может послужить для доказательства выдвинутой в ходе исследования гипотезы.

Еще одной возможностью предоставляемой комплексом является использование его для демонстрации. К сожалению на занятиях для демонстраций отводится не так много времени поэтому необходимо не только наглядно показать явление, получить значение необходимых физических величин, представить графики, но и проделать все это за минимальное количество времени. В то же время ручная обработка данных может стать весьма продолжительным процессом, поэтому была предусмотрена возможность использовать готовые модули, которые предназначены для обработки данных по некоторым шаблонам, что сводит трудоемкий процесс к выбору метода обработки данных, характерного для изучаемого явления, с помощью средств лабораторного комплекса. Модульная основа также позволяет преподавателям и учителям, знакомым с программированием самостоятельно дополнять комплекс и таким образом становиться в свою очередь соавторами.

На последнем этапе разработки в компьютерный лабораторный комплекс была добавлена компонента для изучения звуковых колебаний, пример представлен на рис. 3.

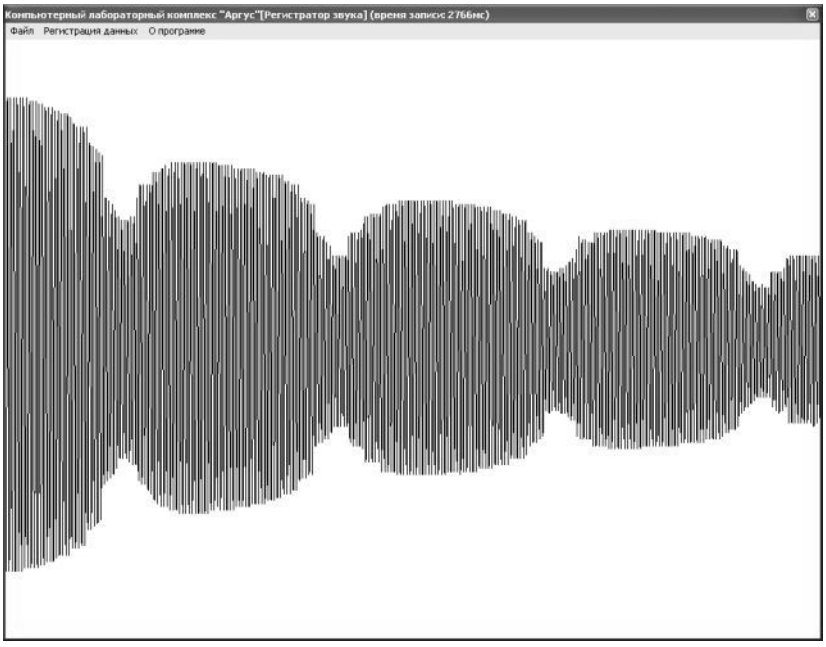


Рис. 3. Результат изучения биений

Также была добавлена возможность использовать комплекс под управлением не только операционной системы Windows, но и под ОС на базе ядра Linux, что делает проект вполне перспективным в случае перехода образовательных учреждений на сво-

бодное программное обеспечение. На стадии разработки находится программное обеспечение для совместного использования с анимационными и другими компьютерными моделями.

Заключение

На сегодняшний день компьютерный комплекс «Аргус» проходит апробацию на базе школы № 286 г. Санкт-Петербурга. В рамках факультативных занятий учащиеся проводят исследования движений тел переменной массы, падений тел в жидкости, равнопеременного движения, распространения волн, а также проводят опыты по определению скорости звука, коэффициента вязкого трения и т.д.. Работы носят исследовательский характер и призваны повысить интерес учащихся к предмету, улучшить информационную компетентность, и наконец, повысить качество знаний по предметам. Такая деятельность может быть направлена на закрепление пройденного материала, его повторение, а также присутствует возможность с помощью организации такого вида работы вводить новые понятия в рамках изучаемого курса.

Разработанный компьютерный лабораторный комплекс в ходе апробации, а также анализа предоставляемых возможностей продемонстрировал, что является не только удобным средством изучения физических явлений, но и мощным дидактическим средством, которое в руках учителя и преподавателя может стать хорошим инструментом для организации экспериментального познания и интегрирования таких дисциплин как физика, математика и информатика.

Литература

1. Панков К.В., Никитин В.В. Использование цифровых мультимедийных технологий для количественного изучения кинематических закономерностей: Сборник тезисов, материалы Четырнадцатой Всероссийской научной конференции студентов-физиков и молодых ученых (ВНКСФ-14 г. Уфа): материалы конференции, тезисы докладов. – Екатеринбург – Уфа: издательство АСФ России, 2008. – 656 с.

УДК 371.398

ОСОБЕННОСТИ АРХИТЕКТУРЫ ОБУЧАЮЩИХ СИСТЕМ ДЛЯ УЧЕНИКОВ МЛАДШИХ КЛАССОВ

А.А. Ахмадеева
Научный руководитель – к.т.н., доцент Н.Н. Горлушкина

Особенности архитектуры обучающих систем для учеников младших классов в соответствии с требованиями современного санитарного законодательства. Структура компьютерной обучающей системы с учетом характерных особенностей обучения учеников младших классов.
Ключевые слова: обучающая система, ученики, младшие классы

Введение

С каждым днем компьютеры все больше используются в различных сферах деятельности человека, образование не стало исключением. Создаются многочисленные обучающие компьютерные программы и приложения, предназначенные для обучения как взрослых, так и детей. Все больше создается обучающих программ для домашнего использования и интернет-ресурсов для самообучения или для обучения без прямого контакта с преподавателем.

Компьютерная обучающая система должна включать три основных блока:

- информационно-справочный блок;
- блок управления процессом обучения;
- блок контроля.

Все блоки должны учитывать характерные особенности учеников младших классов, то есть должно учитываться допустимое время пребывания ребенка за компьютером, индивидуальные особенности каждого ученика, также обучающая информация должна привлекать внимание детей и должна быть изложена в простой, понятной для ученика форме.

Большинство интернет-ресурсов, например, http://www.wunderkinder.narod.ru, http://children.kulichki.net, http://detskiy.nm.ru, http://novakovskiy.narod.ru/kids/kid.html, http://vip.km.ru/vschool, http://www.solnet.ee, ориентированных на младших школьников включают в себя информационно-справочный блок, некоторые из них также содержат блок самоконтроля, но отсутствует блок управления процессом обучения, который следил бы за последовательностью прохождения заданий и за временем занятия. Последнее условие очень важно, так как время пребывания за компьютером ограничено требованиями современного санитарного законодательства, следовательно, компьютерная обучающая система, а также ее содержание должны быть построены с учетом этих требований.

Информационно-справочный блок

Информационно-справочный блок можно представить в виде обучающей подсистемы, которая состоит из программ формирующих знания, умения и навыки. При заполнении информационно-справочного блока для учеников младших классов необходимо учитывать их особенности, связанные с потерей внимания к предмету, и формировать информацию таким образом, чтобы она давалась небольшими порциями.

Программы **формирующие знания** делятся на информационно-справочные и поисковые. Информационно-справочная система представляет собой программную оболочку, хранящую организованный набор теоретических сведений, терминов, развернутых пояснений к ним, обеспечивающая возможность поиска и выборки необходимой тематической информации и реализации запросов. Поисковой системой называется

программная оболочка, обеспечивающая возможность поиска необходимой информации в процессе обучения. Теоретические сведения информационно-справочной системы для учеников младших классов должны быть представлены в красочной форме в виде картинок и описаны простыми, короткими предложениями, понятными для данной аудитории, некоторая информация должна иметь звуковое сопровождение для повышения восприятия информации. Переход по информационно справочной системе должен осуществляться либо родителями, либо блоком управления процессом обучения.

Программы, **формирующие умения и навыки,** для учеников младших классов представляют собой генераторы заданий определенного типа по заданной теме, которые представлены в форме компьютерной игры. Они позволяют провести контрольную или самостоятельную работу, обеспечив каждому учащемуся отдельное задание, соответствующее его индивидуальным возможностям. Для учеников младших классов данные программы целесообразно представлять в **тренировочном типе**, когда за один из ведущих принципов берется подкрепление правильного ответа. Принцип заключается в том, что когда ученик отвечает на вопрос правильно, ему сообщается об этом, для учеников младших классов данное сообщение может быть представлено в виде красивой картинки и положительного звукового сигнала. Если ответ не правильный, ученику сообщается о том, что он ответил не правильно, в зависимости от формы задания сообщается, к какой категории относится выбранный ответ, и уточняется вопрос.

Блок управления процессом обучения

В блок управления процессом обучения входит тренирующая подсистема и подсистема, управляющая процессом чередования режимов обучения и перерывов.

Программы тренировочного типа предназначены преимущественно для закрепления умений и навыков. Предполагается, что теоретический материал уже усвоен. Тренирующая программа случайным образом генерирует задания по пройденным темам. Когда ученик отвечает на задание правильно, ему сообщается об этом, и в систему поступает сообщение, что тема пройдена успешно. Когда ученик отвечает не правильно, то ему даются ещё попытки до тех пор, пока он не найдет правильный ответ, при этом в базу данных поступает информация о количестве попыток, на основании которой, принимается решение о повторении проблемной темы. В следующий раз информационно-справочный блок начнется с повторения плохо изученной темы.

Создание подсистемы, управляющей процессом чередования режимов обучения и перерывов, может стать решением основной проблемы, связанной с определением промежутка времени, нахождения ребенка за компьютером.

Известно [1], что рекомендуемая непрерывная длительность работы, связанной с фиксацией взора непосредственно на экране монитора, на уроке не должна превышать:

- для обучающихся в I–IV классах – 10–15 минут;
- для обучающихся в V–VII классах – 15–20 минут;
- для обучающихся в VIII–IX классах – 20–25 минут;
- для обучающихся в X–XI классах на первом часу учебных занятий – 30 минут, на втором – 20 минут.

Оптимальное количество занятий с использованием компьютера в течение учебного дня для обучающихся I–IV классов составляет 1 урок, для обучающихся в V–VIII классах – 2 урока, для обучающихся в IX–XI классах – 3 урока.

В дошкольных образовательных учреждениях (ДОУ) рекомендуемая непрерывная продолжительность работы с компьютерами на развивающих игровых занятиях для детей 5 лет не должна превышать 10 минут, для детей 6 лет –15 минут.

Игровые занятия с использованием компьютеров в ДОУ рекомендуется проводить не более одного в течение дня и не чаще трех раз в неделю в дни наиболее высокой работоспособности детей: во вторник, в среду и в четверг. После занятия с детьми проводят гимнастику для глаз [1].

Основываясь на [1], в управляющей подсистеме через определенные промежутки времени, отведенные на обучение, проводятся перерывы. Во время перерывов компьютер, выступая в роли ведущего, озвучивает упражнения для глаз или физические упражнения. Экран во время перерыва становится темным, что позволяет гарантировать то, что ребенок отвернется от экрана.

Блок контроля

Контролирующий блок может состоять из программ с контролем в экспертной системе, тестирующих программ и программ, организующих самоконтроль. Контролирующие программы специально рассчитаны на проведение текущего или итогового опроса учащихся. Они позволяют установить необходимую обратную связь в процессе обучения, способствуют накоплению оценок, дают возможность проследить успеваемость каждого учащегося, соотнести результаты обучения с трудностью предлагаемых заданий, индивидуальными особенностями обучаемых, предложенным темпом обучения, объемом материала, его характером. В условиях компьютерного обучения, за счет систематической и продуктивной обратной связи, появляется возможность построения индивидуальной программы обучения для отдельного ученика, которую легко корректировать.

Исследованию проблемы обратной связи посвящена работа [2]. Опираясь на [2], в обучающей системе для учеников младших классов обратная связь осуществляется с помощью тренирующих и контролирующих тестов в игровой форме, а также с помощью веб-камеры.

Для тех, у кого есть веб-камера, существует возможность «контролировать» поведение ребенка во время перерыва. Пока ребенок не встанет из-за компьютера занятие в перерыве не начнется. Также не начнется занятие после перерыва, если ребенок сел за компьютер раньше положенного срока или ещё не успел подойти к компьютеру после перерыва, что позволит гарантировать, что обучение не начнется без учащегося.

Во время обучения некоторые тестовые занятия могут проводиться с помощью веб-камеры. Например, ребенку сначала показали цвета и как они называются, затем предлагают походить по комнатам и принести предмет указанного цвета. Ребенок показывает этот предмет камере, она устанавливает правильного цвета предмет или нет. Ещё один пример, урок был посвящен геометрическим фигурам, ребенку предлагается пойти, поискать предметы, которые похожи на определенную фигуру, или нарисовать на листке бумаги и показать камере.

Заключение

Компьютерные обучающие системы для учеников младших классов должны быть построены таким образом, чтобы информационно-справочный, тренирующий и контролирующий блоки были представлены в интересной для детей, непринужденной игровой форме.

Обратная связь и блок управления обучением должны быть построены таким образом, чтобы процесс обучения корректировался для каждого ученика индивидуально, в зависимости от его успеваемости, индивидуальных особенностей, реакций на трудность предложенных задач, темп обучения, объем и характер материала.

В блоке управления обучением обязательно должно учитываться время непрерывного нахождения обучающегося за компьютером, должны проводиться перерывы в обучении, а также количество обучающих сеансов в день должно быть ограничено в соответствии с [1].

Литература

1. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы: Санитарно-эпидемиологические правила и нормативы СанПиН 2.2.2 / 2.4.1340-03 // Безопасн. жизнедеятельности. – 2005.
2. Лукьяненко О.Д. Технологическое обеспечение обратной связи в дидактическом информационном взаимодействии педагога с детьми 6–7 лет: Диссертация... кандидата педагогических наук. – Армавир. – 2007. – 199 с.
3. Горлушкина Н.Н. Педагогические программные средства. Учебное пособие. Под ред. М.И. Потеева. – СПб: СПб ГУ ИТМО, 2003. – 136 с.

УДК 378.147 + 681.327

ПОВЫШЕНИЕ УРОВНЯ ТВОРЧЕСКОГО МЫШЛЕНИЯ И ПРОФЕССИОНАЛЬНОЙ САМОСТОЯТЕЛЬНОСТИ СТУДЕНТОВ В ОБЛАСТИ МУЛЬТИМЕДИА

С.В. Ильичева
Научный руководитель – к.т.н., доцент Н.Н. Горлушкина

В статье рассматриваются педагогические и психологические особенности повышения уровня творческого мышления и профессиональной самостоятельности студентов в области мультимедиа. Приводятся рекомендации развития творческого потенциала студентов. Затрагивается ассоциативная гипотеза творчества и ее применение. Изложены дидактические рекомендации при использовании компьютерных и мультимедийных технологий для мотивации к самостоятельной познавательной деятельности студентов.

Ключевые слова: интеллект, мотивация, мультимедиа, мышление, профессиональная компетентность, творчество

Введение

Одной из важнейших особенностей современного этапа развития общества является тесная взаимосвязь социально-экономического прогресса и постоянного совершенствования системы образования. Актуальной становится задача создания новой концепции педагогического образования, обеспечивающей гармоничное развитие личности, ее потребностей, способностей, сознания, активной жизненной и профессиональной позиции; стремление к саморазвитию, самоопределению и самосовершенствованию.

В области мультимедиа наблюдается быстрый прогресс методологии, программных и технических средств. По отношению к проблеме изучения учебной дисциплины есть два подхода:

(1) Подход с ориентацией на подготовку пользователя, т.е. человека, пользующегося готовыми программными продуктами и готовыми технологиями.

(2) Подход с ориентацией на подготовку разработчика новых систем и технологий.

Основная часть

Процесс обучения студентов (формирование субъекта деятельности) включает в себя возможность для формирования познавательной и творческой способностей студентов, в ходе обучения должны моделироваться ситуации, требующие от студентов как субъективно, так и объективно новых решений.

При таком подходе студент восходит по иерархической лестнице образования: элементарная и функциональная грамотность, образованность, профессиональная компетентность, культура, менталитет [1].

Основные профессиональные нравственные ценности современного специалиста:

(1) ориентация на нетрадиционные решения;
(2) готовность к преодолению трудностей;
(3) осознание личной ответственности за положение дел;
(4) профессиональное достоинство;
(5) реальное оценивание своей квалификации;
(6) осознание потребности в непрерывном повышении своей компетентности;
(7) готовность принимать рациональные решения в ответственных ситуациях;
(8) гуманистическое осмысление технических проблем.

Креативность не есть некоторая особая характеристика познавательных процессов, а представляет собой одну из самых глубоких характеристик личности. Личность же нельзя «сформировать», а можно только воспитать. Воспитание, в свою очередь, не может быть не чем иным, как созданием условий для самовоспитания личности. Творчество есть прерогатива свободной, способной к саморазвитию личности [2].

Стернберг и Любарт (Sternberg & Lubart, 1996) разработали теорию творчества, основанную на многомерном подходе к данной теме. Эта теория построена вокруг шести признаков. Эти шесть аспектов творческого потенциала таковы [3]:

(1) Интеллектуальные процессы.
(2) Интеллектуальный стиль.
(3) Знания.
(4) Личность.
(5) Мотивация.
(6) Экологический контекст.

Действительно творческая деятельность – явление редкое не потому, что люди испытывают недостаток в каком-либо из этих аспектов, а поскольку трудно добиться того, чтобы все шесть аспектов работали вместе. Ясно, что креативность – это не отдельная черта личности, навык или способность, а комбинация нескольких факторов, которые могут быть идентифицированы и проанализированы. Кроме того, оценка творческого потенциала человека не сводится к простой идентификации выраженности каждого признака и сложению полученных показателей для получения некоего индекса креативности. Скорее, это вопрос идентификации и оценки силы взаимодействий между признаками [3].

Творчество – неформализованный процесс создания или выявления субъектом новых сведений или объектов духовной либо материальной культуры, основанный на мышлении, выходящем за пределы известного, на реализации собственного видения объекта, задачи или проблемы и сознательном отказе от сложившихся представлений или известных способов [4].

Много лет назад в истории когнитивной психологии Уоллес (Wallas, 1926) описал четыре последовательных этапа творческого процесса [3]:

(1) Подготовка. Формулировка задачи и начальные попытки ее решения.
(2) Инкубация. Отвлечение от задачи и переключение на другой предмет.
(3) Инсайт (просветление). Интуитивное проникновение в суть задачи.
(4) Проверка. Испытание и/или реализация решения.

В высшем образовании важно обеспечивать ответственное отношение выпускника как к разработке творческих (научных или конструкторских) проблем, так и к решению повседневных организационных и технических вопросов. Без понимания этих особенностей инженерного труда выпускник, который в вузе был нацелен только на развитие науки как наиболее престижной деятельности, будет чувствовать себя несчастным, работая после окончания вуза на производстве или в эксплуатации технических средств, где есть свои направления творчества.

Но если прямое обучение творчеству невозможно, то вполне реально косвенное влияние на него за счет создания условий, стимулирующих или тормозящих творческую деятельность.

Условия или факторы, влияющие на течение творческой деятельности, бывают двух видов: ситуативные и личностные [2].

К ситуативным факторам, отрицательно влияющим на творческие возможности человека, относятся лимит времени; состояние стресса; состояние повышенной тревожности; желание быстро найти решение; слишком сильная или слишком слабая мотивация; наличие фиксированной установки на конкретный способ решения;

неуверенность в своих силах, вызванная предыдущими неудачами; страх; повышенная самоцензура; способ предъявления условий задачи, провоцирующий неверный путь решения, и др. К личностным факторам, негативно влияющим на процесс творчества, относят конформизм (соглашательство); неуверенность в себе (часто сопутствует общей низкой самооценке), а также слишком сильную уверенность (самоуверенность); эмоциональную подавленность и устойчивое доминирование отрицательных эмоций; отсутствие склонности к риску; доминирование мотивации избегания неудачи над мотивацией стремления к успеху; высокую тревожность как личностную черту; сильные механизмы личностной защиты и ряд других.

Среди личностных черт, благоприятствующих творческому мышлению, выделяют следующие: уверенность в своих силах; доминирование эмоций радости и даже определенную долю агрессивности; склонность к риску; отсутствие боязни показаться странным и необычным; хорошо развитое чувство юмора; наличие богатого по содержанию подсознания; любовь к фантазированию и построению планов на будущее и т.п.

Хейз (Hayes, 1978) полагал, что творческие способности можно развить следующими способами [3]:

(1) Развитие базы знаний.

(2) Создание правильной атмосферы для творчества.

(3) Поиск аналогий.

Ниже приводятся некоторые рекомендации, обобщающие опыт педагогов и психологов, озабоченных развитием творческого потенциала своих воспитанников [2].

(1) Ни в коем случае не подавлять интуицию ученика.

(2) Формировать у учащегося уверенность в своих силах, веру в свою способность решить задачу.

(3) В процессе обучения желательно в максимальной степени опираться на положительные эмоции.

(4) Необходимо всемерно стимулировать стремление учащегося к самостоятельному выбору целей, задач и средств их решения.

(5) Следует в довольно широких пределах поощрять склонность к рискованному поведению.

(6) Важнейшая задача – не допускать формирования конформного мышления, бороться с соглашательством и ориентацией на мнение большинства.

(7) Развивать воображение и не подавлять склонность к фантазированию, даже если оно иногда граничит с выдаванием выдумки за истину. Особенно это касается начальных этапов обучения.

(8) Формировать чувствительность к противоречиям, умение обнаруживать и сознательно формулировать их.

(9) Чаще использовать в обучении задачи так называемого открытого типа, когда отсутствует одно правильное решение, которое остается только найти или угадать.

(10) Шире применять проблемные методы обучения, которые стимулируют установку на самостоятельное или с помощью преподавателя открытие нового знания, усиливает веру учащегося в свою способность к таким открытиям.

(11) Весьма полезным для развития творческого мышления является обучение специальным эвристическим приемам решения задач различного типа.

(12) Важнейшим условием развития творчества студентов является совместная с преподавателем исследовательская деятельность. Она возможна лишь в ситуации, когда решается задача, ответ на которую не знает ни студент, ни преподаватель.

(13) Наконец, самая главная, тринадцатая заповедь, – всячески поощрять стремление человека любого возраста быть самим собой, его умение слушать свое «Я» и действовать в соответствии с его «советами».

Действительно, научить решению конкретных творческих задач нельзя, однако, обучая, можно развивать те качества личности, которые способствуют решению творческих задач. Можно расширить круг интересов и освоенных деятельностей, можно научить рациональным приемам мышления, способствующим уяснению существа и особенностей решаемой творческой задачи. Наконец, можно обучать типовым процедурам выявления тех или иных особенностей и противоречий, типовым приемам устранения определенных противоречий [4].

Несмотря на распространенность концепции инсайта для объяснения актов творчества, концепция эта недостаточно конструктивна. В качестве руководства из нее следует лишь весьма размытая рекомендация; «Непрерывно думай о задаче и жди озарения».

Более конструктивной является ассоциативная гипотеза творчества. По этой гипотезе набор вариантов решения происходит вследствие появления ассоциаций, вызываемых конкретной постановкой решаемой задачи; последующий отбор наиболее подходящей из них и представляется главным моментом творчества. Ассоциативное мышление тем богаче, чем разнообразнее деятельности, в которых участвует индивид. Специалист, ограничивающий свои интересы только профессиональной сферой, обедняет свое творческое мышление. Рассмотренная концепция творчества считается одной из гипотез, поскольку объективных сведений о том, что в действительности происходит в психике человека при проявлении творчества пока нет.

Преподавательская деятельность неразрывно связана с творчеством. Практически при проведении каждого занятия приходится что-то изменять и в содержании учебного материала, и в методике обучения. Каждое занятие каждый раз получается новым. Таким образом, необходим инновационный учебно-методический комплекс.

Педагогическая и дидактическая роли новых информационных средств образовательной деятельности заключается в повышении эффективности всего учебного процесса, расширении возможностей для его управления в повседневной работе преподавателя и в перерастании процесса обучения в самообучение, саморазвитие, самореализацию в обществе. В наиболее явном виде роль новых средств обучения проявляется в лекционном процессе с использованием мультимедийной аудитории с обратной связью [5].

Современное поколение студентов выросло в новой культурной среде массовых увлечений, во многом со стереотипом восприятия окружающей действительности через призму шоу-бизнеса и развлекательных телепередач. С учетом этого, эмоциональная привлекательность для студентов может быть достигнута при использовании следующих приемов и средств подачи учебной информации.

(1) Игрового построения многоуровнего учебного пособия, при котором процесс изучения дидактического материала требует вовлечения в некоторое действие и активного управления им.

(2) Анимация и мультипликация в электронном конспекте лекции, в электронном учебном пособии, в видеослайд-лекции создает дополнительную информационную избыточность академическому учебному материалу, выполняя роль невербальных компонентов актов коммуникаций человека с человеком.

(3) Мультимедийные средства (киноклипы, видеофрагменты, аудиовизуальные вставки) в электронных пособиях восполняют дефицит аудиовизуальных аспектов коммуникаций при общении с «машиной» и придают подаче учебной информации вид, привычный и понятный новому поколению студентов.

(4) Афористичность и ирония в контексте электронных форм учебных материалов допустима в качестве средства создания определенной эмоциональной атмосферы при работе с пособием. Помимо эмоциональной привлекательности новых учебных электронных форм учебных материалов, средством мотивации качества учебной деятельности студентов является правильно организованная рейтинговая система оценок учебных достижений учащихся.

Важным мотивом познавательной деятельности студентов вуза является чувство эмоционального удовлетворения, связанного с самим процессом обучения и с достигнутым результатом обучения. Система оценок достигнутых результатов призвана формировать у студентов мотивацию к повышению качества результатов их труда.

Поиск соответствующей организационной структуры и учреждений образования (особенно, образования взрослых), которые обеспечили бы переход от принципа «образование на всю жизнь» к принципу «образование через всю жизнь» – важнейшая проблема XXI века [5].

Студенческий возраст характерен и тем, что в этот период достигаются многие оптимумы развития интеллектуальных и физических сил [6].

Значительная часть студентов стремится рационализировать свою учебную деятельность, найти наиболее эффективные приемы изучения материала. Успешность их усилий в данной области зависит от уровня развития:

(1) интеллекта;

(2) самоанализа;

(3) воли.

К оптимизации учебного процесса психология и педагогика могут подходить с разных позиций: совершенствования методов обучения, разработки новых принципов построения учебных программ и учебников, совершенствования работы деканатов, создания психологической службы в вузах, индивидуализации процесса обучения и воспитания при условии более полного учета индивидуальных особенностей обучающегося и др. Во всех этих подходах центральное звено – личность обучающегося. Знание психологических особенностей личности студента – способностей, общего интеллектуального развития, интересов, мотивов, черт характера, темперамента, работоспособности, самосознания и т.д., – позволяет изыскивать реальные возможности их учета в условиях современного массового обучения в высшей школе.

В настоящее время необходимо осуществить переход от информационно-объяснительного обучения студентов к деятельному, развивающему. Важными становятся не только усвоенные в вузе знания, но и способы усвоения, мышления и учебной деятельности, развитие познавательных сил и творческого потенциала студента. А этого можно добиться только при условии демократичности методов обучения, раскрепощения студентов, разрушения искусственных барьеров между преподавателями и студентами.

Развивающее обучение предполагает переход от типичной для традиционного обучения схемы «услышал – запомнил – пересказал» к схеме «познал путем поиска вместе с преподавателем и товарищами – осмыслил – запомнил – способен оформить свою мысль словами – умею применить полученные знания в жизни».

Знания, умения, навыки в области своей профессии – стержневая часть подготовки и развития студента.

В учебной деятельности объединятся не только познавательные функции деятельности (восприятие, внимание, память, мышление, воображение), но и потребности, мотивы, эмоции, воля.

Важнейшей педагогической задачей является конструирование особых базовых деятельностей, проблемных ситуаций в их функционировании и организации рефлексии. И такой путь обучения часто оказывается единственным, поскольку многому нельзя обучить прямо.

Если повысить уровень творческого мышления до уровня информационной культуры в области мультимедиа, развитие творческого мышления станет основой профессиональной самостоятельности в период начала трудовой деятельности [7].

Заключение

Содержание курса «Мультимедиа» не должно ограничивать тех, кто будет творить эту дисциплину завтра. Для этого преподавателям необходимо ставить такие творческие задачи, которые предполагают систематическое и последовательное преобразование имеющихся средств и технологий с учетом субъективного опыта студентов. Это, в свою очередь, предполагает развитие системного, диалектического мышления, продуктивного, пространственного воображения, применение алгоритмических и эвристических методов организации творческой деятельности. Подобные методы особенно эффективны в такой быстро меняющейся области знаний, как мультимедиа.

Литература

1. Гершунский Б.С. Философия образования для XXI века: Учеб. пособие для самообразования. – М.: Пед. о-во России, 2002. – 508 с.
2. Смирнов С.Д. Педагогика и психология высшего образования: от деятельности к личности: Учеб. пособие для студ. высш. пед. учеб. заведений. – М.: Издательский центр «Академия», 2001. – 304 с.
3. Солсо Р. Когнитивная психология – 6-е изд. – СПб.: Питер, 2006. – 589 с.
4. Фокин Ю.Г. Преподавание и воспитание в высшей школе: Методология, цели и содержание, творчество: Учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский центр «Академия», 2002. – 224 с.
5. Стародубцев В.А. Компьютерные и мультимедийные технологии в естественнонаучном образовании. – Томск: Дельтаплан, 2002. – 224 с.
6. Буланова-Топоркова М.В. Педагогика и психология высшей школы: Учеб. пособие. – Ростов н/Д: Феникс, 2002. – 544 с.
7. Шлыкова О.В. Культура мультимедиа – М.: ФАИР-ПРЕСС, 2004. – 414 с.

УДК 378.147

ЕВРОПЕЙСКАЯ КРЕДИТНО-ТРАНСФЕРТНАЯ СИСТЕМА КАК ФАКТОР ПОВЫШЕНИЯ МЕЖДУНАРОДНОЙ КОНКУРЕНТОСПОСОБНОСТИ ОБРАЗОВАТЕЛЬНЫХ УСЛУГ

Г.Н. Подгорная
(Белорусский государственный экономический университет)
Научный руководитель – к.т.н., доцент Б.А. Железко
(Белорусский государственный экономический университет)

Анализируются результаты реализации в странах СНГ Болонского процесса по созданию единого европейского образовательного пространства на примере внедрения рейтинговых систем оценки знаний, умений и навыков студентов. При этом анализируется опыт вузов Украины, России и Беларуси. Отмечается, что внедрение кредитно-модульной системы является действующим фактором повышения международной конкурентоспособности образовательных услуг отечественных вузов.

Ключевые слова: Болонский процесс, рейтинговые системы оценки знаний, Европейская кредитно-трансфертная система

Введение

Повышение международной конкурентоспособности образовательных услуг отечественных вузов является объективной необходимостью, поскольку может обеспечить скорейшее преобразование высокого интеллектуального потенциала сферы высшего образования в реальный экспортный потенциал. Одним из условий такого преобразования является обеспечение реализации единой международной процедуры измерения и сравнения результатов обучения студентов, их академической успеваемости [1]. При этом за основу берется Европейская кредитно-трансфертная система (ECTS).

Основная часть

В работе анализируются результаты реализации в странах СНГ Болонского процесса по созданию единого европейского образовательного пространства на примере внедрения рейтинговых систем оценки знаний, умений и навыков студентов. При этом анализируется опыт вузов Украины, России и Беларуси как показано в табл. 1.

Таблица 1. Обзор рейтинговых систем Украины, России и Беларуси

Название ВУЗа (страна)	Система обучения	Особенности	Период внедрения	Источник информации
Киевский национальный торгово-технический университет, Украина	Кредитно-модульная система организации учебного процесса (ECTS)	Учебный год приравнивается 60 кредитам. Для получения степени бакалавра, что насчитывает 3–4 года обучения, приравнивается к 180–240 кредитам.	5 лет	[2]
Поморский Государственный Университет им. М.В. Ломоносова, Россия	Система зачетных единиц	Трудоемкость учебной работы во всех учебных планах устанавливается в зачетных единицах. Рабочий план должен включать три группы дисциплин.	3 года	[3]

Название ВУЗа (страна)	Система обучения	Особенности	Период внедрения	Источник информации
Мурманская Академия Экономики и Управлении, Россия	Регулярная аттестация студентов (ретинговый принцип)	За семестр можно зарабатывать до 100 баллов. Сама рейтинговая система складывается из следующих составляющих: 1. до 78 баллов можно получить за три промежуточных экзамена (каждый экзамен оценивается максимум 26 баллов); 2. до 12 баллов можно получить за РГЗ; 3. 10 баллов дается авансом за посещаемость практических занятий и ответы на них.	–	–
Дальневосточный Государственный Университет, Россия	Рейтинговая система	Компьютерное сопровождение рейтингового контроля осуществляется с помощью информационно-аналитической системы WEBRATE ДВГУ	–	[4]
Белорусский Государственный Экономеческий Университет, Беларусь	Рейтинговая система	Система включает подсчет и учет баллов, полученных студентами в течение семестра. Удельный вес отдельных видов текущего контроля устанавливается кафедрой с учетом специфики предмета и должен составлять не менее 20%	1 год	[5]

В **Украине** (например, в Киевском национальном торгово-экономическом университете) реализована модель организации учебного процесса, основанная на объединении модульных технологий обучения и зачетных кредитов (кредитно-модульная система организации учебного процесса). Для реализации в высших учебных заведения Украины кредитно-модульной системы организации учебного процесса необходимо было в течении нескольких лет подготовить следующие элементы ECTS: 1) Полный информационный пакет – сведения про университет, названия направлений, специальностей, специализаций, содержания модулей с обозначением обязательных факультативных курсов, методики и технологии преподавания, зачетные кредиты, формы и условия проведения контрольных знаний, система оценивания качества знаний. 2) Договор на обучение между студентом и руководством ВУЗа – направление обучения, научно-квалификационный уровень, порядок расчетов. 3) Академическая справка оценивания полученных знаний – свидетельство достижений студента в системе кредитов, по шкале национального уровня и по системе ECTS. Пример соответствия шкалы оценивания ECTS национальной системе оценивания в Украине приведен в табл. 2.

Оценка по шкале ECTS	Определение	Оценка	
		По национальной системе Украины	По 100-й системе
A	Отлично – отличное выполнение с незначительным количеством ошибок	Отлично	90–100

Оценка по шкале ECTS	Определение	Оценка	
		По национальной системе Украины	По 100-й системе
B	Очень хорошо – выше среднего уровня с некоторыми ошибками.	Хорошо	82–89
C	Хорошо – правильная работа с определенным количеством значимых ошибок.		75–81
D	Удовлетворительно – неплохо, но с значительным количеством ошибок	Удовлетворительно	69–74
E	Достаточно – удовлетворительное выполнение минимального критерия		60–68
FX	Неудовлетворительно – необходимо поработать перед пересдачей	Неудовлетворительно	35–59
F	Неудовлетворительно – необходима серьезная дополнительная работа, обязательный повторный курс.		1–34

Таблица 2. Соответствия шкалы оценивания ECTS национальной системе оценивания в Украине

В **российских** вузах реализовано внедрение балльно-рейтинговой системы в университетское образование. Этим обеспечивается переход от коллективной к индивидуальной форме обучения и студент становиться непосредственным участником организации своей образовательной деятельности, которая оценивается подсчетом баллов, «заработанных» в течение семестра. При этом предусматривается три уровня контроля успеваемости. *Академический рейтинг студента* – уровень успешности студента в освоении образовательных дисциплинах в сравнении с другими студентами. Определяется количество набранных баллов за определенный промежуток времени (например, семестр), в соответствии с максимальным количеством баллов по этой дисциплине, утвержденным учебным планом. *Рубежная аттестация* – контроль успеваемости студента, проводимый, как правило, 1 раз в середине семестра. Может быть проведена в двух вариантах: (1) преподаватель подсчитывает общее количество баллов за отчетный период; (2) студент набирает очередное количество баллов, выполняя проверочную работу (включена в технологическую карту), в форме, определяемой преподавателем. *Итоговая аттестация* – контроль успеваемости, в результате которого набирается очередное количество баллов, осуществляется один раз в конце семестра в форме, определяемой преподавателем.

Например, в Поморском Государственном Университете имени М.В. Ломоносова трудоемкость учебной работы во всех учебных планах устанавливается в зачетных единицах (1 зачетная единица, как правило, равна 36 академическим часам). По степени обязательности и последовательности усвоения содержания образования рабочий план должен включать три группы дисциплин: (а) группа дисциплин, изучаемых обязательно и строго последовательно во времени; (б) группа дисциплин, изучаемых обязательно, но, возможно, не последовательно; (в) дисциплины, которые студент изучает по своему выбору. Индивидуальный учебный план формируется по установленной форме на каждый учебный год лично студентом, при необходимости с помощью академического консультанта.

По результатам текущей аттестации студенту выставляется зачет в целых единицах (кредитах), характеризующих трудоемкость освоения дисциплины, и в

баллах, и в соответствующих им оценках, определяющих качество освоения студентом знаний, умений и навыков в рамках данной дисциплины.

Организация рейтинговой системы оценивания в Мурманской Академии Экономики и Управления (МАЭУ) проходит по следующей системе.

В МАЭУ рассматривается один из вариантов равномерной работы студентов. За основу был взят международный опыт регулярной аттестации студентов. Для обработки методики была взята дисциплина «Теория систем и системный анализ». Из форм контроля по дисциплине предусмотрено расчетно-графическое задание (РГЗ) и экзамен.

В течение семестра студенты сдают три письменных экзамена. Каждый из экзаменов содержит блок из 70–200 вопросов теоретического и практического характера, требующих конкретных ответов. На экзамене студент получает список всех вопросов блока и номера 15-ти, на которые надо дать письменные ответы. Каждый вопрос, в зависимости от сложности, оценивается от 1 до 3-х баллов. Экзамен длиться 2 академических часа.

При выполнении РГЗ возникают две проблемы: небрежное выполнение и несвоевременная сдача. Для их решения применяется следующее.

В целом РГЗ оценивается в 12 баллов, из них 9 баллов за полноту раскрытия темы и до 3 баллов за оформление. Далее, за досрочную сдачу РГЗ на неделю добавляется 2 балла, а за каждый день задержки – вычитается 1 балл.

На практических занятия имеют место две проблемы: студенты пропускают занятия и не готовятся к занятиям дома, надеясь все выучить перед экзаменом. В связи с этим вводятся штрафные баллы:

1. за каждый пропуск по неуважительной причине практического занятия вычитается 1 балл;
2. за отказ отвечать на практическом занятии – 0,5 балла.

Итоговая оценка складывается из результатов промежуточных экзаменов, оценки за РГЗ и отрицательных баллов за работу на практических занятиях.

Основная проблема – большая трудоемкость по подготовке и проверке результатов письменного экзамена. Наверное, экзамен в форме теста было бы менее трудоемко проверять, но он не дает глубины проверки и не заставляет студента формулировать свои мысли.

Организация рейтинговой системы оценивания в Дальневосточном Государственном Университете (ДВГУ) проходит по следующей системе.

Итоговая рейтинговая оценка учебной деятельности студента выражается в процентах и показывает степень освоения им учебного материала, предусмотренного рабочей программой учебной дисциплины. Рейтинговая оценка может быть определена по одной, нескольким, всем дисциплинам учебного семестра и по итогам выполнения образовательной программы.

Компьютерное сопровождение рейтингового контроля осуществляется с помощью информационно-аналитической системы WEBRATE ДВГУ, которая является собственной разработкой ДВГУ и удостоена золотой медали Выставки достижений Дальневосточного Федерального округа.

При применении моделей рейтингового оценивания используется понятие «идеальный студент». Сравнивая успеваемость реальных студентов с учебными «достижениями» введенного эталона, можно оценить степень усвоения студентами содержания учебной дисциплины.

Вид контроля учебной деятельности студентов определяется преподавателем в зависимости от формы занятий, предусмотренных рабочим учебным планом:

– для лабораторных занятий – традиционная проверка отчетов, оценка выполненных заданий и др.;

– для практических (семинарских) занятий – оценка выступления, решения задач, выполнения контрольных работ (в том числе тестирование) и др.;

– для лекций – тестовая оценка знаний студентов (бланковое тестирование на лекционном занятии или компьютерное тестирование в установленное преподавателем время), коллоквиум, экспресс-опрос и др.

Оценка учебной деятельности производится преподавателем одновременно для всех студентов по выбранным формам контроля на каждом занятии или так часто, как этого требует специфика дисциплины и вид занятия, но не реже 4 раз за учебный семестр:

– для лабораторных занятий – на каждом занятии или по мере завершения лабораторной работы и сдачи отчета;

– для практических (семинарских) занятий – по мере изучения темы, блока тем или раздела (модуля);

– для лекций – по мере завершения изучения модуля.

Преподаватель проводит текущее оценивание учебных достижений студентов по дисциплине, в соответствии с графиком контрольных мероприятий в рейтинг-плане. Эта информация регулярно вносится в систему WEBRATE ДВГУ, которая автоматически осуществляет перевод текущих оценок в рейтинговые баллы.

Деканаты факультетов, в день выставления оценок на основе рейтинга, получают из системы WEBRATE ДВГУ итоговую таблицу рейтинговой оценки успеваемости студентов (рейтинговую ведомость) по всем дисциплинам, участвующим в рейтинговом контроле. Рейтинговая ведомость в распечатанном виде, заверенная подписью декана, выдается преподавателю вместе с бланком экзаменационной (зачетной) ведомости и служит основанием для подведения итогов аттестации согласно рекомендованной шкале соответствия рейтинговых и традиционных оценок.

В **Республике Беларусь** (например, в Белорусском государственном экономическом университете) внедряется рейтинговая система оценки знаний, умений и навыков студентов. Система включает подсчет и учет баллов, полученных студентами в течение семестра на практических, лабораторных и семинарских занятиях, оценку по индивидуальной (письменной контрольной) работе и экзаменационную оценку. Система предполагает постоянный контроль знаний, умений и навыков студентов, который осуществляется преподавателями не реже трех-четырех раз в семестр после изучения отдельных тем и разделов курса с обязательной оценкой. Содержание и форма контроля знаний определяются по каждой дисциплине в рабочей программе, обсуждаются и утверждаются на кафедре и доводятся до сведения студентов на первом занятии по данной дисциплине. Текущая оценка знаний учитывается при определении итоговой (выставляемой на экзамене) оценки. Удельный вес отдельных видов текущего контроля устанавливается кафедрой с учетом специфики предмета и должен составлять не менее 20 %.

Заключение

Таким образом, проведенный анализ показывает, что хотя европейская кредитно-трансфертная система разработана для обеспечения мобильности студентов, упрощения понимания и сравнения учебных программ и учебных достижений студентов, ее внедрения на постсоветском образовательном пространстве происходит поэтапно и сопряжено с необходимостью гармонизации законодательной базы и преодоления инерции мышления как со стороны преподавателей, так и со стороны студентов. Тем не менее, она является реально действующим фактором повышения международной конкурентоспособности образовательных услуг отечественных вузов

Литература

1. Мижевич О.М. Европейское сотрудничество в области высшего образования: опыт и перспективы// Инновационные технологии в бизнес-образовании: сборник научных статей Международного весеннего форума: в 2 ч. / редкол.: С.Н. Лебедева, Л.В. Мисникова, Г.С. Митюрич. – Гомель: учреждение образования «Белорусский торгово-экономический университет потребительской кооперации», 2008. – Ч.2. – С. 169–174.
2. Сучасні освітні технології у віщій школі: Матеріали міжнар. наук.-метод. конф. (Київ, 1–2 листопада 2007 року): Тези доповідей: У 2 ч. – Ч.2/ Відп. ред. А.А. Мазаракі. – К.: Київ. нац.торг. екон.ун-т, 2007. – 259 с.
3. О реализации принципов Болонской декларации в Поморском университете [Электронный ресурс]. – 2004. Режим доступа: www.pomorsu.ru/_doc/quality/normativ/26_02_04.pdf – дата доступа: 14.01.2009.
4. Козлов В.А. Результаты внедрения рейтинговой системы оценки знаний в учебный процесс / В.А. Козлов, А.В. Голенков, Г.Д. Аникин // Известия Российской академии образования. – 2002. – № 1. – С. 85–89.
5. Положение о рейтинговой системе оценки знаний, умений и навыков студентов в УО «Белорусский государственный экономический университет» (БГЭУ) [Электронный ресурс]. – 2008. Режим доступа: http://www.bseu.by/russian/student/reyting.htm. – дата доступа: 15.02.2009.

УДК 378; 311.4

МОНИТОРИНГ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ И ПРОГНОЗИРОВАНИЕ ОСНОВНЫХ ПАРАМЕТРОВ ЕГО РАЗВИТИЯ В Г. САНКТ-ПЕТЕРБУРГЕ

А.С. Осташова
Научный руководитель – д.э.н., профессор С.Б. Смирнов

В статье раскрыты такие понятия, как: мониторинг, его характеристика, цели и задачи, описана методика его проведения, а также сделаны прогнозы тенденций развития спроса на образование в Санкт-Петербурге.

Ключевые слова: высшее профессиональное образование, мониторинг, прогнозирование

Введение

Проводимая в РФ реформа всей системы образования на основе федеральной Концепции модернизации образования предполагает перенос на региональный уровень решения многих важных вопросов формирования, поддержания и развития сферы высшего образования. Реализация этой политики в Санкт-Петербурге требует разработки механизмов концентрации ограниченных ресурсов и оптимизации структуры, основных параметров функционирования и развития системы ВПО. Очевидно, что эффективное решение этих задач возможно только на основе мониторинга, комплексной оценки и анализа реального состояния системы ВПО. Требуются исследования, позволяющие выявить закономерности развития данной сферы в Санкт-Петербурге, спрогнозировать ее состояние на будущее с целью упреждающего реагирования органами исполнительной власти Санкт-Петербурга, учреждениями ВПО на выявленные тенденции.

Общая характеристика мониторинга

Термин «мониторинг» получил массовое распространение в последние два десятилетия. Так, упоминание мониторинга встречается более чем в 6 тыс. документов, принятых российскими законодателями на разных уровнях государственного управления.

Мониторинг высшего профессионального образования – это комплексная система наблюдений за его состоянием, системный анализ всех закономерностей его развития и прогноз изменений под воздействием социальных, экономических и иных факторов.

Назначение системы мониторинга состоит в создании и поддержании информационной базы управления развитием системы высшего профессионального образования.

Цель мониторинга – разработка методов анализа и прогнозирования состояния научно-образовательного потенциала высшего профессионального образования Санкт-Петербурга путем создания постоянно действующей системы сбора и обработки данных, получаемых методом проведения ежегодного мониторинга высших учебных заведений Санкт-Петербурга различных организационно-правовых форм [2].

Задачи мониторинга:

– сбор и статистическая обработка комплекса показателей и индикаторов, характеризующих текущее состояние системы высшего образования в городе;

– подготовка предложений по оптимизации структуры системы высшего профессионального образования (ВПО) Санкт-Петербурга с разработкой методических и нормативных подходов к ее реорганизации на основе интеграционных

подходов, обеспечивающих оптимизацию и повышение эффективности функционирования системы в современных условиях;

– разработка методов анализа и прогнозирования состояния научно-образовательного потенциала высшего профессионального образования Санкт-Петербурга путем создания постоянно действующей системы сбора, обработки и хранения данных, получаемых методом проведения ежегодного мониторинга образовательных учреждений, включая мониторинг соблюдения лицензионных и аккредитационных требований и нормативов;

– формирование прогноза развития наиболее важных факторов, влияющих на состояние системы высшего профессионального образования Санкт-Петербурга, включая ее кадровое обеспечение (прогнозирование потребности в профессорско-преподавательских кадрах).

Научная ценность ожидаемых результатов заключается в возможности исследования закономерностей развития научно-образовательного потенциала системы ВПО Санкт-Петербурга.

Методика проведения мониторинга

Методика проведения предполагает следующие виды работ:

1) организация сбора статистических и социологических данных;

2) оценка и системный анализ полученной информации, выявление тенденций и динамики происходящих в сфере образования процессов;

3) создание информационной базы данных;

4) оценка полученной информации, выявление тенденций и динамики происходящих процессов;

5) представление результатов исследования всем заинтересованным пользователям (органам управления образованием, местному и профессиональному сообществу).

Прогнозирование основных параметров развития мониторинга высшего профессионального образования в г. Санкт-Петербурге

Прогнозирование – опережающее отражение будущего; вид познавательной деятельности, направленный на определение тенденций динамики конкретного объекта или события на основе анализа его состояния в прошлом и настоящем.

Прогноз составлен с помощью программы SPSS (Statistical Package for Social Science). SPSS для Windows – это мощная система статистического анализа и управления данными. Анализ временного ряда осуществлен с помощью процедуры подгонки кривых, которая позволяет вычислять статистики и строить сопутствующие графики для 11 различных регрессионных моделей оценки кривых. Для каждой зависимой переменной подобрана отдельная модель, наиболее точно описывающая временной ряд, на основании которой составлен прогноз. В качестве основных параметров прогнозирования взяты численность и прием студентов в ВУЗах Санкт-Петербурга [4, 5].

В результате анализа было выявлено, что квадратичная модель наиболее точно описывает оба параметра. С помощью этой модели были сделаны прогнозы, изображенные на рис. 1 и 2 пунктирной линией.

За последние года наблюдается уменьшение приема студентов в ВУЗы Санкт-Петербурга. Такая отрицательная тенденция неудивительна, если взглянуть на динамику численности выпускников общеобразовательных учреждений (рис. 3).

Данный анализ позволяет нам с определенной точностью сказать, что потребление населением образовательных услуг в Санкт-Петербурге уменьшается с каждым годом.

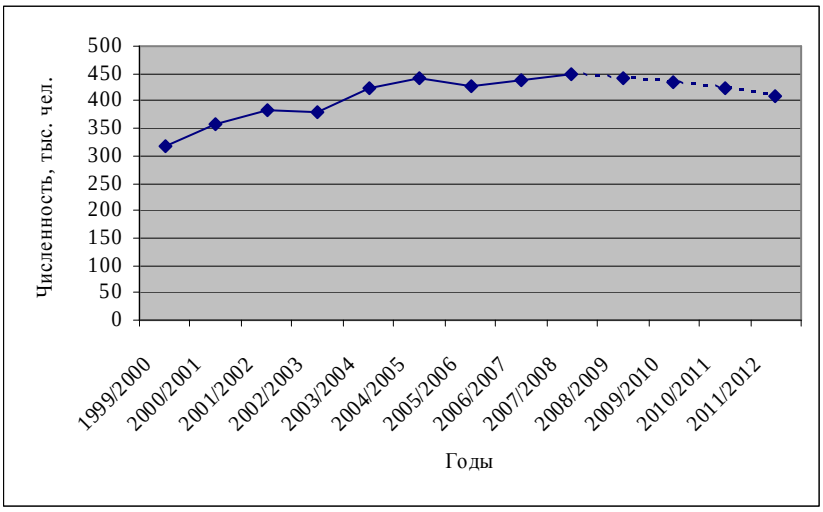


Рис. 1. Динамика численности студентов в ВУЗах Санкт-Петербурга

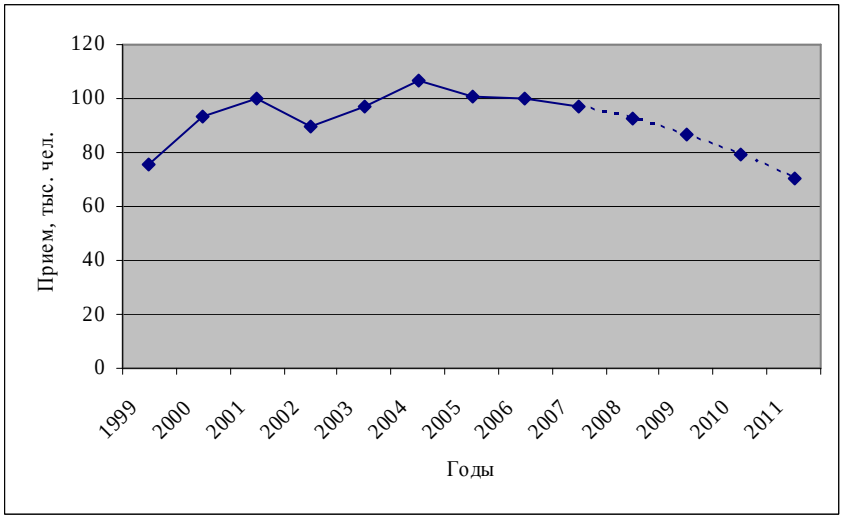


Рис. 2. Динамика приема студентов в ВУЗы Санкт-Петербурга

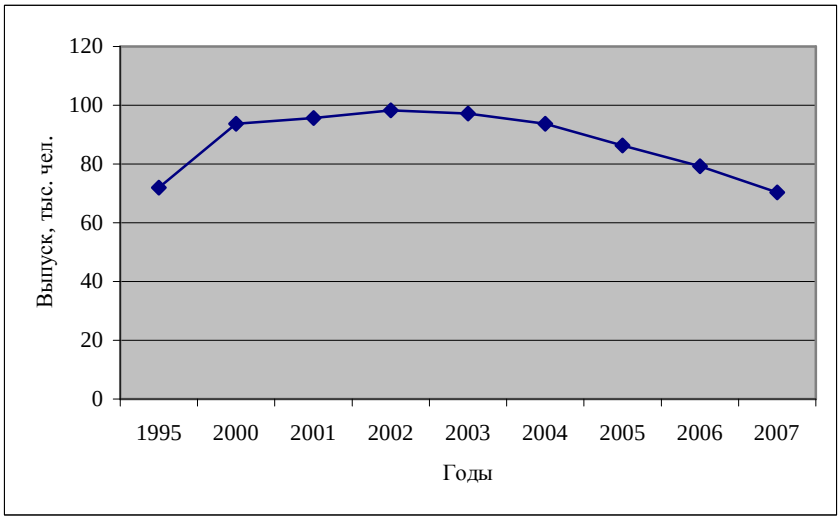


Рис. 3. Динамика численности выпускников дневных общеобразовательных учреждений Санкт-Петербурга

Заключение

В наши дни Россия стремительно развивается практически по всем направлениям. Данное развитие, отчасти, является результатом роста числа квалифицированных специалистов в различных областях и улучшения социально-экономического положения и уровня жизни населения в стране в целом. Одним из наиболее важных факторов, влияющих на данное развитие, является рост доступности образования и улучшение его качества, что возможно только путем создания постоянно действующей системы сбора и обработки данных, получаемых методом проведения ежегодного мониторинга высших учебных заведений различных организационно-правовых форм.

За последние годы наблюдается значительное уменьшение количества выпускников школ, что является отрицательной тенденцией и, конечно, не может не отразиться на рынке образовательных услуг. В Санкт-Петербурге за 2004–2007 годы наблюдается уменьшение количества принятых в высшие учебные заведения студентов на 9 тыс. человек. Ожидается, что такая отрицательная тенденция сохранится на следующие несколько лет.

Литература

1. Агранович М. Система высшего образования региона и устойчивое развитие: попытка статистического анализа / М. Агранович // Сборник докладов и материалов Всероссийского научно-практического семинара «Образование и наука как факторы устойчивого развития региона». – Тверь, 2003. – С. 101–108.
2. Абдуллина О.А. Мониторинг качества профессиональной подготовки / О.А. Абдуллина. – М.: Пед. вуз, 1998. – 154 с.
3. Майоров А.Н. Мониторинг в образовании / А.Н. Майоров. – М.: Интеллект-Центр, 2005. – 432 с.
4. Регионы России. Социально-экономические показатели. 2005: Р32 Стат. сб. / Росстат. – М., 2006. – 982 с.
5. Регионы России. Социально-экономические показатели. 2008: Р32 Стат. сб. / Росстат. – М., 2008. – 999 с.

УДК 378.14 + 378.374

АНАЛИЗ МОТИВАЦИИ СТУДЕНТОВ СПБГУ ИТМО К ПОИСКУ РАБОТЫ ПО СПЕЦИАЛЬНОСТИ

О.В. Зеленская
Научный руководитель – к.т.н., доцент Н.Н. Горлушкина

В настоящее время проблема трудоустройства выпускников высших учебных заведений по специальности является актуальной. Для вуза важно обеспечить конкурентоспособность на рынке труда своих выпускников именно по специальности, полученной в период обучения. Для этого важно иметь представление о мотивации студентов к поиску работы по специальности. Первым и важнейшим шагом к разработке стратегии университета по содействию в трудоустройстве студентов и выпускников по своей специализации является анализ мотивации студентов университета.

Ключевые слова: мотивация, поиск работы, трудоустройство, специальность

Введение

Процесс совершенствования подготовки будущих специалистов в условиях современного образования обусловлен многими факторами, среди которых существенным является *мотивация* студентов. Проблема мотивации является одной из фундаментальных в социологии и в психологии [1]. Социологические исследования в среде студентов имеют существенное практическое значение для оптимизации учебного процесса. На протяжении многих лет публикуются материалы в различных изданиях, посвященные мотивации студенчества [1–8].

В качестве мотивов личности могут выступать предметы внешнего мира, представления, идеи, чувства и переживания – словом, все то, в чем находит воплощение потребность [9].

Как показывают социологические исследования [1–5], мотивация студентов неоднородна, она зависит от множества факторов: индивидуальных особенностей студентов, характера ближайшей референтной группы, уровня развития студенческого коллектива. С другой стороны, мотивация поведения человека (в нашем случае – студента) всегда есть отражение взглядов, ценностных ориентации, установок того социального слоя, представителем которого он является. Поэтому условием и источником познавательной, научной, общественной активности студентов, побудительной причиной их разнообразной деятельности в вузе является сложная структура мотивов. Например, учебная мотивация студентов выступает как частный вид мотивации, включенный в определенную деятельность, в данном случае – учебную. Она определяется рядом специфических факторов; во-первых, самой образовательной системой, образовательным учреждением; во-вторых, – организацией образовательного процесса; в-третьих – субъективными особенностями обучающегося; в-четвертых, – особенностями педагога и, прежде всего, системы его отношений к студенту; в-пятых, – спецификой учебного предмета [2].

Отношение студентов к профессии, т.е. к целям вузовского обучения, наполняется профессиональным смыслом и содержанием в ходе учебной деятельности, которая выступает относительно профессиональных целей обучения в качестве средства их достижения. Отношение к учению как к средству достижения профессиональных целей образует *мотивацию профессиональной деятельности.* По степени ее сформированности можно судить о готовности студентов к профессиональной деятельности.

Постановка задачи

В университете два раза в учебном году проводятся «Ярмарки вакансий» для всех факультетов, выпускающих специалистов по различным направлениям подготовки.

Любая фирма или предприятие предлагает вакансии, на которые могут претендовать выпускники любой специальности Санкт-Петербургского государственного университета информационных технологий, механики и оптики (СПбГУ ИТМО). Однако, «Ярмарки вакансий» не способны охватить весь спектр фирм и предприятий, учитывая специфику подготовки специалистов некоторых факультетов, так как чаще всего фирмы подбираются таким образом, чтобы на ярмарке присутствовали один-два представителя для каждого факультета. Например, сложность в выборе вакансии возникает, когда речь заходит, об инженере – проектировщике оптических систем. В данном случае речь идет именно о фирме или предприятии, осуществляющих свою деятельность в этом направлении. В вузе есть два факультета: факультет оптико-информационных систем и технологий (ФОИСТ) и инженерно-физический факультет (ИФФ), которые выпускают специалистов для оптической промышленности. На факультете оптико-информационных систем и технологий (ФОИСТ) в 2008 году обучалось 842 человека и 350 из них – представители 4, 5, 6 курсов. Согласно материалам исследования Р.К. Малинаускаса «Мотивация студентов разных периодов обучения» [1], заинтересованы в поиске работы по специальности именно студенты старших курсов, в частности студенты 4-го года обучения. Вполне естественно представить, что подавляющее большинство специалистов только ФОИСТа не могут быть обеспечены работой на «Ярмарке вакансий», даже если проводить это мероприятие чаще. Тем более, не смогут их обеспечить рабочими местами на «Ярмарках вакансий», проводимых в других вузах. Специалистов этого профиля готовит только СПбГУ ИТМО. Возникает ситуация, когда в целях более подробного знакомства необходимо проводить похожие мероприятия для отдельных факультетов. Чаще всего студенты именно этих двух факультетов: ФОИСТ и ИФФ, подрабатывают во время обучения не по специальности, как, впрочем, и после окончания вуза устраиваются на работу. Причиной является неосведомленность о фирмах соответствующего профиля, страх перед работодателем (например, мои теоретические знания не соответствуют требованиям и т.д.), неуверенность в востребованности выбранной специальности на рынке труда.

В качестве решения выявленной проблемы можно предложить несколько вариантов:

1) проведение тематических «Ярмарок вакансий» в университете;
2) проведение мероприятия на каждом факультете «Знакомство с будущим работодателем», учитывающим специфику подготовки студентов факультета;
3) выявление мотивации студентов к поиску работы по специальности, и исходя из полученных результатов, разработка программы работы со студентами.

Цель исследования

Целью исследования было изучение мотивации студентов разных курсов факультета оптико-информационных систем и технологий к поиску работы по специальности. При проведении эксперимента учитывались материалы исследования Р.К. Малинаускаса «Мотивация студентов разных периодов обучения».

Методы исследования

Использовались следующие методы опроса: анкетирование студентов разных курсов обучения. Анкета содержала вопросы закрытого и открытого типа, в анкете содержались перекрестные вопросы. Опросы проводились в три этапа – 2005, 2006 и 2008 годы, в статье проведен сравнительный анализ полученных результатов. В 2006 году проводились опросы студентов университета на «Ярмарке вакансий», при обработке сравнивались результаты ответов студентов ФОИСТа и студентов других факультетов университета, сравнительные таблицы приведены в заключительной части статьи.

Основной результат

Исследование проводилось в течение 4 лет в три этапа. Первый этап – 2005 год – с целью мониторинга мнений студентов факультета об актуальности организации и проведения мероприятия в рамках факультета, проводилось анкетирование студентов ФОИСТ – ни один студент не принял участия в анкетировании, распространялись памятки для выпускников факультета – ни один выпускник не откликнулся (146, включая вечерников).

Второй этап – 2006 год – решение об организации и проведении мероприятия было принято без учета мнения студентов – анкетирование студентов факультета проводилось непосредственно на мероприятии. В итоге 23 человека из 88 зарегистрировавшихся участников (фактическое число варьировалось от 100 до 150 человек) ответили на вопросы анкеты, что составило 26% от общего числа зарегистрированных участников. Аудитория оказалась неподготовленной к опросу. Студенты ответили не на все вопросы. Наибольшие затруднения возникли с ответами на вопросы, в которых необходимо было сформулировать собственное мнение.

Третий этап – 2008 год – опорос также проводился на мероприятии, 44 человека из 142 ответили на вопросы анкеты, что составило 31% от общего числа студентов, посетивших мероприятие.

	2006	2008
Количество человек, ответивших на вопросы анкеты	23	44
1. Наличие опыта трудоустройства:		
Есть	47,8%	50%
Нет	30%	27,3%
2. Готовность рассказать о себе работодателям:		
Да	69,6%	75%
Нет	4,3%	9%
Не ответили	26,1%	16%
3. Для формирования программы работы со студентами по социальной адаптации к рынку труда предлагалось выбрать наиболее интересующие пункты:		
Возможность общения с работодателями		
Технологии поиска работы	73,9%	77,3%
Как писать резюме	43,5%	59%
Консультация юриста	21,7%	27,3%
Общение с выпускниками	17,4%	4,5%
	17,4%	6,8%

Таблица 1. Сравнительная таблица ответов студентов в 2006 и 2008 гг. всех курсов

«Знакомство с будущим работодателем» стало мероприятием, проведенным впервые для студентов ФОИСТа в 2006 году. Цель мероприятия состояла в том, чтобы дать студентам факультета краткий обзор предприятий и фирм, работающих в области оптической промышленности; ознакомить студентов с требованиями работодателей; предоставить возможность личного общения с работодателями, предлагающими рабочие места по специальности. На мероприятие были приглашены студенты Инженерно-физического факультета, обучающиеся по оптическим направлениям. Посетить мероприятие могли все желающие.

Мероприятие было запланировано в форме презентаций каждой отдельной компании. Была предусмотрена возможность свободного перемещения по аудитории по окончании презентаций и общения с представителями компаний.

Перед началом мероприятия проводилась регистрация студентов пришедших на мероприятие: до начала мероприятия зарегистрировалось 88 человек, из них 74% со-

ставили студенты ФОИСТ, 19% – студенты ИФФ, 3% – студенты ФКТУ, 4% – выпускники университета. Данное распределение иллюстрирует Диаграмма 1.

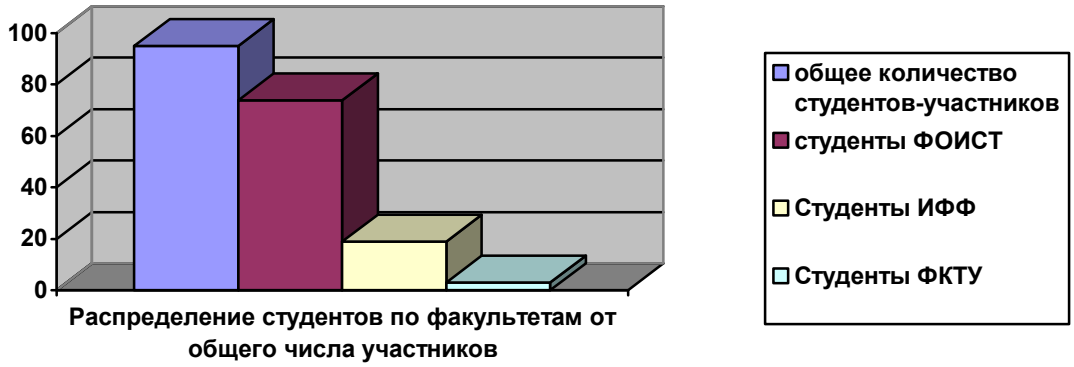


Диаграмма 1

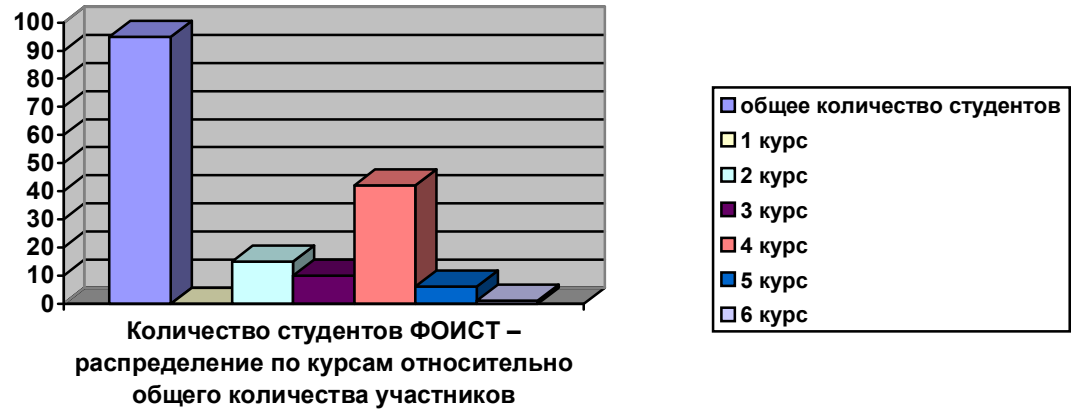


Диаграмма 2

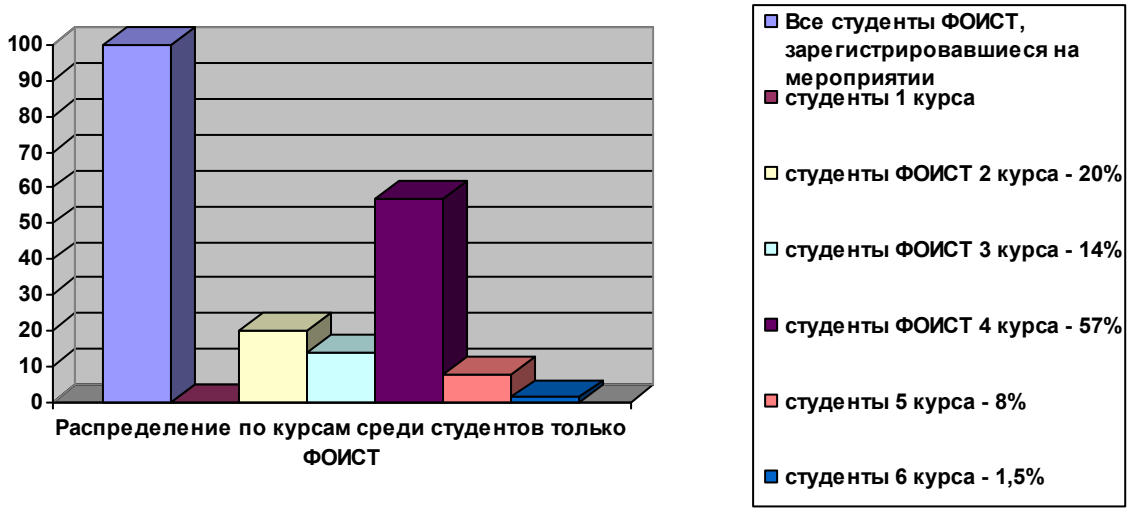


Диаграмма 3

Дальнейший анализ результатов показал, что из всех студентов, посетивших мероприятие, распределение по курсам произошло следующим образом: из первокурсников не зарегистрировался ни один человек, представители второго курса составили 15% от общего числа зарегистрировавшихся, 3 курс – 10%, 4 курс – 42%, 5 курс – 1%, 6 курс – 3%. Диаграмма 2 иллюстрирует полученное распределение по курсам.

Далее, анализ результатов показал, что из всех студентов, пришедших на мероприятие распределение студентов ФОИСТ по курсам произошло таким образом: из представителей 1 курса не зарегистрировался ни один человек, 2 курс составил 20% от общего числа зарегистрировавшихся студентов ФОИСТ, 3 курс – 14%, 4 курс – 56,9%, 5 курс – 8%, 6 курс – 1,5%. Данное распределение показывает Диаграмма 3.

В 2006 году 39,1% студентов отметили вопросы, связанные с рынком труда волнующие их больше всего – возможность работы по своей специальности; зарплата и график; проблема трудоустройства в период обучения. В 2008 году 59% от общего числа ответивших отметили такие вопросы, как: зарплата, условия труда, востребованность специальности, возможность трудоустройства студентов на время учебы и дальнейшая работа по специальности; перспективность; возможность профессионального и карьерного роста; возможность развития личности; международный уровень поиска работы.

В 2006 году на вопрос о том, с какими проблемами пришлось столкнуться при поиске работы ответили 34,8% респондентов. Среди перечисленных проблем чаще всего встречаются такие как отсутствие заинтересованности работодателей в приеме на работу студентов старших курсов; проблема оформления документов; недостаточный опыт трудоустройства; совместимость графика работы с учебой; для работы по специальности требуется опыт работы на ней. В 2008 году на этот же вопрос ответили 56,8% опрошенных, указали такие проблемы, как «трудно совмещать работу с учебой»; требование опыта работы; отсутствие возможности общения с работниками организации, чтобы услышать отзывы; несоответствие обещаний действительности; нехватка опыта, отсутствие резюме и опыта работы; сложность при прохождении собеседования; неготовность работодателя трудоустроить на краткосрочный период; высокие требования к выпускнику.

В 2006 году на вопрос о том, какие фирмы интересуют, ответили 34,8% студентов. Ответы были расплывчатыми, общего характера, фирмы, указанные в анкетах не все соответствовали направлению подготовки специалистов данного профиля. В 2008 на этот же вопрос ответили 54,6% респондентов, в своих ответах студенты указали конкретные фирмы, среди которых встречаются названия фирм, принимавших участие в мероприятиях «Знакомство с работодателями», появляется интерес не только к фирмам, где можно работать по специальности, выражается желание заниматься проектированием, разработками, научной деятельностью в рамках специализации.

На вопрос, каким видом деятельности хотелось бы заниматься, ответы студентов ФОИСТ распределились таким образом: разработка технических изделий – 39,1%; эксплуатация техники – 30,4%; производственные процессы – 17,4%; реклама, маркетинг – 26%. Последний вопрос предлагаемой анкеты оставался открытым, в 2006 году инициативу не проявили, в 2008 году – появились ответы, сформулированные самими студентами: управление производством; фундаментальные исследования в области оптико-электронных приборов и систем.

Результаты моделирования

В 2006 году проводился опрос студентов, посетивших вторую ярмарку вакансий, проводимую в университете. В опросе приняло участие 138 студентов разных специальностей и представлявших разные курсы обучения, 50% составили студенты, обучающиеся по оптическим специальностям. Впоследствии при обработке ответов студентов на вопросы анкеты был проведен сравнительный анализ ответов студентов, обучающихся по оптическим специальностям и студентов разных факультетов университета. Результаты анализа приведены в табл. 2.

	Студенты оптических специальностей	Студенты университета других специальностей
Нуждаетесь ли вы в помощи при поиске желаемой работы: Да Нет	100%	86,8% 13,16%
Хотели бы работать по специальности: Да Нет Не знаю Все зависит от конкретного места работы	94,7% 5,3%	89,5% 2,6% 2,6% 2,6%
Работаю: Не работаю: Ищу работу: Ищу производственную практику: Учусь, поэтому не работаю	21% 73,7% 47,4% 5,3% 42,1%	23,7% 23,7% 71% 2,6%
Приоритеты: 1) зарплата 2) работа по специальности 3) работа по интересам 4) рядом с домом 5) возможность частичной занятости 6) возможность совмещения с учебой	 26,3% 10,5% 36,8% 15,8% 10,5% 31,6%	 31,5% 13,2% 42% 18, 4% 13,2% 31,6%

Таблица 2. Сравнительная таблица ответов студентов всех курсов, обучающихся по оптическим специальностям и студентов университета, обучающихся по остальным специальностям

Результаты опроса показали, что в течение 2-х лет изменились представления студентов ФОИСТа о размере заработной платы, и условиях труда, а также требованиях работодателей, в конечном итоге, они стали более приближенными к действительности. Увеличилось количество студентов, желающих совмещать работу с учебой. Количество студентов, получивших опыт трудоустройства, увеличилось на 2,5% при этом количество студентов, не имеющих подобного опыта, сократилось на 2,7%.

Также за два года увеличилось число студентов ФОИСТ, проявивших желание не только работать по специальности, но и заниматься научной деятельностью в рамках получаемой профессии.

Результаты проведенного исследования коррелируются с результатами, представленными в работе [1]. Действительно, как показали результаты исследования, большинство студентов 4 курса имеет профессиональную мотивацию, в равных пропорциях, как внутреннюю, так и внешнюю [10]. Это позволяет надеяться на искреннее желание выпускников факультета реализоваться на профессиональном поприще. При проведении мероприятий на факультете значительно возросла активность студентов. Как результат, в 2008 году по инициативе студентов ФОИСТ был создан при Студсовете факультета комитет по содействию в трудоустройстве, пока единственный в СПбГУ ИТМО.

Разработана программа работы со студентами на 2008–2009 год, которая в настоящее время реализуется.

Заключение

Известно, что большинство абитуриентов, поступающих в университет, руководствуются такими критериями как близость к дому, желание родителей и т.д. Возможно, целенаправленная деятельность университетов по знакомству студентов с предприятиями, на которых они могут работать приведет к тому, что число выпускников будет искать работу по специальности. Тем более по таким специальностям, которые с полным правом можно назвать уникальными. Во всяком случае, проведенное исследование выявило интерес со стороны студентов к получаемой ими специальности.

Смоделированное мероприятие «Знакомство с будущим работодателем» является мероприятием факультетского уровня, идентичные мероприятия можно проводить на любом отдельном факультете, что не противоречит проведению «Ярмарок вакансий» на университетском уровне. Также вышеуказанное мероприятие может служить моделью для проведения тематических «Ярмарок вакансий».

Литература

1. Малинаускас Р.К. Мотивация студентов разных периодов обучения // Социологические исследования. – 2005 г. – № 2. – С. 134–138.
2. Багдасарьян Н.Г., Немцов А.А., Кансузян Л.В. Послевузовские ожидания студенческой молодежи // Социологические исследования. – 2003. – № 2.
3. Виштак О.В. Мотивационные предпочтения абитуриентов и студентов // Социологические исследования. – 2003. – № 2.
4. Попов В.А., Кондратьева О.Ю. Изменение мотивационно-ценностных ориентаций учащейся молодежи // Социологические исследования. – 1999. – № 6.
5. Щенникова Л.С. Духовные ориентиры псковских студентов // Социологические исследования. – 1999. – № 8.
6. Антипова В.М. Формирование мотивов учебной деятельности студентов в условиях учебно-научного комплекса вуза // Проблемы оптимизации учебного процесса в вузе. Ростов-на-Дону; Изд-во Рост, ун-та, 1981.
7. Вербицкий А.А., Бакшаева Н.А. Развитие мотивации в контекстном обучении // Вестник высшей школы. – 1998. – № 1.
8. Вербицкий А.А., Кругликов В. Контекстное обучение: формирование мотивации // Высшее образование в России. – 1998. – № 1.
9. Божович Л.И. Проблема развития мотивационной сферы ребенка // Изучение мотивации поведения детей и подростков. – М. Педагогика, 1972. С. 41–42.
10. Рогов М.Г. Мотивация учебной и коммерческой деятельности студентов // Высшее образование в России. – 1998. – № 4.

УДК 004.9

СИНТЕЗ УЧЕБНЫХ ПЛАНОВ НА ОСНОВЕ КОМПЕТЕНТНОСТНОЙ МОДЕЛИ ВЫПУСКНИКА

М.В. Плешкова
Научный руководитель – к.т.н., доцент А.В. Лямин

Настоящая статья описывает синтез учебных планов на основе компетеностной модели выпускника в информационно-образовательной среде AcademicNT. Представлено описание компетентностной модели выпускника. Рассмотрено построение модели результата обучения в виде план-графа.
Ключевые слова: компетенция, образование, результат обучения, программа

Введение

В последнее десятилетие и особенно после публикации текста «Стратегии модернизации содержания общего образования» и «Концепции модернизации российского образования на период до 2010 года» в России происходит резкая переориентация оценки результата образования с понятий «подготовленность», «образованность», «общая культура», «воспитанность», на понятия «компетенция», «компетентность» обучающихся. Т.е. делается существенная ставка на компетентностный подход в образовании [1, 2].

Краеугольным понятием компетентностного подхода являются понятия результата обучения (РО) и компетенции [3]. РО являются отображением образовательных возможностей преподавателей, но принципиально по-новому – с точки зрения ожиданий обучаемого: что он будет знать и уметь делать в конце обучения. Ожидания обучаемого можно выразить, прежде всего, с помощью компетенций. Компетенции описывают ту или иную деятельность специалиста, освоение которой является целью обучения. Поэтому компетенции являются самым важным, определяющим идентификатором РО.

Компетентностная модель выпускника

Компетенция – динамичная совокупность знаний, умений, навыков, способностей и ценностей, необходимая для эффективной профессиональной и социальной деятельности и личностного развития выпускников; компетенцию они обязаны освоить в процессе подготовки и продемонстрировать после завершения части или всей образовательной программы [4].

Компетенция выпускника, определяющая отдельную задачу по его подготовки, имеет следующий вид:

КОМПЕТЕНЦИЯ: = <деятельность> <объект деятельности>

Понятие <деятельность> задается глагольной группой (проектировать, планировать и т.п.), а <объект деятельности> – именной (типовые изделия и узлы, размещение технологического оборудования и т.п.).

Компетентностная модель (КМ) выпускника представляет собой совокупность учебно-методической документации, регламентирующей цели и задачи, а также ожидаемые результаты их подготовки. КМ выпускника является мощным инструментом для управления отбором в избыточном образовательном пространстве компетентностно-ориентированного содержания образования, реализация которого в целостном образовательном процессе будет необходимой и достаточной для подготовки конкурентоспособного выпускника, востребованного рынком труда.

Ожидаемый результат подготовки – это пороговый (минимальный, необходимый) уровень академической и профессиональной подготовленности, который, как ожидается, должен быть достигнут выпускниками после завершения основной образо-

вательной программы. Ожидаемый результат подготовки в КМ выпускника описывается с помощью двух групп компетенций выпускника – универсальных и профессиональных.

Универсальные компетенции выпускника инвариантны к видам профессиональной деятельности, т.е. являются надпрофессиональными. В группе универсальных компетенций выделены три подгруппы: *социально-личностные*, *общенаучные* и *инструментальные* компетенции выпускника. Социально-личностные компетенции формируют в процессе подготовки такие важные качества у выпускников как целеустремленность, организованность, трудолюбие, ответственность, гражданственность, коммуникативность, толерантность, повышение общей культуры и т.п. Общенаучные компетенции формируют в процессе подготовки понимание роли науки в развитии цивилизации, основных философских учений и теорий, сущности государства и права, владение общей методологией научного познания, готовность применять фундаментальные знания по естественно-научным направлениям подготовки (физике, математике, информатике и др.) и т.п. Инструментальные компетенции формируют в процессе подготовки базовые навыки принятия решений в сфере техники и технологий, владение современными информационными и коммуникационными технологиями, владение иностранными языками и т.п. Универсальные компетенции во многом определяются требованиями ФГОС к уровню подготовленности выпускника данного направления и уровня образования (бакалавр, магистр, специалист).

Профессиональные (специальные) *компетенции выпускника* описывают совокупность основных типичных черт какой-либо профессии, определяющих конкретную направленность ООП ВПО, ее содержания. Профессиональные компетенции выпускника разрабатываются на основе вышеизложенного подхода. Перечень профессиональных компетенций структурируется в соответствии с теми основными видами профессиональной деятельности, к которым должен быть подготовлен выпускник, например: *научно-исследовательские*, *проектные*, *производственно-технологические* и *организационно-управленческие* компетенции. Самой подвижной частью КМ выпускника являются его профессиональные компетенции, т.к. они определяют профиль подготовки выпускника и являются во многом оригинальными (иначе не было деления на направления и специализации).

Синтез учебных планов

Компетентностный подход к образованию принципиальным образом меняет структурирование образовательного пространства. Теперь не содержание, а результаты образования и их идентификаторы должны определять структуру и состав образовательных модулей для компетентностного обучения и аттестаций. Идентификаторы ожидаемого РО, в свою очередь, определяют отбор образовательных модулей для подготовки специалистов, а учебно-методический комплекс (УМК), синтезированный из таких модулей, должен обеспечивать освоение компетенций ожидаемого РО в объеме, необходимом и достаточном для требуемого уровня компетентности, уровня и профиля образования. Виды и характеристики учебной нагрузки модулей УМК будут также идентифицировать ожидаемый РО.

Электронный учебно-методический комплекс имеет иерархический, модульный характер. Верхнюю ступень в структуре УМК занимает учебный план подготовки учащегося по определенной специальности. Система авторизации обеспечивает доступ каждого пользователя к соответствующему учебному плану. Рабочие программы дисциплин, определенных учебным планом, составляют второй уровень.

Каждая дисциплина может включать несколько семестровых электронных курсов. Каждый электронный курс, в свою очередь, состоит из ряда аттестующих, обучающих

и информационных модулей, позволяющих реализовывать все виды учебной работы. В системе определены следующие виды электронных модулей:

- электронные конспекты;
- информационные ресурсы;
- электронные тесты;
- виртуальные лабораторные работы;
- электронные практикумы.

Учебная программа как перечень дидактических единиц определяется результатами разработки ее компетентностной модели. Компетентностная модель учебной программы задает причинно-следственные связи между ключевыми знаниями и умениями программы и определяет не только структуру УМК данного модуля, но и порядок (сценарий) его изучения и аттестаций освоенных компетенций.

Для построения траектории образовательного процесса по достижению ожидаемого РО определим дискретное пространство Q на множестве таких состояний компетенций $X = \{x_0, x_1, \ldots, x_n\}$, каждый элемент которого x_i характеризуется уникальным набором знаний и умений. Процесс подготовки специалиста рассматривается в пространстве формирования компетентности Q как процесс перехода от одного состояния к другому (рис. 1). Отношение непосредственной вложенности компетенций РО, установленной в ходе детализации некоторой исходной компетенции РО, а также дальнейшая декомпозиция РО, соответствующих освоению элементарных компетенций, по уровням компетентности, профилям и уровням образования в соответствии со структурой предмета данной элементарной компетенции определяет модель иерархии РО в виде корневого дерева, где Y_0 – корень дерева, моделирующий совокупный РО всего образовательного пространства; $Y_1, Y_2, \ldots, Y_n$ – подмножества вершин, моделирующих РО, полученные при декомпозиции РО. Таким образом, модель РО в виде план-графа отражает иерархию РО и устанавливает причинно-следственные связи между их состояниями компетентности в дискретном пространстве Q, что позволяет использовать эту модель для проектирования различных образовательных траекторий по подготовке компетентных специалистов.

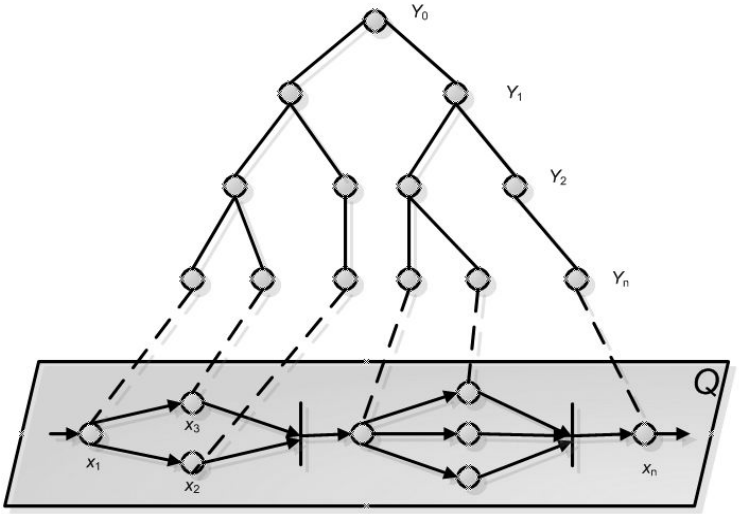


Рис. 1. Иерархия результатов обучения и их связь с состояниями компетентности

Образовательный модуль для освоения элементарных компетенций должен иметь модульную структуру и состоять из таких базовых образовательных модулей (БОМ), каждый из которых обеспечивает при изучении глав, разделов и т.д. предмета приращение компетентности у обучаемого, определяемое на основе требований, предъявляемых к уровням компетентности, профилям и уровням образования (рис. 2). Причем каждый БОМ характеризуется трудоемкостью.

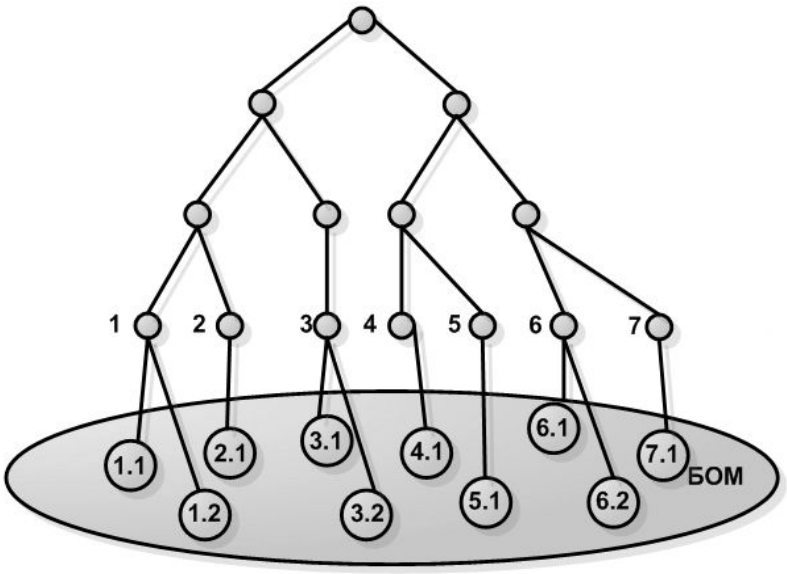


Рис. 2. Связь элементарных компетенций с базовыми образовательными модулями

Таким образом, взаимнооднозначное соответствие элементарных РО и БОМ в пространстве Q позволяет рассматривать процесс формирования компетентности обучаемого, с одной стороны, как процесс планирования ожидаемого РО на основе элементарных РО и, с другой стороны, как процесс синтеза модульного электронного УМК на основе БОМ, как показано на рис. 3. Ключевым понятием для такого соответствия является понятие план-графа.

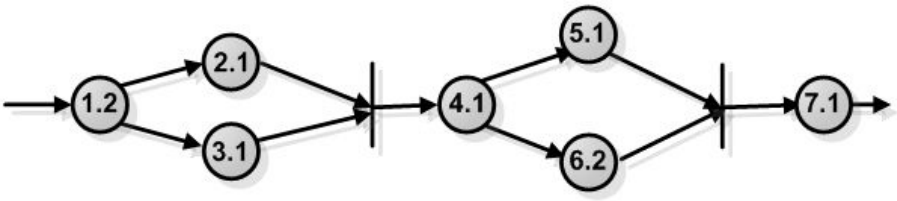


Рис. 3. План-граф

Проектирование образовательных траекторий по план-графу имеет неоспоримое преимущество, так как требует от разработчиков РО только идентификации исходного и ожидаемого РО в виде состояний компетентности исходной и целевой компетентности соответственно; промежуточные состояния устанавливаются автоматически по план-графу в процессе проектирования этой траектории.

В информационно-образовательной среде AcademicNT существует возможность создания и редактирования компетентностных моделей. На рис. 4 представлен список элементарных компетенций. При изменении компетенции история изменений сохраняется, измененные компетенции помечаются значком H. При редактирования элементарной компетенции указываются уровень компетенции, связь с исходной компетенцией, а так же список содержательных компетенций. Если в процессе работы были внесены изменения, то система сообщает о них.

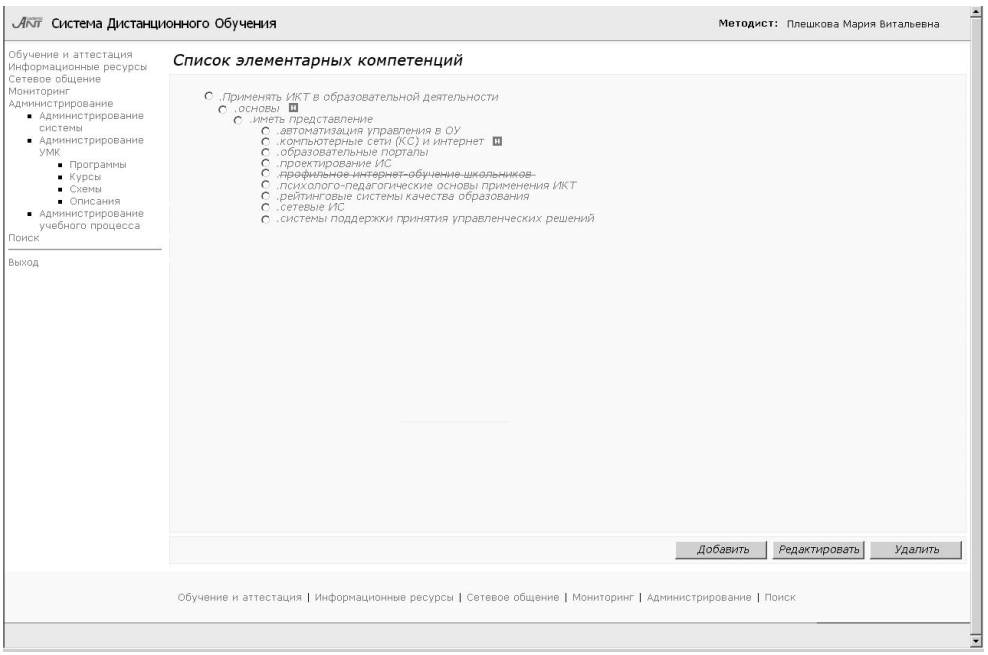


Рис. 4. Список элементарных компетенций

Содержательные компетенции выпускника являются выражением мнения о том, каким образом (способом) следует решать поставленную задачу подготовки, чтобы достичь запланированные элементарные РО. В содержательной компетенции (рис. 5) указываются название и индекс, владельцы и разработчики учебных материалов. Так же заполняется перечень ЗУНов: вносятся значения в поля «Знать», «Понимать», «Иметь навык».

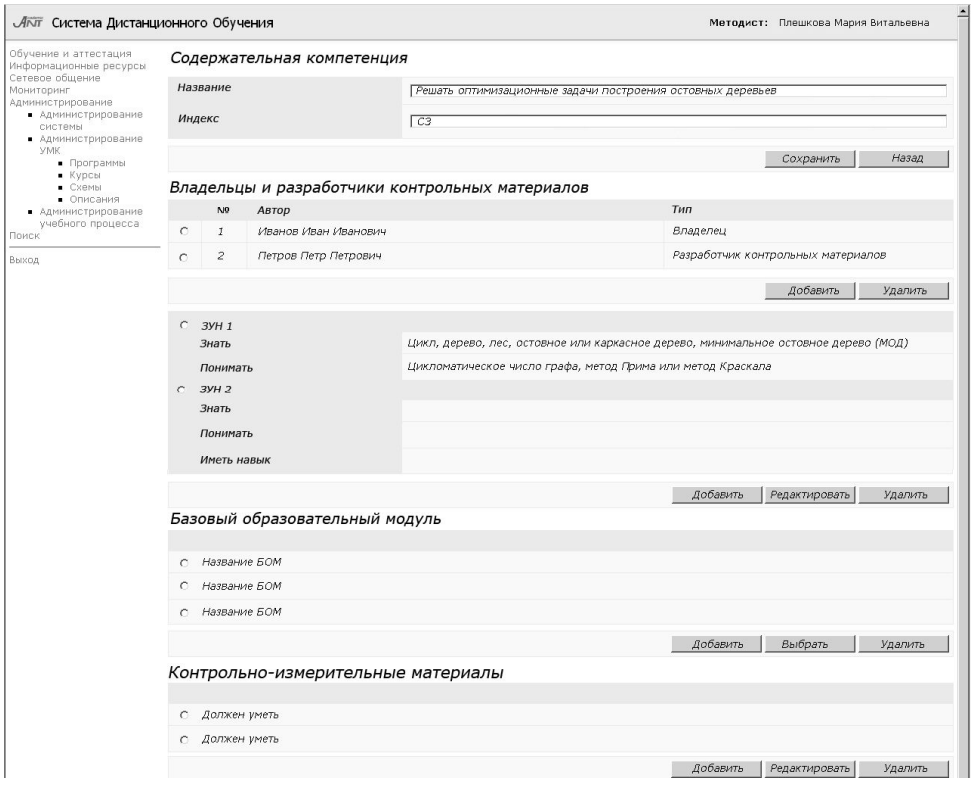


Рис. 5. Содержательная компетенция

При выборе БОМ в списке переходит к обзору его УМК. В следующем окне будут отображены паспорт и учебная программа выбранного БОМ. Отображаемая информация содержит также часть информации из паспорта его образовательных моду-

лей. БОМ ставит ссылки на узлы графа и выбирает оптимальную траекторию по трудоемкости.

Таким образом, при изменении модуля происходит изменении в содержании дисциплины, а соответственно в учебном плане.

Отбор образовательных модулей в системе AcademicNT, состав которых обеспечивает необходимое и достаточное содержание обучения для достижения ожидаемого РО, является целью реализации компетентностного подхода к обучению. При этом учебный план, а соответственно и траектория образовательного процесса, определяется результатами разработки РО.

Заключение

Переход к компетентностному подходу при разработке государственных образовательных стандартов высшего профессионального образования является своевременным и необходимым, так как интегральная оценка качества подготовки выпускника может быть наиболее полно получена только при определении его компетентности в выбранной области профессиональной деятельности.

Учебный план подготовки учащегося моделируется и проектируется по план-графу, для построения и модификации которого в информационно-образовательной среде AcademicNT имеются специальные средства автоматизации.

Литература

1. Стратегия модернизации содержания общего образования. Материалы для разработки документов по обновлению общего образования. – М. – 2001. – 34 с.
2. Концепция модернизации российского образования на период до 2010 года. – М. – 2002.
3. Лисицына Л.С. Теория и практика компетентностного обучения и аттестаций на основе сетевых информационных систем. – СПб: СПбГУ ИТМО. – 2006. – 147 с.
4. Лисицына Л.С. Средства и технологии для управления самостоятельной работой студентов. Методическое пособие. – СПб: СПбГУ ИТМО. – 2008. – 53 с.

УДК 551.46:004.4

КОНЦЕПЦИЯ СЕРВИС-ОРИЕНТИРОВАННОЙ ИНФРАСТРУКТУРЫ ЕДИНОЙ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ИНФОРМАЦИИ ОБ ОБСТАНОВКЕ В МИРОВОМ ОКЕАНЕ

К.В. Белова
(Всероссийский научно-исследовательский институт гидрометеорологической информации – мировой центр данных)
Научный руководитель – к.ф.-м.н. А.А. Воронцов
(Всероссийский научно-исследовательский институт гидрометеорологической информации – мировой центр данных)

В работе описываются предварительные решения по построению сервис – ориентированной инфраструктуры (СОИ) единой государственной системы информации об обстановке в Мировом океане (ЕСИМО). Приведен краткий обзор существующих реализаций в области применения сервис-ориентированной архитектуры в качестве технологии организации распределенных систем. Дано краткое описание обобщенной (ссылочной) модели ЕСИМО в условиях использования СОИ. Рассмотрены методы и средства СОИ ЕСИМО, при использовании которых осуществляется взаимодействие компонент ЕСИМО.

Ключевые слова: сервис-ориентированная инфраструктура, ЕСИМО, сервисная шина, интерфейсное взаимодействие

Введение

Для принятия обоснованных стратегических и оперативных решений по вопросам морской деятельности необходима полная и своевременно доставленная комплексная информация об обстановке в Мировом океане – гидрометеорологические условия, размещение судов и объемы морских перевозок, портовая деятельность, добыча биологических и нефтегазовых ресурсах, экологические условия и т.п.

Для эффективного решения этой задачи в рамках федеральной целевой программы «Мировой океан» создается Единая Государственная Система Информации об обстановке в Мировом океане (далее, ЕСИМО). В основу ЕСИМО [1] заложена идея создания единого распределенного информационного пространства в области обстановки в Мировом океане. Предметом ЕСИМО являются массивы, базы данных, программные приложения, содержащие и (или) создающие данные и информацию (далее информационные ресурсы) о морской среде и морской деятельности. Модель ЕСИМО основана на принципиальном условии – ЕСИМО реализуется на основе существующих ведомственных информационных систем без перестройки их внутренней организационной структуры, информационных технологий, баз данных и других составных частей.

В настоящее время в ЕСИМО разработана и внедрена технология, интегрирующая распределенные информационные ресурсы в области морской среды и морской деятельности в виде системы распределенных баз данных (СРБД) ЕСИМО. В контексте ЕСИМО под термином «распределенные базы данных» понимается как файловые системы фактографических, структурированных, пространственных данных, электронных документов, так и базы данных.

В течение последних нескольких лет значительный интерес вызывает новый подход к построению информационных систем – сервис-ориентированная архитектура (СОА), основанный на использовании сервисов (служб) со стандартизованными интерфейсами. В рамках развития ЕСИМО и построения полнофункциональной

системы предусматривается разработка инфраструктуры ЕСИМО, основанной на принципах и решениях СОА, называемая сервис – ориентированной инфраструктурой ЕСИМО (СОИ ЕСИМО).

Краткий обзор существующих реализаций

Сервис-ориентированная архитектура – подход к разработке программного обеспечения, основанный на использовании сервисов (служб) со стандартизованными интерфейсами. Компоненты системы могут быть распределены по разным узлам сети, и предлагаются как независимые, слабо связанные, заменяемые сервис – приложения [2].

В настоящее время СОА получает все большее распространение во многих областях индустрии информационных технологий. Такая проблема как, разрозненность различных наборов данных в рамках задачи интеграции информационных ресурсов потребовала унификации используемых стандартов и формирования распределенной информационной среды.

В рассматриваемой предметной области примером существующей реализации инфраструктуры, основанной на принципах и подходах СОА, является концепция SDI [3] (Spatial Data Infrastructure) – инфраструктура пространственных данных. Основными задачами развития данной концепции являются: построение глобальной инфраструктуры информационных технологий и геоданных; гармонизация спутниковой информации; использование согласованного набора стандартов, понятных всем участникам данной системы; интероперабельность между независимо созданными приложениями и совмещение их интерфейсов и форматов данных; поддержка единой политики доступа к данным. Одной из реализации концепции SDI является проект США NSDI[4] (National Spatial Data Infrastructure) – национальная инфраструктура пространственных данных. Основными целями данной программы являются: совершенствование механизма доступа к данным путем организации центров информационного обмена и создания баз метаданных; создание баз пространственных данных; создание тематических данных, критически важных для государства; координация сбора и использования пространственных данных.

В Европе реализацией SDI является проект INSPIRE[5] (Infrastructure for Spatial Information in Europe) – Глобальной геоинформационной инфраструктуры данных в Европе. Разработан геопортал INSPIRE, основной целью которого является создание основы единой Европейской инфраструктуры пространственных данных, формируемой за счет интеграции пространственной информации и сервисов с использованием единых стандартов и протоколов обмена данными. Проекты, аналогичные NSDI и INSPIRE, были созданы в ряде таких стран как Китай (Geospatial Data Infrastructure), Канада (Canadian Geospatial Data Infrastructure), Испания (Spanish National Spatial Data Infrastructure), Индия (Indian National Spatial Data Infrastructure).

Попыткой создания инфраструктуры, объединяющей организации стран Европы в единую информационную сеть, где каждый поставщик услуг равноправен, является система SSE [6] (Service Support Environment) – среда поддержки сервисов. Основу среды составляют сервисы, которые базируются на технологии web – сервисов [7]. Целью создания SSE является реализация открытой сервис - ориентированной распределённой среды между потребителями и поставщиками информации, позволяющей интегрировать данные наблюдения за Землёй, метеорологические данные и данные геоинформационных систем.

В качестве единых стандартов и протоколов обмена данными в приведенных реализациях концепции СОА предпочтение отдается таким стандартам как ISO [8] (International Organization for Standardization) – международная организация по стандартизации, OGC [9] (Open Geospatial Consortium) – Открытый

геопространственный консорциум, W3C[10] (World Wide Web Consortium) – Консорциум Всемирной паутины.

Применение сервис-ориентированного подхода при построении полнофункциональной ЕСИМО позволит как предоставить различным пользователям доступ к данным по морской природной среде и морской деятельности, так и организовать удалённый вызов методов их обработки, функционирующих на стороне поставщика данных. Ориентация на сервисы позволит предоставлять пользователям механизмы обработки данных, в то время как технически детали обработки и логика алгоритмов будут скрыты.

Ссылочная модель ЕСИМО

Инфраструктура проекта ЕСИМО, построенная по принципам сервис-ориентированной архитектуры, представляет собой совокупность функциональных подсистем, информационных ресурсов, технологий, которые взаимодействуют через телекоммуникационные средства на основе технических спецификаций и электронных web-сервисов, где web-сервис представляет собой стандартизированное программное приложение, к которому можно удаленно обратиться посредством компьютерной сети, и предоставляющее некоторые функциональные возможности запрашивающей стороне. Ниже дано краткое описание модели полнофункциональной ЕСИМО на основе методов и средств СОИ.

Модель полнофункциональной ЕСИМО построена на основе RM-ODP [11] (Reference Model of Open Distributed Processing) – Эталонная модель для открытой распределенной обработки, определяющей общую концептуальную основу для построения распределенных систем данных и обработки данных. RM-ODP определяет пять стандартных представлений описывающих различные аспекты распределенной системы. Представления ЕСИМО в условиях применения СОИ представлены ниже:

– функциональное (или корпоративное). Является обобщенным представлением СОИ ЕСИМО, в котором основное внимание уделяется целям и задачам СОИ, масштабам и схемам применения;

– информационное. Характеризует семантику информации и данных, обрабатываемых с помощью СОИ ЕСИМО;

– вычислительное. Представляет собой функциональную декомпозицию ЕСИМО на объекты, которые будут взаимодействовать с помощью интерфейсов;

– проектное. В данном представлении определяются типы компонентов ЕСИМО и предварительные технические требования для поддержки распределенного взаимодействия между компонентами;

– технологическое. Сконцентрировано на выборе информационных технологий реализации полнофункциональной ЕСИМО с применением СОИ.

На рис. 1 представлена структура ЕСИМО с применением методов и средств СОИ.

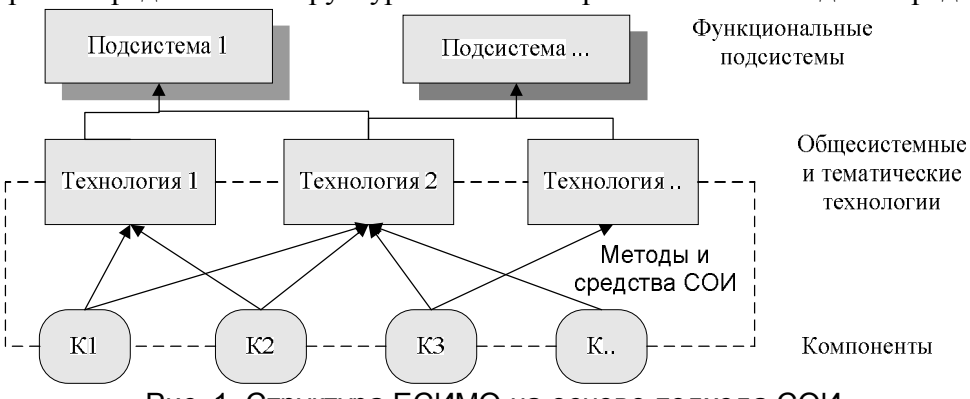


Рис. 1. Структура ЕСИМО на основе подхода СОИ

Компонент представляет собой IP-адресуемый комплекс средств (программный комплекс, измерительный комплекс, база данных и др.), осуществляющий определенный процесс обработки данных и характеризуемый входными данными, бизнес-логикой и выходными данными. Взаимодействуя между собой с помощью методов и средств СОИ, компоненты составляют технологии, на которых в свою очередь основываются функциональные подсистемы.

Выделяются тематические информационные технологии и общесистемные технологии информационного взаимодействия. Тематические информационные технологии обеспечивают формирование информационных ресурсов центрами системы на основе взаимодействия с системами наблюдений, источниками данных и другими ресурсами ведомственных информационных систем. В целом функционирование первой очереди ЕСИМО осуществляется с применением 87 тематических технологий. Информационное взаимодействие баз данных, создаваемых центрами на основе тематических информационных технологий, осуществляется с применением общесистемных технологий. К ним относятся: технология виртуальной телекоммуникационной сети; технология ведения централизованной базы метаданных и мониторинга информационной деятельности; технология ведения общих классификаторов и кодов; технология интеграции информационных ресурсов.

Методы и средства СОИ ЕСИМО

Каждая из технологий может основываться на компонентах любой другой технологии, а новые технологии могут создаваться путем комбинации уже существующих компонент. Такая информационная и программная взаимосовместимость достигается за счет применения технических спецификаций и специализированного программного обеспечения – сервисной шины.

Компоненты взаимодействуют между собой не напрямую, а через программные средства, предоставляемые сервисной шиной, и по законам и правилам, отраженных в технических спецификациях. Такое взаимодействие через шину-посредника дает возможность избавиться от огромного числа прямых соединений приложений между собой. Вместо интеграции каждого компонента с каждым обеспечивается возможность подключения компонентов к единой сервисной шине, которая обеспечивает регистрацию и нахождение компонентов. Компоненты подключаются к общей шине через стандартные соединения. Одним из стандартов взаимодействия являются web-сервисы. Несмотря на то, что web-сервисы являются неотъемлемой частью сервисной шины, интеграция уже имеющихся или предполагаемых к приобретению приложений необязательно должна подразумевать их перекодировку в web-сервисы – при интеграции старых приложений происходит «обертывание» приложений в web-сервисы [12].

Основными функциями шины являются:

- обеспечение уникальной идентификации компонент;
- вызов компонент;
- обнаружение компонент;
- обеспечение доступа к реестру сервисов и компонентов;
- обеспечение доступа к словарю операций сервисов;
- обеспечение доступа к каталогу сценариев;
- мониторинг работы с компонентами.

Сервисная шина состоит из трех основным элементов: реестра компонент, словаря операций и блока управлением процессами.

Реестр компонент представляет собой набор подробных описаний компонент. От полноты и четкости представленной в реестре информации о компоненте зависит его потребляемость другими приложениями. Реестр должен быть доступен через сеть,

должен хранить информацию о поставщике компонента, информацию о самом компоненте с описанием его функций, входных и выходных данных, интерфейсное описание (например, на языке WSDL [13] (Web Services Description Language) – язык описания web-сервисов). Также реестр должен обеспечивать регистрацию новых компонент и предоставлять механизмы поиска существующих компонент и их функций.

Словарь операций содержит четко установленные, стандартные для всех компонентов названия функций компонентов, которые используются в рамках системы. Компоненты при взаимодействии не знают о существовании друг друга, единственное, что им известно – название функции из Словаря операций, которую они запрашивают. Специализированные механизмы шины, разработанные для взаимодействия со Словарем операций, перенаправляют запрос нужному компоненту, ориентируясь по заданному названию функции. Таким образом, изменение названия одного из взаимодействующих компонентов или его операций, замена одного компонента другим, смена местоположения вызываемого компонента не влияет на остальные взаимодействующие с ним компоненты. Все необходимые изменения происходят в сервисной шине, не затрагивая при этом связанные компоненты. Словарь операций должен быть доступен через сеть, должен содержать механизмы поиска и предоставления описаний, содержащихся в нем операций, также должен иметь жесткую связь с реестром компонент.

Блок управления процессами, взаимодействуя с реестром компонент и словарем операций, содержит механизмы вызовов компонент и механизмы составления бизнес-процессов из нескольких компонент [14]. Такой составной бизнес-процесс в конечном итоге предоставляется как стандартный компонент СОИ ЕСИМО.

Для обеспечения единого интерфейсного взаимодействия компонент между собой необходимо разработать следующие технические спецификации: спецификация на создание и выделение компонент и сервисов; техническая спецификация взаимодействия с шиной; техническая спецификация на разработку web-сервисов.

Спецификация на создание и выделение компонент и сервисов должна содержать правила, устанавливающие процесс внедрения компонента в СОИ ЕСИМО. При внедрении компонента в СОИ ЕСИМО сначала определяется задача, решаемая этим компонентом, реестр компонент и сервисов проверяется на наличие компонент, решающих данную задачу. Компоненты с одинаковыми функциями не должны существовать в системе, т.к. одним из принципов построения инфраструктуры на основе подходов СОА является повторное использование компонент. Далее происходит проверка интерфейсов компонентов на их соответствие техническим спецификациям взаимодействия с шиной и разработку web-сервисов. Если компонент удовлетворяет всем пунктам данных спецификаций, то происходит его регистрация в реестре компонент и сервисов, что делает его доступным для использования другими компонентами, входящими в состав СОИ ЕСИМО.

Техническая спецификация взаимодействия с шиной содержит основные требования, предъявляемые к протоколу взаимодействия, к типам операций компонент и к форматам входных/выходных сообщений, которыми обмениваются компоненты при взаимодействии. Заранее известные, установленные форматы операций и входных/выходных сообщений позволят максимально автоматизировать взаимодействие компонент между собой.

Заключение

Построение сервис-ориентированной инфраструктуры ЕСИМО позволит упростить интеграцию приложений в единую систему, обеспечит прозрачное информационное взаимодействие с другими системами.

Построение инфраструктуры ЕСИМО по принципам сервис-ориентированной архитектуры позволит сделать все компоненты системы независимыми друг от друга. Исключение одних компонент из системы и добавление новых не будет влиять на работу системы в целом, сделает ее более масштабируемой, гибкой и готовой к постоянным изменениям.

Методы и средства СОИ ЕСИМО представляют собой совокупность технических спецификаций и программного обеспечения и предоставляют компонентам возможность единообразного унифицированного взаимодействия между собой. Реестр компонент позволит получать быстрое и полное описание созданных компонент и выполняемых ими функций, а блок управления процессами позволит составлять новые компоненты из уже существующих.

Литература

1. Единая система информации об обстановке в Мировом океане (ЕСИМО). [Электронный ресурс]. – Режим доступа: http://www.oceaninfo.ru/, свободный.
2. Богданов А.В., Станкова Е.Н., Мареев В.В. Сервис-ориентированная архитектура: новые возможности в свете Grid технологий [Электронный ресурс]. – Режим доступа: http://window.edu.ru/window_catalog/pdf2txt?p_id=27125, свободный.
3. Spatial Data Infrastructure (SDI). [Электронный ресурс]. – Режим доступа: http://www.gsdi.org/, свободный.
4. National Spatial Data Infrastructure (NSDI). [Электронный ресурс]. – Режим доступа: http://www.fgdc.gov/nsdi/nsdi.html, свободный.
5. Infrastructure for Spatial Information in Europe (INSPIRE). [Электронный ресурс]. – Режим доступа: http://inspire.jrc.ec.europa.eu/, свободный.
6. Service Support Environment (SSE). [Электронный ресурс]. – Режим доступа: http://services.eoportal.org/, свободный.
7. Эрик Ньюкомер. Веб-сервисы: XML, WSDL, SOAP and UDDI. – Питер. – 2003. – 256 с.
8. International Organization for Standardization (ISO). [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/home.htm, свободный.
9. Open Geospatial Consortium (OGC). [Электронный ресурс]. – Режим доступа: http://www.opengeospatial.org/, свободный.
10. World Wide Web Consortium (W3C). [Электронный ресурс]. – Режим доступа: http://www.w3.org/, свободный.
11. Reference Model of Open Distributed Processing (RM-ODP). [Электронный ресурс]. – Режим доступа: http://www.rm-odp.net/, свободный.
12. Шаблоны проектирования. Новый подход к объектно-ориентированному анализу и проектированию: Пер. с англ. – М.: Издательский дом «Вильямс». – 2002. – 288 с.
13. Web Services Description Language (WSDL). [Электронный ресурс]. – Режим доступа: http://www.w3.org/TR/wsdl, свободный.
14. Робинсон Р. Функции Enterprise Service Bus [Электронный ресурс]. – Режим доступа: http://www.ibm.com/developerworks/ru/library/ws-esbscen/index.html, свободный.

УДК 004.434:004.4'232

ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ КЛИЕНТСКОЙ ЧАСТИ ВИРТУАЛЬНОЙ ЛАБОРАТОРИИ ПО СОЗДАНИЮ МОДЕЛЕЙ СИСТЕМ МАССОВОГО ОБСЛУЖИВАНИЯ НА ЯЗЫКЕ GPSS

В.А. Асташкина
Научный руководитель – к.т.н., доцент А.В. Лямин

В статье представлены основные результаты работы над созданием клиентской части виртуальной лаборатории, предназначенной для построения и исследования моделей на языке GPSS; указаны особенности представления модели и процесса моделирования разработанным интерпретатором GPSS-программ, а также описан пользовательский интерфейс среды создания моделей.

Ключевые слова: имитационное моделирование, GPSS, виртуальная лаборатория

Введение

В настоящее время в рамках нескольких направлений подготовки в том или ином виде рассматриваются вопросы построения моделей систем массового обслуживания (СМО). Для описания имитационных моделей СМО существует специальный язык программирования – GPSS [1]. Однако, как показал анализ соответствующих сред создания моделей, на сегодняшний день отсутствует инструмент, позволяющий подготовить специалистов, владеющих приемами построения моделей на языке GPSS. Из рассмотренных сред следует отметить GPSS World (разработка американской компании Minuteman Software) и WebGPSS (разработка Стокгольмской Высшей Школы Экономики).

GPSS World представляет собой среду, позволяющую создавать достаточно сложные модели и исследовать их. Однако это среда именно для профессиональной разработки, и, как следствие, при использовании ее в учебном процессе возникает ряд трудностей. В частности, отсутствуют такая важная возможность, как построение блок-диаграмм моделей. Нужно отметить, что в 2006 году прекращена поддержка и выпуск бесплатной студенческой версии GPSS World.

Среда WebGPSS создана специально для обучения студентов. Но она имеет очень узкие функциональные возможности, ее дизайн не отвечает требованиям эргономичности. Кроме того, приложение устарело (оно реализовано на языке программирования Java, но не работает с современными виртуальными машинами Java).

На основе информации, полученной при изучении аналогов, был сформулирован ряд требований к разрабатываемой среде моделирования, в частности:

- среда должна давать возможность построения блок-диаграмм моделей и написания программ на языке GPSS;
- во время прогона модели автоматически должна собираться статистическая информация, а по его окончании должен формироваться отчет;
- среда должна предоставлять возможность построения графиков по результатам прогона модели.

Интерпретатор языка GPSS

Основу клиентской части виртуальной лаборатории составляет интерпретатор GPSS-программ. Согласно описаниям языка, приведенным в [2–5] были разработаны алгоритмы функционирования интерпретатора GPSS.

GPSS – это язык декларативного типа, построенный по принципу объектно-ориентированного языка. Основными элементами этого языка являются транзакты и блоки, которые отображают соответственно динамические и статические объекты моделируемой системы [3]. Программа на языке GPSS записывается как последователь-

ность операторов. Операторы бывают двух видов – команды и блоки GPSS. Для каждого оператора отводится ровно одна строка (за исключением команды FUNCTION). У операторов может присутствовать один или несколько операндов различных типов.

Наиболее оптимальный способ реализации интерпретатора предполагает использование объектно-ориентированного подхода:

– модель в терминах языка GPSS представляет собой совокупность взаимодействующих объектов (статических и динамических);
– статическая структура модели – это набор объектов-блоков;
– динамические элементы – объекты, хранящие информацию о своем состоянии;
– посредством динамических объектов изменяются состояния статических элементов модели;
– статистическая информация сохраняется статическими объектами модели.

Интерпретатор состоит из двух основных частей – первая предназначена для разбора GPSS-программы, вторая – для ее выполнения.

Особенности разбора GPSS-программы

Разбор GPSS-программы происходит по методу рекурсивного спуска. Для каждого оператора описан класс, содержащий методы его разбора. Среди особенностей модуля разбора следует отметить способ определения корректности операндов оператора GPSS.

Для каждого операнда в классе, предназначенном для разбора оператора, имеется список возможных типов данных, которые являются корректными. Сначала проверяется, имеет ли найденный операнд тип из этого списка. Если тип операнда является недопустимым, в список ошибок разбора добавляется информация об ошибке и происходит переход к разбору, следующего оператора GPSS. Если операнд имеет корректный тип, происходит обработка этого операнда в соответствии с его типом.

В зависимости от расположения и особенностей оператора операнд может быть:

– обязательным или необязательным;
– единственным, первым, последним, находящимся между первым и последним.

Для реализации методов разбора операндов были выявлены их общие черты и описаны методы, производящие разбор:

– необязательного первого операнда;
– необязательного последнего операнда;
– необязательного единственного операнда;
– необязательного операнда, находящегося между первым и последним операндами;
– обязательного единственного или последнего операнда;
– обязательного первого операнда или операнда, находящегося между первым и последним операндами оператора.

Таким образом, при разборе операторов выполняется следующая последовательность действий:

1) вызов метода разбора операнда в зависимости от его расположения и того, является ли этот он обязательным для данного блока или команды;
2) определение корректности типа данных операнда;
3) вызов метода обработки операнда в зависимости от его типа данных.

Объекты GPSS

Все объекты языка GPSS делятся на две категории: статические и динамические.

Под статическими объектами GPSS будем понимать блоки или низкоуровневые объекты. К низкоуровневым относятся объекты, с которыми пользователь не может работать непосредственно:

- очереди;
- устройства;
- накопители;
- логические ключи;
- генераторы случайных чисел и др.

Во время разбора GPSS-программы создаются списки блоков и команд модели.

Операторы блоков и команд имеют схожую структуру. Для их реализации были описаны родительские классы *Block* (для блоков) и *Command* (для команд), в которых определены методы, общие для операторов данного типа. К примеру, метод *run()* должен присутствовать в каждом операторе, поскольку именно этот метод отвечает за его функциональность. Метод вызывается интерпретатором для выполнения команды или реализации действий над транзактом в блоке и возвращает целое число, указывающее на успешность выполнения или возникшую ошибку.

Динамическими объектами являются транзакты (заявки). Объект «Транзакт» хранит информацию о своем состоянии: внутренний номер, семейство, список очередей, в которых он зарегистрирован, время входа в систему, список параметров и т.п. Важно, что транзакт также хранит номер блока, в котором он сейчас находится, и номер блока, в который он направится далее. Это позволяет не организовывать сложных для понимания и реализации схем передачи транзактов между блоками. Все блоки модели пронумерованы, и текущий активный транзакт передается блоку с нужным номером. Значения номеров блоков для транзакта определяются каждый раз при передаче этого транзакта блоку и зависят от типа текущего блока.

Выполнение GPSS-программы

Выполнение GPSS-программы происходит по следующей схеме. Последовательно выполняются все команды из списка команд. Для выполнения команды вызывается метод *run()* объекта, соответствующего команде. Команда START запускает процесс моделирования, тогда активируются методы *run()* блоков и начинается движение транзактов.

Механизм передачи транзактов между блоками основан на взаимодействии со списками событий. Основных списков два: список текущих событий (СТС) и список будущих событий (СБС). В СТС находятся транзакты, которые могут перемещаться между блоками в текущий момент времени. СБС содержит транзакты, которые ожидают наступления определенного времени моделирования. Когда нужный момента времени наступает, транзакты перемещаются из СБС в СТС. Транзакты перемещаются из одного списка в другой до тех пор, пока не будет выполнено условие прекращения процесса моделирования.

Процесс моделирования прекращается в следующих случаях:

- счетчик завершения процесса моделирования стал равным нулю или отрицательным;
- получена команда HALT;
- произошла ошибка выполнения;
- выполнено условие останова, определенное командой STOP.

На рис. 1 показана диаграмма классов, составляющих внутренне представление модели и реализующих процесс моделирования.

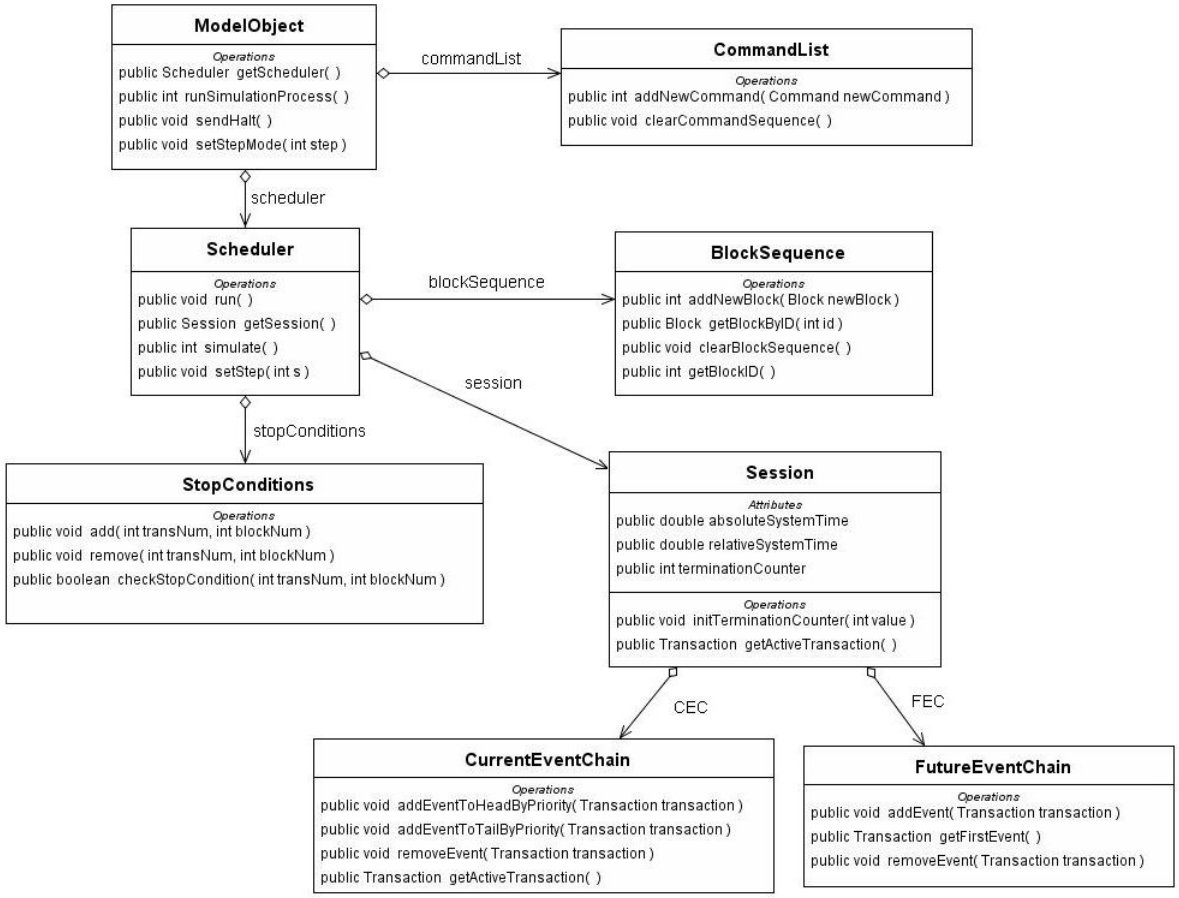


Рис. 1. Диаграмма классов, реализующих процесс моделирования

Объект класса *ModelObject* содержит планировщик (объект класса *Scheduler*) и список команд (объект класса *CommandList*) модели. В список команд попадают команды GPSS, найденные интерпретатором во время разбора программы либо переданные уже существующему объекту *ModelObject*. Каждая новая команда помещается в конец списка команд. Исключение составляют срочные команды (например, HALT), которые выполняются немедленно, минуя список команд.

Планировщик отвечает за непосредственную реализацию процесса моделирования. В его задачи входит:

- продвижение модельного времени;
- планирование наступления следующего события;
- проверка условий прекращения процесса моделирования;
- проверка успешности завершения отработавшего метода, перехват исключений и реакция на ошибки выполнения;
- организация передачи транзактов между блоками.

Объект класса *BlockSequence* хранит список блоков. Через объект сессии (*Session*) можно получить всю информацию о текущем состоянии модели в любой момент времени. Условия прекращения процесса моделирования, которые определены командой STOP, хранит объект класса *StopConditions*.

Пользовательский интерфейс

Разработанная среда моделирования позволяет писать программы на языке GPSS и строить блок-диаграммы. На рис. 2 и 3 представлены редактор программ и редактор блок-диаграмм соответственно.

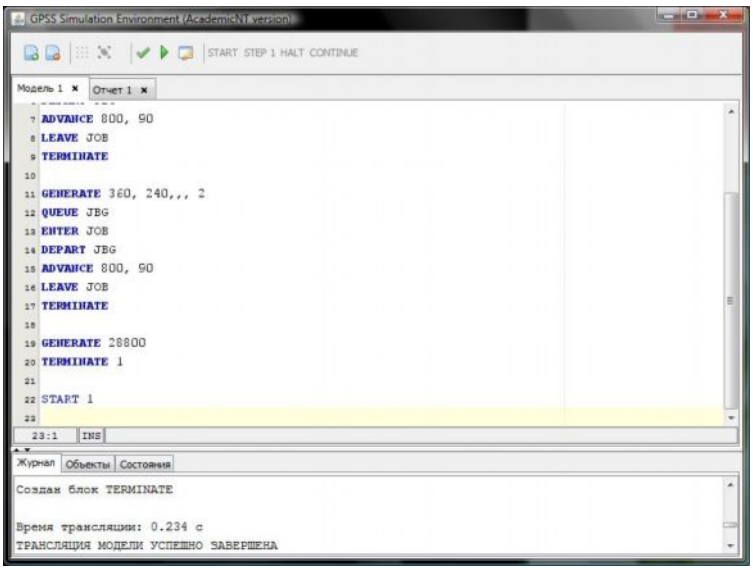


Рис. 2. Редактор GPSS-программ

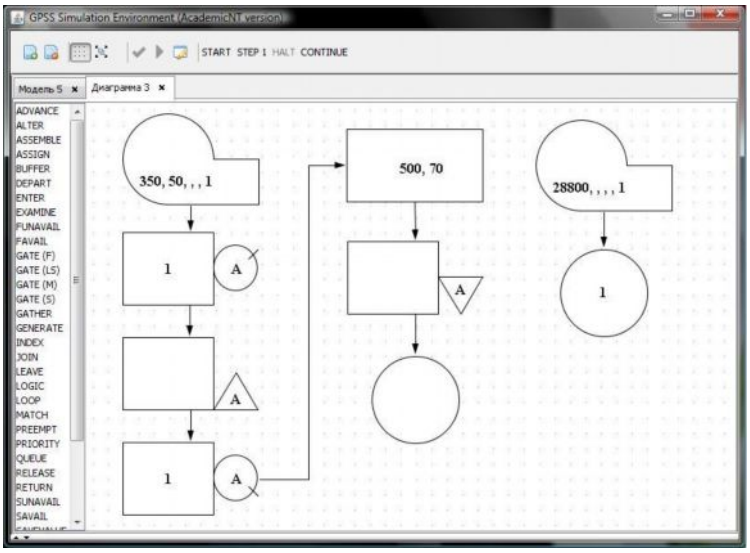


Рис. 3. Редактор блок-диаграмм

В верхней части окна находится панель инструментов с кнопками для создания и удаления вкладок с графическим или текстовым редактором, настройками редактора диаграмм, трансляции и запуска программы, а также наиболее часто используемыми при моделировании командами, которые могут быть переданы существующему процессу моделирования без повторной трансляции модели.

В нижней части окна располагаются информационные панели, показывающие состояние процесса моделирования. На вкладке «Журнал» отображается текущее событие или действие, выполняемое интерпретатором. Вкладки «Объекты» и «Состояния» предоставляют информацию об очередях, устройствах, накопителях, блоках, списках событий и т.п.

По результатам прогона модели среда автоматически формирует отчет. В отчете содержится информация о времени моделирования, блоках модели, устройствах, очередях (для которых были описаны регистраторы) и других объектах. Пример отчета представлен на рис. 4.

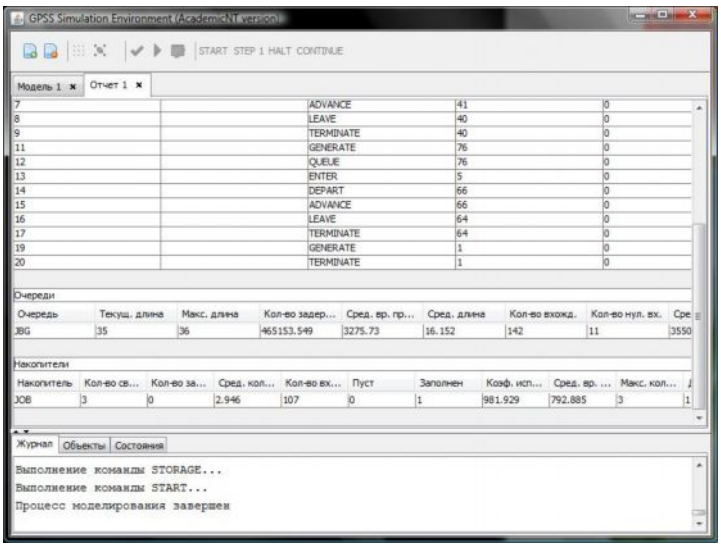


Рис. 4. Отчет

В отчет также включаются графики, если их создание было задано в настройках.

Заключение

Среда для создания GPSS-моделей выполнена на языке программирования Java. На текущий момент она позволяет:

– писать программы на языке GPSS, запускать их на выполнение и получать отчеты по результатам прогонов модели, содержащие информацию о состояниях объектов и статистические данные, собранные в процессе моделирования;

– строить графики по времени любых величин, которые указывает пользователь;

– строить блок-диаграммы с помощью имеющихся в библиотеке элементов GPSS-модели.

Среда ориентирована на специфику учебных задач и разрабатывается как элемент системы дистанционного обучения СПбГУ ИТМО для проведения лабораторных работ в рамках дисциплины «Моделирование систем». Следующим этапом развития проекта должна стать разработка проверяющей части виртуальной лаборатории.

Литература

1. GPSS. Имитационное моделирование систем [Электрон. ресурс] – Электрон. дан. – Режим доступа: http://www.gpss.ru , свободный. – Загл. с экрана.
2. Руководство пользователя по GPSS World: перевод с англ. / ООО «Элина – Компьютер» – Казань: Мастер Лайн, 2002. – 385 с.
3. Томашевский В. Имитационное моделирование в среде GPSS / В. Томашевский, Е. Жданова – М.: Бестселлер, 2003. – 416 с.
4. Кудрявцев Е.М. GPSS World. Основы имитационного моделирования различных систем / Е.М. Кудрявцев – М.: ДМК Пресс, 2004. – 320 с.
5. Боев В.Д. Инструментальные средства GPSS World: учеб. Пособие / В.Д. Боев – СПб.: БХВ-Петербург, 2004. – 368 с.

УДК 658.512

МЕТОДИКА КОМПЬЮТЕРНОЙ ОЦЕНКИ АНАЛИЗА ДРЕБЕЗГА КОНСТРУКЦИЙ ТЕЛЕ- И РАДИОАППАРАТУРЫ В СРЕДЕ LS-DYNA

А.А. Бурносенко (СООО «Микро Экспресс Инт'л», Беларусь),
Е.-А.А. Прохорова
(Объединенный институт проблем информатики НАН Беларуси)
Научный руководитель – д.т.н., профессор В.И. Махнач
(Объединенный институт проблем информатики НАН Беларуси)

Рассматривается актуальная задача анализа резонансных явлений, возникающая при проектировании аудио- и видеотехники. Рассмотрены возможности современных CAE-систем для проведения частотного анализа. В данной статье рассматриваются особенности частотного анализа на примере монитора ПО «Горизонт».

Ключевые слова: частотный анализ, конечно-элементная модель, резонанс

Введение

Одной из важных задач, решаемых при проектировании теле- и радиоаппаратуры, является акустический анализ дребезга в рабочем диапазоне звуковых частот. Дребезг возникает в элементах конструкции, собственная частота которых лежит в звуковом диапазоне. Сложность данной задачи заключается в выявлении таких элементов конструкции. При этом необходимо учитывать практически все составные части изделия, вплоть до самых мелких элементов.

Степень детализации конструктивной модели влияет на размер создаваемой конечно-элементной модели (КЭМ), что определяет важность выбора вычислительных средств расчета. Параллельно с выбором CAE-системы необходимо рассматривать модели, которые обеспечат требуемые для практики время получения результата с приемлемой точностью. Подробная модель изделия позволяет с высокой степенью точности выполнить расчет, при котором в конечном итоге можно составить оценку долговечности и качества работы конструкции, соизмеримые с реальными результатами. Такой анализ может быть выполнен и на персональном компьютере, однако потребует значительных временных затрат.

В условиях рынка, когда требуются обеспечить сжатые сроки на проведение компьютерного анализа, который в среднем должен составлять не более одного дня, актуальным становится разработка методики расчета для конструкций теле- и радиоаппаратуры и расчет с применением суперкомпьютера.

Постановка задачи для проведения акустического анализа

Целью акустического анализа является определение наличия или отсутствия критических частот, при которых выходное ускорение превышает входное более чем в 5 раз.

Анализ выполняется для одного из изделий монитора, который является частью комплекта интерактивной развлекательно-информационной универсальной системы СИРИУС ПО «ГОРИЗОНТ». Исходные данные представляют собой конструкторские 3D-модели деталей и сборок монитора, выполненные в среде CAD-системы PRO/ENGINEER.

Монитор закреплён на воздушном судне в подлокотнике пассажирского кресла. Необходимо определить распространение нежелательных колебаний по корпусным элементам монитора и участки конструкции, подверженные резонансу.

Расчет проводится в динамической постановке задачи. При расчетах необходимо учитывать спектральный состав возбуждающего воздействия, а также массы основных узлов, монтируемых на корпусе [1]. Динамические расчеты позволяют наглядно показать, как в начальный момент времени (перед тем, как достигается состояние установившихся свободных колебаний) в материале кожуха распространяется ударная волна, амплитуда колебаний узла, максимальная вначале, со временем уменьшается – энергия передается от точек, через которые в систему сообщается возбуждающее воздействие, во все участки системы.

Для динамических расчетов использована система LS-DYNA. При динамическом анализе можно рассмотреть колебания в корпусе при единичном воздействии, либо при явно заданном по времени акустическом сигнале. Отклик конструкции в этом случае представлен в явном виде и пригоден для статистической обработки (переход из временной в частотную область).

К изделию по каждой оси прикладывают по три удара, имеющих форму полусинусоидальных импульсов и номинальной длительностью каждого импульса 11 мсек. Итоговые данные должны включать расчеты с учетом нагрузки по осям: ±X, ±Y, ±Z.

Рассматривается поведение системы, нагруженной пиковым продольным ускорением по трем осям. Расчет производится в нелинейной динамической постановке в явном (интегрирование по времени) виде.

Проведение акустического анализа позволяет:

– определить параметры аналитической модели, которые давали бы наиболее приближенные к натурным испытаниям результаты;

– на ранних стадиях проектирования выявить зоны возникновения явления резонанса;

– обеспечить снижение отклика корпусных деталей на наиболее критических возмущающих частотах и вывод резонансных частот корпуса за воспроизводимый диапазон через усовершенствование конструкции элементов в выявленных зонах.

Необходимо разработать рекомендации, алгоритмы и модели для решения задачи инженерного анализа на платформе ВМВС (высокопроизводительная мультипроцессорная вычислительная система).

Подготовка математической модели и проведение анализа

Процесс выполнения частотного анализа включает в себя три этапа: *подготовка конструкторских данных, подготовка аналитической модели* и *оценка результатов.* Создание конечно-элементной модели осуществляется в среде HYPER MESH.

Существует ряд допущений, позволяющих с достаточной точностью получить требуемые данные. В процессе работы были даны рекомендации относительно моментов, на которые следует обратить внимание при подготовке конструкторской и расчетно-аналитической модели, дан перечень шагов и их особенностей.

Подготовка конструкторских данных включает в себя модификацию геометрической модели сборки монитора с целью ее упрощения. На данном этапе необходимо выполнить следующие шаги:

1. определить соответствия модели конструкторским чертежам;
2. с помощью технической документации определить положение динамиков и места контакта деталей в анализируемой сборке;
3. выявить основные детали конструкции (корпус, матрица, кожух и т.д.), для которых требуется провести частотный анализ;
4. выявить и устранить элементы геометрии, которые могут повлиять на создание корректных элементов конечно-элементной модели (КЭМ);
5. выявить элементы конструкции, которые могут не участвовать в частотном анализе (рис. 1).

Рассматриваемая сборка состоит из 6 деталей. Все детали, за исключением кронштейна, представляют собой оболочечные тела.

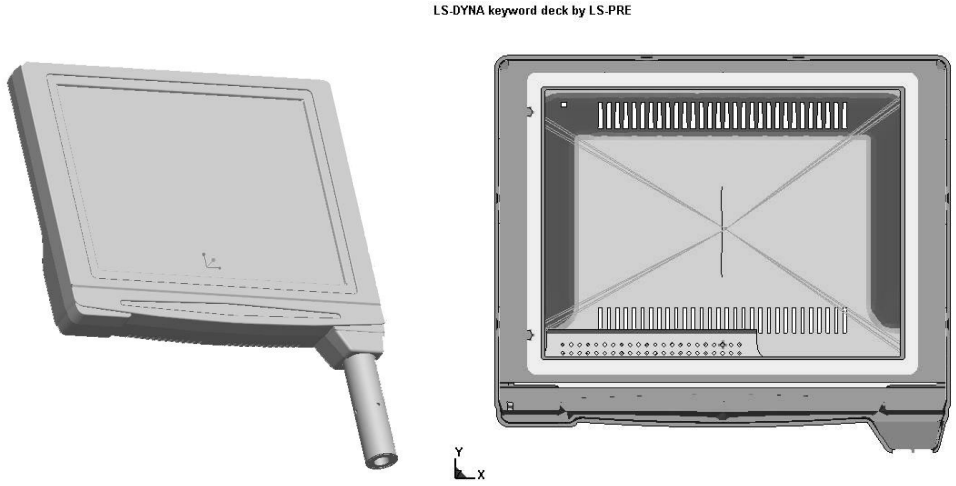


Рис. 1. Конструкторская (слева) и аналитическая модель монитора

Подготовка аналитической модели включает в себя генерацию сетки конечных элементов для моделей деталей монитора, а также формирование связей между взаимодействующими деталями и назначение нагрузок, определение материалов, свойств конечных элементов и других параметров в терминах системы LS-DYNA.

Общая схема проведения акустического анализа приведена на рис. 2.

Для создания аналитической модели используется система LS-PREPOST. Детали, не оказывающие значительного влияния на результаты расчетов, заменяются точечными массами соответствующей величины. Причем положение узла соответствует положению центра массы детали в сборке. Подготовка аналитической модели включает следующие этапы: задание схемы закрепления, материала, нагрузки и других ограничений, времени выполнения расчета.

При данной постановке задачи рассматривается нагрузка по трем (OX, OY, OZ) осям, созданы три расчетно-аналитических модели с разными заделками. При этом используется ряд допущений. Например, штанга, с помощью которой монитор крепится в салоне самолета, заменяется узлом с точечной массой и заданием взаимодействия с соседними деталями. Заделка прикладывается следующим образом: узлу запрещены все перемещения, кроме того, в направлении которого прикладывается нагрузка.

Допущения касаются также поверхностей контактирующих деталей и особенностей задания ограничений. Например, в рассматриваемой сборке все винтовые соединения рассматриваются как жесткие. Задание ограничений позволяет выполнить имитацию взаимодействия деталей. Созданы наборы точек, включающие точки контактирующих деталей. Далее полученные наборы точек сшиваются с соответствующими деталями.

Задание нагрузки осуществляется в три этапа и учитывает характер воздействия входных данных. Первый этап – задание точки приложения нагрузки. Второй – задание формы нагрузки в виде кривой нагрузки. Третий - приложение нагрузки.

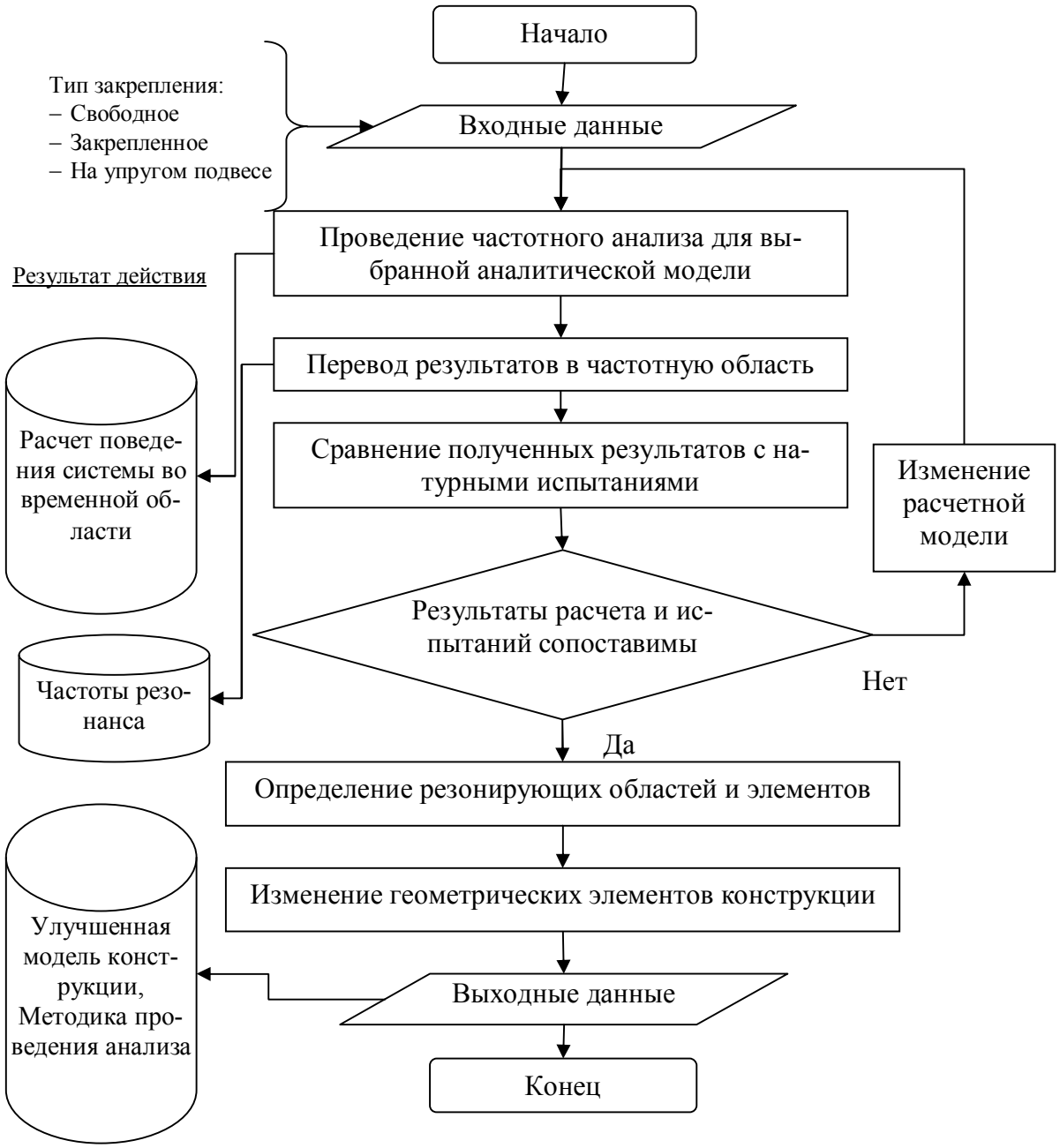


Рис. 2. Схема выполнения акустического анализа монитора

Результаты расчета должны иметь достаточный объем и разрешающую способность для последующего перехода в частотную область при помощи быстрого преобразования Фурье. Поскольку расчет поведения системы проводится во временной области, то главный параметр расчета с этой точки зрения – моделируемое время. Дискретность вывода результатов при расчете нужно выбирать такой, чтобы не терялись пики колебаний интересующих величин (напряжения, ускорения узлов). Если потолок интересующей частоты равен 300 Гц, то дискретность вывода должна составлять $5 \cdot 10^{-4}$ с.

Получение результата

Расчет полученной аналитической модели выполнен с помощью BMBC в пакете LS-DYNA [2, 3] на 5 узлах. Применение BMBC позволяет сократить время расчетов примерно в 8–9 раз по сравнению с расчетами на персональном однопроцессорном

компьютере (процессор AMD Athlon64 3000+, ОЗУ 1.5 Гб, Windows XP SP2). Расчет выполнен для каждого из трех вариантов закрепления, время расчета для каждого варианта составило 6ч.

Результаты расчета – продольные ускорения характерных точек сборки монитора – переведены из временной области в частотную, поскольку более четкое представление о природе происходящих процессов дает спектральное, а не временное представление. При необходимости результаты расчета (ускорения характерных точек деталей) можно использовать для модального анализа конструкции.

Перевод данных в частотную область осуществляется средствами постпроцессора (LS-PREPOST). Для получения спектра сигнала полученные данные преобразуются в ряд Фурье [4, 5], когда ось X представляет собой частотную ось, а по оси Y отсчитывается спектральная плотность ускорений, составляющих выходной сигнал. Ряд Фурье позволяет представить сигнал в виде суммы бесконечного множества гармонических колебаний, каждая из которых имеет свою собственную частоту, амплитуду и фазу. Такой ряд может быть получен для любой точки анализируемой конструкции и позволяет выделить резонансные частоты.

Как и предполагалось, основные области пиковых частот находятся на кожухе монитора. По результатам расчета наблюдаются напряжения в области левой и правой бобышек кожуха и соответствующих отверстий рамы, а также креплении моста к штативу.

Во всех трех случаях приложения нагрузки выявлена область резкого увеличения ускорений в зоне нижнего левого угла кожуха. Также выделены области повышенных значений в зоне боковых левой и правой стенки непосредственно в зонах крепления планки, на верхней решетке, в левой части средней решетки и на нижней решетке. Боковые зоны находятся в местах расположения бобышек, через которые осуществляется крепление матрицы и рамы. Непосредственно в нижней боковой зоне размещаются бобышки для крепления кожуха к корпусу кронштейна и происходит контакт кронштейна с бобышками кожуха. Было рекомендовано рассмотреть конструкцию смежных деталей и размещение мест крепления в выделенных зонах с целью выявления и устранения резонирующих элементов конструкции.

По результатам расчетов для монитора СИРИУС явление резонанса почти отсутствует, присутствуют зоны незначительного увеличения значения колебаний на частотах в пределах 200 Гц. Сравнение с натурными данными также показало наличие частоты, при которой наблюдается рост ускорений в отдельных узлах, однако, нарушений прочности узлов не наблюдается по причине их отсутствия.

Заключение

Применение средств инженерного анализа при проектировании радиоэлектронных устройств позволяет повысить акустические качества телеаппаратуры и устранить возможные проблемы ее эксплуатации уже на стадии проектирования.

Разработанные схема и рекомендации подготовки и проведения частотного анализа монитора позволяет сократить время анализа для разнообразных конструкций теле- и радиоаппаратуры, позволяя оценить характер поведения модели с достаточным приближением к натурным испытаниям.

Согласованность натурных и расчетных результатов позволяет считать разработанную методику и получаемые с их помощью расчетные модели адекватными и рекомендовать для работы с аналогичными конструкциями мониторов.

Время подготовки данных для проведения расчета и получения результатов составляет в среднем 5–7 часов, что позволяет осуществлять анализ и выполнять улучшение конструкции в реальном режиме проектирования изделия.

К экономическим последствиям внедрения данного анализа в сквозной цикл производства можно отнести:

– сокращение затрат на проведение натурных испытаний за счет сокращения количества необходимых опытных образцов;

– сокращение затрат на проектирование за счет повышения его качества и сокращения исправлений, извещений, доработок, в целом циклов повторного проектирования;

– сокращение затрат на проведение натурных испытаний за счет изменения и сокращения программы испытаний.

Литература

1. Ротенберг Р.В. Подвеска автомобиля. – М.: Машиностроение, 1972. – 392 с.
2. LS-DYNA. Руководство пользователя. Часть 1. Версия 960. – Ливермор, Калифорния: Livermore Software Technology Corporation, 2001. – 1421 с.
3. Абламейко С.В., Абрамов С.М., Анищенко В.В., Парамонов Н.Н. Суперкомпьютерные конфигурации «СКИФ». Мн.: ОИПИ НАН Беларуси, 2005. – 195 с.
4. Павлейно М.А., Ромаданов В.М. Спектральные преобразования в MatLab. – СПб: 2007. – С. 160.
5. Сергиенко А.Б. Цифровая обработка сигналов. – 2-е. – СПб: Питер, 2006. – С. 751.

УДК 004.855.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВОЗМОЖНОСТЕЙ СОЦИАЛЬНЫХ СЕТЕЙ ДЛЯ ПРИМЕНЕНИЯ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

А.В. Ольшевская, Д.Г. Николаев
Научный руководитель – к.т.н., доцент Д.Г. Штенников

В статье содержится сравнительный анализ двух русскоязычных социальных сетей, которые являются наиболее популярными и по-прежнему сохраняют бесплатными регистрацию и многие другие услуги. В ней отражены основные достоинства и недостатки данных сервисов. Также рассмотрены те услуги социальных сетей, которые возможно использовать в образовательном процессе.

Ключевые слова: социальная сеть, образовательный процесс, профайл, веб-сайт, форум, чат, гостевая книга, блог, видеофайл, аудиофайл, фотография, группа пользователей, аккаунт, сетевой преподаватель, фотоальбом, опрос, обсуждение, консультация, дистанционное обучение

Введение

Наиболее важной составляющей развития интернет-технологий является возможность непосредственного общения людей. Существует множество форм организации взаимодействия пользователей между собой с помощью веб-технологий: форумы, чаты, гостевые книги, блоги и т.д. Благодаря развитию подобных сервисов стали образовываться социальные сети – веб-сайты, направленные на построение сообществ в интернете из пользователей, которые непосредственно формируют контент подобных сайтов.

Социальная сеть – в обычном значении этого слова – это множество социальных объектов и определенное на нем множество отношений. В интернете социальная сеть – виртуальная сеть, являющаяся средством обеспечения сервисов, связанных с установлением связей между его пользователями, а также разными пользователями и соответствующими их интересам информационными ресурсами, установленными на сайтах глобальной сети. По сравнению с уже обычными на сегодняшний день службами общения пользователей интернета, социальные сети имеют ряд дополнительных возможностей [1].

Участники таких сетей объединены не только средой общения, но и явно установленными связями между собой. В последнее время популярность социальных сетей возрастает, так как кроме неформального общения, например, выпускников какого-либо ВУЗа, они постепенно становятся рабочим инструментом для ведения различного рода деятельностей. Будь то бизнес, творчество или организация учебного процесса.

Основной целью данной работы является выбор двух социальных сетей, их сравнительный анализ с последующим формированием представления о том, как возможно их использовать в образовательном процессе.

Для изучения и анализа были выбраны два проекта: MySpace и VKontakte. Основными критериями в данном вопросе были: популярность, бесплатная регистрация, возможность выбора русской версии сайта. В большинстве рейтингов оба этих сервиса занимают высокие позиции и, при этом, основные их услуги остаются бесплатными. Также проекты ориентированы на русскоязычную аудиторию, что является немало важным аспектом выбора MySpace и VKontakte [2].

Регистрация в социальных сетях MySpace и VKontakte

На главной странице сайта http://www.myspace.com/ располагается много рекламы проекта MySpace и информации о нем. Главная страница социальной сети http://vkontakte.ru/ предоставляет только основную информацию о сообществе VKontakte, что является явным преимуществом по сравнению с первым сайтом.

Регистрация имеет некоторые различия. На первом сайте, для удобства пользователей, при установке курсора в поля регистрационной страницы появляются подсказки, что позволяет точнее разобраться в том, как правильно создавать свой аккаунт. При прохождении регистрации в проекте VKontakte пользователю предоставляется меньше полей для заполнения, что экономит его время.

При регистрации на обоих сайтах необходимо вводить специальный код, отображаемый на картинке. В проекте VKontakte он сложно различим, а при неправильном вводе приходится заполнять несколько полей вновь, что сильно затрудняет процесс создания аккаунта. В проекте MySpace эта проблема решена. Под кодом располагается круглая кнопка обновления, благодаря которой проще выбрать более понятный код для введения в поле. Также существует специальная инструкция под картинкой, чтобы пользователь мог точно ввести то, что на ней изображено. Но если вовремя не ввести код, то через определенное количество секунд он автоматически обновится, после чего придется изменять введенные данные, что не совсем удобно для пользователей, регистрирующихся на сайте.

После регистрации на указанный e-mail отправляется письмо с регистрационными данными и ссылкой на подтверждение аккаунта, после перехода, по которой профайл пользователя становится активным и он может войти на веб-сайт.

Группы пользователей

Создание группы в проекте VKontakte происходит без особых проблем, так как для каждого пункта существуют соответствующие подсказки, располагающиеся, как правило, под пунктом заполнения. Предусмотрено несколько типов групп: академическая группа, клуб, группа выпускников, организация, приватная (частная) группа. Информацию, которая была введена при создании группы, можно изменять. Также существует возможность редактировать руководство и состав отдельной группы. Все это позволяет пользователям более мобильно контактировать с участниками сообщества быть в курсе последних изменений.

В каждой из групп присутствуют следующие сервисы: «Свежие новости», «Обсуждения», «Фотографии», «Аудиозаписи», «Видеофайлы», «Участники», «Стена». Они позволяют организовать достаточно удобный процесс обучения. Например, сервис «Обсуждения» может заменить форум, который обычно реализуется в дистанционном обучении, а сервисы «Фотографии», «Аудиозаписи», «Видеофайлы» позволят сделать процесс обучения более увлекательным.

Удаление групп проекта VKontakte происходит автоматически при выходе всех пользователей из ее состава.

В проекте MySpace группу можно создать только по истечении 7 дней с получения аккаунта, что является неудобным для участников сообщества. При добавлении новой группы на странице сайта есть пункт «URL-адрес», который может вызвать непонимание у неопытных пользователей, что приведет к множеству ошибок. Ко всем остальным пунктам добавлены полноценные справки, что помогает корректно создавать новые группы. Плюсом MySpace является то, что количество категорий, по которым добавляются группы, гораздо больше, чем существует в VKontakte. К ним относятся: «Литература и искусство», «Музыка», «Наука и история», «Государство и политика», «Студенческие сообщества» и т.д. Однако для осуществления процесса дистанционного обучения типы групп имеют небольшое значение и вполне достаточно пяти, реализованных в VKontakte.

После добавления группы существует возможность ее изменения, можно пригласить новых участников для общения, а также добавить изображение, объявление или тему для обсуждения. Возможность добавить аудио отсутствует, а демонстрация видео

в группе может быть осуществлена только после предварительной погрузки видеофайла в профайл какого-либо пользователя.

Лидер группы в MySpace может сам удалить ее. Для этого необязательно всем участникам покидать группу, как это осуществлено в проекте VKontakte. После удаления группы все данные будут уничтожены.

Размещение видеофайлов, аудиофайлов и фотографий

При дистанционном обучении преподаватель и обучаемый пространственно отделены друг от друга, поэтому очень сложно постоянно поддерживать интерес последнего к какому-либо занятию. Чем качественнее и нагляднее предоставляемый материал, тем процесс обучения будет более увлекательным для обучаемого. В этом плане незаменимыми становятся такие ресурсы, как фотографии, видеофайлы, аудиофайлы.

Для пользователей очень важным аспектом является время, которое будет затрачено на загрузку фотографий, аудиофайлов и видеофайлов. На рис. 1 представлен график, который позволяет проанализировать в какой из социальных сетей удобнее и быстрее добавляются фотографии. Для его построения были подобраны файлы различного объема, которые поочередно погружались в каждую из сетей.

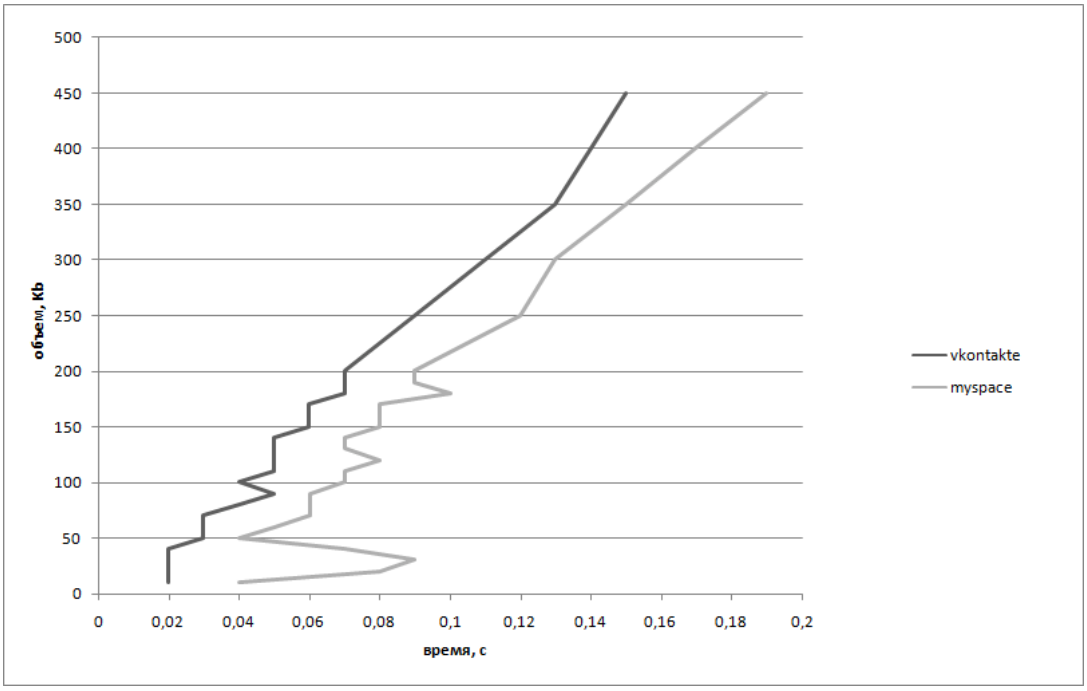


Рис. 1. График загрузки фотографий

Вначале были подобраны файлы, имеющие маленький объем и разницу в нем. Время на их загрузку было приблизительно одинаковым, поэтому график получился зигзагообразным. Но, начиная с 200 Kb, разница в объеме файлов увеличилась, что и привело к появлению линейной зависимости. Судя по графику, загрузка фотографий в обоих проектах осуществляется примерно одинаково.

На рис. 2 представлен график, демонстрирующий временные затраты при загрузке аудиофайлов в проекте VKontakte. В социальной сети MySpace, к сожалению, невозможно добавлять аудиозаписи. Этот факт является большим недостатком данного проекта.

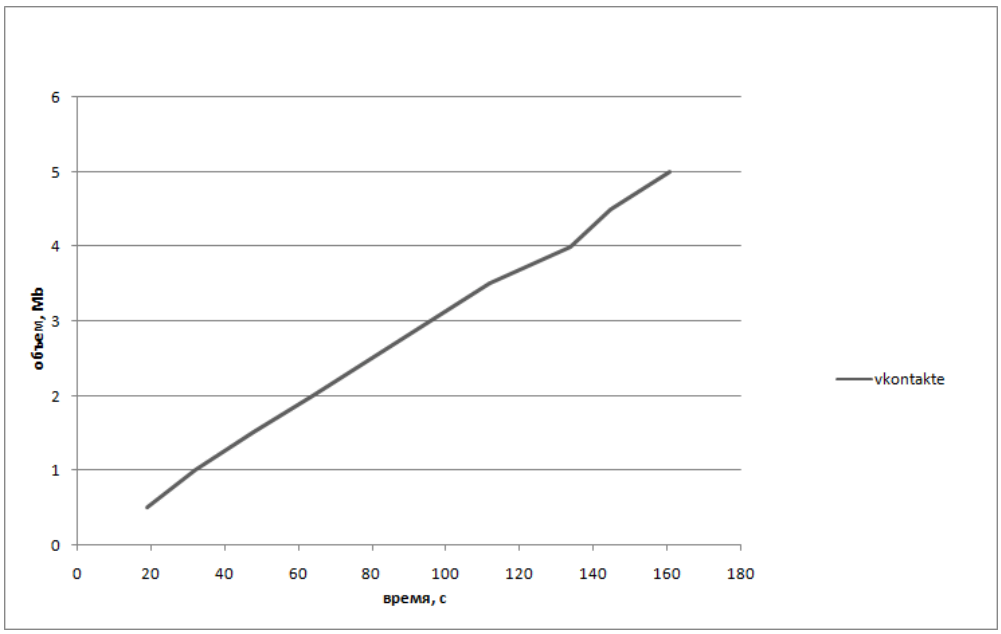


Рис. 2. График загрузки аудиофайлов

В табл. 1 представлены временные затраты на погрузку трех видеофайлов. Исходя из этих данных получается, что для загрузки подобных файлов проект MySpace подходит лучше. Однако разрыв небольшой, тем более, если учитывать некоторую погрешность в измерениях.

№ файла	Размер файла	Вес файла, Мб	Формат	Время загрузки в Vkontakte, мин.	Время загрузки в MySpace, мин.
1	5-минутный	28,1	wmv	16,42	15,2
2	10-минутный	82,6	wmv	57,39	45,01
3	20-минутный	134	wmv	77,37	73,29

Таблица 1. Загрузка видеофайлов

Создание опросов, тем для обсуждения

В созданных группах проекта VKontakte можно сформировать темы для обсуждения, которые по принципу своей работы схожи со стандартными форумами. Отличие заключается в том, что обсуждение происходит только в текстовой форме, и в процессе дискуссии нет возможности указать на какое именно сообщение отвечает пользователь. К созданной теме обсуждения можно добавить опрос. Максимальное количество вариантов ответа – 15. При необходимости, опрос может быть вынесен на главную страницу группы, но на ней может быть размещено не более одного опроса. В нем могут принимать участие только зарегистрированные пользователи группы. Однако опрос происходит анонимно, то есть нельзя посмотреть, какой вариант ответа выбрал тот или иной пользователь.

Темы обсуждения в группах проекта MySpace так же похожи на стандартные форумы. Их отличительной особенностью является возможность цитирования сообщения при ответе. При этом в рамках обсуждаемой темы нет возможности использовать опрос.

Добавление учебного материала

При организации процесса обучения с использованием социальных сетей существует возможность размещения обучающего материала и выполненных заданий в различных электронных форматах. Помимо обычного текста, в группах проекта VKontakte можно добавлять:

(1) графический материал (в форматах .gif, .jpg, .bmp, .png);

(2) аудиозаписи (в формате .mp3);

(3) видеозаписи (в форматах .avi, .mp4, .3gp, .mpeg, .mov, .mp3, .flv, .wmv).

Кроме этого проект VKontakte позволяет преподавателю размещать различные приложения в формате .swf.

По сравнению с проектом VKontakte, MySpace имеет ограничения в видах электронной информации. При работе с группой в этом проекте можно использовать только:

(1) графический материал (в форматах .gif, .jpg, .bmp, .png), а также и gif-анимацию;

(2) видеозаписи (в форматах .avi, .asf, .dv, .wmv, .mov, .qt, .3g2, .3gp, .3gp2, .3gpp, .gsm, .mpg, .mpeg, .mp4, .m4v, .mp4v, .cmp, .divx, .xvid, .264, .rm, .rmvb, .flv, .mkv, .ogm).

Размещение видеофайлов в группах проекта MySpace может быть выполнено только в виде объявления, с предварительной загрузкой самого файла на страницу участника группы.

Размещение приложений

Проект VKontakte позволяет преподавателю, как руководителю группы размещать приложения в формате .swf. Для образовательного процесса это могут быть интерактивные презентации, тесты, обучающие игры, примеры выполненных работ. Другие участники группы не могут размещать свои приложения в группе. Наряду с авторскими, есть возможность добавления приложений из уже существующего списка приложений проекта. При формировании группы для применения в образовательном процессе, наиболее подходящим стандартным приложением является чат, который может быть использован для организации сетевого взаимодействия участников группы.

Проект MySpace исключает возможность размещения авторских приложений. Среди приложений проекта не нашлось тех, которые можно использовать в образовательном процессе.

Осуществление взаимодействия с преподавателем

Сетевое взаимодействие с преподавателем может осуществляться в двух режимах: синхронном и асинхронном.

В проекте VKontakte обмен личными сообщениями и возможность размещения в группе тем для обсуждения позволяют реализовать асинхронный режим общения. В зависимости от настроек прав доступа, темы для обсуждения могут быть созданы как самим преподавателем, так и другими участниками группы. Подключение приложения «Чат» позволит организовать в группе синхронный режим взаимодействия. Использование чата дает возможность любому участнику группы задать вопрос преподавателю и в режиме реального времени получить на него ответ.

Проект MySpace позволяет организовать только асинхронный режим общения при помощи форума и обмена личными сообщениями.

Версии социальных сетей для мобильных устройств

Разработчики проекта VKontakte предусмотрели версию сайта для мобильных устройств (http://pda.vkontakte.ru). Однако набор функций, доступный в мобильной версии, очень ограничен. В ней невозможно использовать фотоальбомы, аудио- и видеозаписи, опросы, приложения. В мобильной версии сайта остались новости, темы обсуждений, стена, где можно использовать лишь текстовые сообщения, и возможность отправлять личные сообщения. У проекта MySpace также существует версия для мобильных устройств (http://m.myspace.com). Однако эта версия не позволяет работать с созданными в проекте группами.

Итоговое сравнение

В табл. 2 и 3 приведены все плюсы и минусы сравниваемых социальных сетей, которые были выявлены в процессе исследования.

№	Недостатки MySpace	Достоинства MySpace
1	большое количество рекламы	возможность размещения gif-анимации
2	использование некоторых сервисов доступно только через 7 дней с момента регистрации	при обсуждении можно цитировать сообщения
3	«недружественность» интерфейса	
4	избыточные для образования элементы	
5	нет стандартной возможности размещать собственные аудиозаписи	
6	«неудобный» принцип размещения видеозаписи в группе	
7	нет возможности создания в группе нескольких фотоальбомов	
8	нет возможности создания опроса	
9	нет настройки ролей участников группы	

Таблица 2. Достоинства и недостатки проекта MySpace

№	Недостатки VKontakte	Достоинства VKontakte
1	нет возможности размещения gif-анимации	хорошо продуманный интерфейс
2	только администраторы группы могут добавлять приложения	возможность формирования нескольких фотоальбомов
3	при обсуждении нет возможности цитировать сообщение	возможность создания опроса
4		возможность добавления дополнительных приложений
5		возможность размещения аудио- и видеозаписей

Таблица 3. Достоинства и недостатки проекта VKontakte

Заключение

Сравнительный анализ наиболее популярных социальных сетей показал, что для применения в образовательном процессе проект VKontakte выгодно отличается от проекта MySpace. Возможности VKontakte позволяют преподавателю провести дистанционное обучение, используя в основном стандартные сервисы проекта, такие как размещение в группе графического материала (с разделением по тематикам), аудиофайлов, видеофайлов, формирование тем для обсуждения (с возможностью опроса), добавление flash-приложений.

Литература

1. Мерзлякова С.В., Пирская А.С., Смирнова Е.В. Основы работы в сети Интернет. – СПб.: СПбГУ ИТМО, 2008. – 120 с.
2. Блог о социальных сетях [Электронный ресурс] / Социальные Сети - Блог, 2008. – Режим доступа: http://socseti.com, свободный. – Загл. с экрана.
3. Социальные Сети Рунета. Web 2.0 [Электронный ресурс] / Revolution Code Blue, 2008. – Режим доступа: http://socialok.net, свободный. – Загл. с экрана.

УДК 004.418

ИНТЕГРАЦИЯ ОБРАЗОВАТЕЛЬНЫХ И СОЦИАЛЬНЫХ ФУНКЦИЙ ШКОЛЫ В WEB-СИСТЕМЕ JUNIOR U

А.В. Беляев, М.И. Гаврилов, А.Н. Ситников
Научный руководитель – к.т.н., доцент Э.В. Денисова

В статье рассматриваются типы социальных сетей: сетей общего назначения и нишевых сетей. Дано обоснование целесообразности создания школьной социально-образовательной сети. Рассмотрены функциональные особенности и аспекты реализации подобной сети Junior U – WEB-сайта, являющегося социальной сетью с образовательным уклоном.
Ключевые слова: web, социальная сеть, дистанционное обучение

Введение

Современные наиболее популярные социальные сети рассчитаны на широкую аудиторию и объединение людей по интересам в них происходит с помощью механизма групп. Подобные социальные сети общего назначения обладают схожей функциональностью:

- группы (круги, сообщества);
- блоги (заметки, журналы);
- сообщения;
- медиа (фотографии, видео, аудио).

Одновременно развиваются так называемые нишевые социальные сети, которые рассчитаны на более узкую целевую аудиторию, предоставляя некоторые специализированные сервисы для данной аудитории:

- подбор персонала;
- сервисы знакомств;
- коллективные блоги.

Нишевые социальные сети обеспечивают удобное взаимодействие пользователей с учетом специфики их деятельности. Образовательные сайты для учебных заведений и для дистанционного обучения обычно предоставляют следующие функции:

- разделение ролей (учитель, ученик);
- дневники;
- расписания занятий;
- журнал оценок;
- система раздачи заданий и сбора выполненных заданий;
- коллекция материалов (библиотека).

Идея объединить социальную сеть общего назначения с образовательным сайтом, т.е. создать специализированную (нишевую) социальную сеть для образования появилась относительно недавно. Если, скажем, для системы высшего образования польза подобного объединения сомнительна, то для школы есть некоторые очевидные и неочевидные плюсы.

Концепция безопасности

Для детей школьного возраста критическим аспектом работы в Интернете и в социальной сети в частности является безопасность:

- ограничения на контент;
- ограничение возможностей третьих лиц на общение с детьми;
- отсутствие анонимных угроз.

Данные аспекты безопасности сложно обеспечить в социальной сети общего назначения, т.к. регистрация открыта для всех. Сложно также обеспечить верификацию возраста и идентифицировать регистрируемого.

Концепция Junior U, объединяя в себе функции социальной сети и образовательного сайта, позволяет решить проблему безопасности школьников. Для этого вводятся следующие роли:

- ученик;
- учитель;
- родитель ученика.

Для пользователей действуют правила регистрации:

- учитель регистрируется на сайте, указывая свою школу;
- его учетная запись активизируется администратором сайта по звонку в школу;
- учитель может регистрировать учеников и их родителей.

Таким образом, учетные записи учителей связаны с конкретными учителями. Учителя подписывают на сайт учеников и родителей, также обеспечивая соответствие пользователя типу учетной записи.

Ограничения на контент работают автоматически, т.к. учителя и родители имеют возможность контролировать контент, созданный учениками. Более того, коль скоро каждая учетная запись связана с конкретным человеком, он несет ответственность за созданный контент в полной мере. Нежелательные элементы не могут зарегистрироваться на сайте ни в качестве учителей (из-за верификации), ни в качестве школьников или родителей (последних регистрирует учитель). Анонимные угрозы отсутствуют, т.к. за каждой учетной записью стоит конкретный человек.

Функциональность

Как уже было сказано, на сайте есть три типа пользователя: ученик, учитель, родитель. Часть функций доступна всем типам пользователей, часть функций могут выполнять лишь определенные типы пользователей. Социальные функции, разумеется, доступны всем:

- заметки с возможностью комментирования;
- фотографии с возможностью комментирования;
- сообщения;
- профайлы (странички, где пользователь может указать различные данные о себе: имя, возраст, фото и т.д.).

Важным аспектом сайта является сущность школы. Для всех школ автоматически создаются профайлы, с указанием контактных данных школы и ее директора. Пользователи-ученики и пользователи-учителя при регистрации ассоциируются с одной из школ. Учителям доступны следующие функции:

- регистрация учеников школы и их родителей;
- создание классов из учеников школы;
- рассылка заданий в классе;
- ведение журнала оценок класса.

Ученики, как основные (по количеству) пользователи системы, имеют следующие возможности:

- доступ к персональному расписанию;
- просмотр своих оценок;
- просмотр своих классов и их свойств;
- возможность загрузить файл выполненного задания к заданию учителя;
- доступ к профайлам своих родителей.

Родители, помимо общего контроля за контентом, могут делать следующее:

– смотреть профайлы своих детей;
– контролировать успеваемость своих детей, просматривая их расписание и оценки.

Реализация

Описанная функциональность была реализована с использованием современных WEB-технологий: Взаимодействие этих технологий в виде компонентов представлено на рис. 1.

Технология	Назначение
Python	Основной язык программирования серверной логики [1]
PostgreSQL	Сервер баз данных [2]
JuniORM	Собственная библиотека для организации ORM с кэшированием в Memcache
Memcache	Распределенный кэш для объектов ORM и отрендереных страниц [3]
Nginx	Фронт WEB-сервер и балансировщик нагрузки [4]
CherryPy	WSGI-сервер для бекэнда [5]
Mako	Рендерер HTML, XML страничек [6]
PIL	Библиотека обработки графических файлов
SimpleJson	Сериализатор JSON
FormEncode	Верификатор данных форм
Psycopg2	Библиотека доступа к PostgreSQL из Python

Таблица 1. Используемые технологии

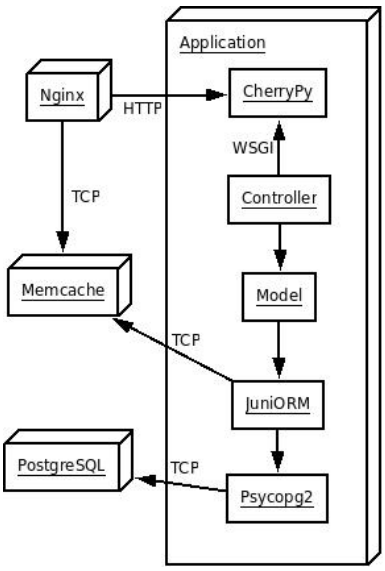


Рис. 1. Взаимодействие технологий и компонентов

Параллелепипедами на диаграмме обозначены процессы, а прямоугольниками – компоненты и библиотеки. HTTP запрос поступает на WEB-сервер Nginx, который, в свою очередь, смотрит, есть ли нужный прокэшированный запрос в распределенном кэше Memcache. Если есть, то выдает результат оттуда, если нет, то передает запрос в процесс приложения по протоколу HTTP. Внутри процесса приложения WEB-сервер CherryPy по протоколу WSGI вызывает методы контроллера, который, обрабатывая параметры запросов и используя модель, генерирует ответ. Модель для хранения данных в базе данных использует ORM (Object-Relational Mapper) JuniORM. JuniORM использует распределенный кэш Memcache для кэширования объектов базы данных. Тем самым облегчается нагрузка на базу данных и увеличивается общая производительность приложения. JuniORM использует библиотеку Psycopg2 для взаимодействия с сервером базы данных PostgreSQL. Подобная архитектура позволяет масштабировать приложение на несколько физических машин, как показано на рис. 2.

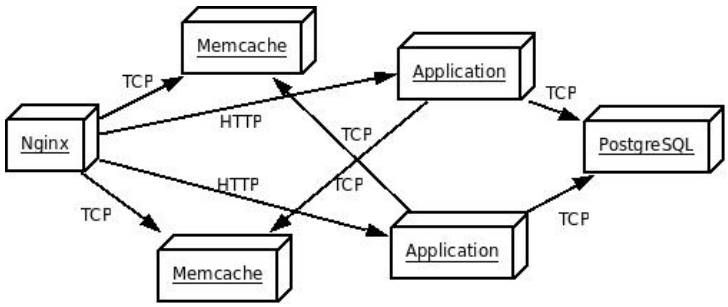


Рис. 2. Масштабирование

Процессы Application и Memcache присутствуют в нескольких экземплярах. Распределение процессов по физическим машинам может быть, например, следующим. Первая машина – балансировщик нагрузки с Nginx. Вторая и третья машины – серверы приложений и распределенного кэша. Каждая из них содержит процессы Memcache и Application. Четвертая машина – сервер базы данных с процессом PostgreSQL. Подобная схема масштабирования называется горизонтальным масштабированием, поскольку позволяет увеличивать производительность системы, просто добавляя машины. Горизонтальное масштабирование хорошо освещено в статьях [7].

Заключение

В статье дано обоснование наличия ниши для школьных социальных сетей. На примере проекта Junior U рассмотрены функциональные особенности таких сетей. Описана архитектура Junior U, как машстабируемого WEB-сервиса.

Литература

1. Python Porgramming Language [Электронный ресурс] / Python Software Foundation, 2009. – Режим доступа: http://python.org, свободный – Загл. с экрана. – Яз. англ.
2. Postgresql [Электронный ресурс] / Postgresql Global Development Group, 2009. – Режим доступа: http://postgresql.org, свободный – Загл. с экрана. – Яз. англ.
3. Memcached Distributed Cache [Электронный ресурс] / Livejournal LLC, 2009. – Режим доступа: http://danga.com/memcached, свободный – Загл. с экрана. – Яз. англ.
4. Nginx [Электронный ресурс] / И. Сысоев, 2009. – Режим доступа: http://sysoev.ru/nginx, свободный – Загл. с экрана. – Яз. англ.
5. CherryPy [Электронный ресурс] / Python Software Founation, 2009. – Режим доступа: http://cherrypy.org, свободный – Загл. с экрана. – Яз. англ.
6. Mako Templates for Python [Электронный ресурс] / M. Bayer, 2009. – Режим доступа: http://makotemplates.org, свободный – Загл. с экрана. – Яз. англ.
7. HighScalability [Электронный ресурс] / T. Hoff, 2009. – Режим доступа: http://highscalability.com, свободный – Загл. с экрана. – Яз. англ.

УДК 004.4:658

К ВОПРОСУ О СОЗДАНИИ СИСТЕМЫ УПРАВЛЕНИЯ ЗНАНИЯМИ В ПРОЦЕССЕ ВНЕДРЕНИЯ ERP-СИСТЕМ

Н.Д. Торопова
(Уфимский государственный авиационный технический университет)
Научный руководитель – доцент Т.К. Гиндуллина
(Уфимский государственный авиационный технический университет)

В данной статье рассматривается вопрос управления знаниями на предприятиях России. В процессе внедрения и адаптации корпоративных информационных систем вся информация о работе с ней, в лучшем случае, отражается в документах, расположенных независимо от внедряемой системы, а, порой, и не сохраняется вовсе. Такая ситуация ведет к потере знаний о работе в системе и отказу работников переходить на новые информационные технологии, снижая тем самым эффективность деятельности и конкурентоспособность предприятия. Описывается ход работ по созданию системы управления знаниями на предприятии и путей ее дальнейшего развития.

Ключевые слова: знания, корпоративная информационная система, система управления знаниями, предприятие, ERP-система, инструкция, архив, пользователь, разработчик, поддержка, справка

Введение

> «В современном мире знания представляют собой значительную силу. Знания, как таковые, являются ключом к развитию и совершенствованию» [1]
>
> Питер Друкер

В настоящий момент на предприятиях России ведутся проекты по внедрению ERP-систем. Так, многие предприятия, предъявляющие высокие требования к производству, продвижению и оказанию услуг, возлагают решение вопросов повышения эффективности своей деятельности на различные ERP-системы.

Не секрет, что далеко не многие, даже самые удачные, проекты, реализованные на предприятиях, реально справляются с возложенными на них задачами.

Так, например, результаты исследований компании Standish Group, которая проанализировала итоги выполнения более 23 тысяч проектов, связанных с разработкой ПО, утверждает, что всего 16,2% проектов завершились в срок, не превысили запланированных бюджет и реализовали все требуемые функции и возможности [2].

Одной из основных проблем при внедрении ERP-систем, является отсутствие квалифицированных специалистов по работе в системе, либо необходимость в обучении персонала предприятия силами организации. Любому, даже самому преуспевающему человеку, хотя бы на первых этапах работы с незнакомой программой, необходимо обращение к функциональной и информационной справочной системе по работе с данным продуктом в соответствии с особенностями конкретного предприятия. Отсутствие такой поддержки ведет к некорректной работе системы в целом, и как следствие, к снижению эффективности работы ERP-системы.

Каждая корпоративная информационная система (далее КИС) проходит адаптацию на предприятии-пользователе, в процессе которой информация о вносимых изменениях и вновь разработанных модулях не фиксируется практически ни в одной ERP-системе.

Многие организации, своими силами адаптирующие систему, разрабатывают инструкции по работе с каждым из сеансов КИС, однако, вся эта информация, в большинстве случаев, хранится совершенно не зависимо от ERP-системы, работа в

которой для работников предприятия становится всё более непонятной. Такая ситуация является одной из причин отказа работников от перехода на новые информационные технологии и, как следствие, застоя в развитии компании [3].

Проблемы такого рода были выявлены на одном из крупнейших промышленных предприятиях – ОАО «Уфимское моторостроительное производственное объединение» (далее ОАО «УМПО»), отдавшее в 2000-ом году предпочтение в выборе КИС компании Альфа-Интегратор. Продуктом компании Альфа-Интегратор является КИС BAAN, сфокусированная на предоставлении отраслевых информационных решений и связанных с ними услуг производителям в различных отраслях промышленности. Использование значительного опыта компании позволяет её клиентам достичь минимальной стоимости владения и максимально быстрого достижения экономического эффекта от внедряемых решений.

Итак, справочная система BAAN на ОАО «УМПО» реализована в виде отдельных электронных текстовых документов, распределённых по ЭВМ разработчиков. Для основного состава пользователей BAAN организовано разовое обучение ведению бизнес-процессов в BAAN и последующая поддержка по горячей линии.

Проведенный анализ выявил следующие проблемы:

– работники предприятия тратят слишком много времени на получение необходимой информации, а разработчики на ее поиск;

– в большинстве случаев, опыт ведущих и наиболее квалифицированных сотрудников используется только ими самими;

– ценная информация захоронена в огромном количестве документов и данных, доступ к которым затруднен;

– дорогостоящие ошибки повторяются из-за недостаточной информированности и игнорирования предыдущего опыта.

Такие проблемы являются ничем другим, как самым актуальным списком причин, который заставляет серьезно задуматься о проблеме управления знаниями на предприятии.

По данным одного из отчетов американского журнала «Fortune», 40% компаний, входящих в список «Fortune 1000», имеют в своем составе специального сотрудника, ответственного за создание инфраструктуры и развитие культуры совместного использования знаний [4].

Сегодня с такой необходимостью столкнулись и российские предприятия.

Так, организация независимого архива инструкций не охватывает все аспекты рассматриваемой проблемы. Необходима разработка интегрированной с BAAN системы поддержки работы пользователей. Такая система должна обеспечивать пользователей необходимой информацией по работе в конкретной КИС в соответствии с особенностями организации в процессе всего жизненного цикла каждого из бизнес-процессов на предприятии.

В целях же дополнительного обучения и удобства пользователей организован доступ к справочной системе BAAN с Web-портала предприятия, где для каждой инструкции планируется организовать ссылку на демоверсию сеанса, о котором идёт речь. Таким образом, сотрудники предприятия смогут не только найти и прочесть интересующий их материал, но и попробовать ее «на вкус», используя демонстрационный пример конкретного сеанса в КИС BAAN, ведь, не зря говорят, что теория без практики мертва.

Анализ предметной области

Рассмотрим процесс создания инструкций по работе в КИС BAAN на ОАО «УМПО».

На данный момент на ОАО «УМПО» в отделе ОРИТ установлено 6 рабочих мест. На каждого специалиста приходится определенный блок инструкций, подлежащий по необходимости доработке, корректировке, поиску и распространению их персоналу предприятия, что влечёт за собой нерациональное использование памяти ЭВМ в связи с большими объемами хранения дублируемой и устаревшей информации.

В процессе работы с BAAN, сотрудникам бывает необходима дополнительная информация по работе с системой, за которой они непосредственно обращаются в ОРИТ, где занимаются разработкой документации (инструкций) и обучением персонала работе в BAAN. Работник любой из служб путем запроса по телефонной линии связи оповещает о необходимости определенной инструкции. При этом в ОРИТе происходит поиск данной информации по всем шести рабочим местам, после чего, инструкция распечатывается и передается посредством курьера в службу. Однако, эти рутинные работы занимают немало времени как работников ОРИТ, так и сотрудников других служб.

В результате анализа бизнес-процесса обеспечения сотрудников ОАО «УМПО» справочными материалами по работе в системе BAAN были выявлены следующие недостатки:

– отсутствие полноценной справочной системы по работе в системе BAAN на ОАО «УМПО»;

– большая трудоемкость поиска необходимой информации;

– излишняя дублируемость информации.

Таким образом, имеем полное право утверждать, что на данный момент справочная система в BAAN не реализована.

Предложение по устранению выявленных недостатков

Для исключения вмешательства ОРИТ в процесс поиска инструкций рассмотрим предлагаемую систему поддержки работы пользователей в BAAN, при использовании которой нет необходимости ни в запросе по телефонной линии, ни в принтере для печати, ни в курьере для доставки. Все это заменяется архивом инструкций на сервере, где происходит непосредственно электронный поиск инструкций в созданной базе данных.

Итак, в обязанности ОРИТ, в данном случае, входит создание и корректировка инструкций в базе данных (точка зрения разработчика), а задачами служб будет создание запроса и работа с этой базой данных (точка зрения пользователя). Далее работник службы получает инструкцию в электронном виде по локальной сети с сервера и, по необходимости, распечатывает ее непосредственно на своем рабочем месте.

Результаты моделирования

На этапе моделирования системы построены мнемосхемы существующего и будущего бизнес – процессов, а так же средствами динамического моделировщика предприятия (Dynamic Enterprise Modeler), как одного из инструментов моделирования предприятия в ERP BAAN [5], был построен локальный классификатор. В данном случае использован иерархический метод классификации, где модули делятся на подмодули, каждый из которых в свою очередь содержит инструкции, отсортированные по определенной тематике с выделением ключевых слов и ответственных подразделений к каждой из них (рис. 1).

На основе локального классификатора, с использованием последовательного метода кодирования, получили пятиразрядную систему кодирования информации в

электронном архиве инструкций, а так же разработали информационную модель базы данных системы поддержки пользователей по работе в BAAN (рис. 2).

Модуль 1	Модуль 1.1	Модуль 1.1.1	Наименование инструкции	Ответственное подразделение	Ключевые слова в инструкции
WH Складирование	WH_1 Оператор центральных складов	WH_1_1 Комплект инструкций по учету движения материалов с центрального склада в цех	Бизнес-процесс по партионному учету материалов	Кладовщик	Материалы, склад, учет, партия
			Инструкция для бухгалтера (подтв выдачи мат с центр склада)	Бухгалтерия	Цех, центральный склад, выдача
			Инструкция для бухгалтера (подтверждение выдачи материалов и канцелярии)	Бухгалтерия	Цех, канцелярия, материалы, выдача
			...	...	...
	WH_2 Складирование между цехами перемещения деталей	-	Подтверждение заказов на перемещение	Бухгалтерия	Складской заказ, перемещение
			Инструкция по работе с отчетом «движение материалов»	Кладовщик	Материалы, отчет, склад
			...	...	...
	WH_3 Дополнительно	-	Инструкция для кладовщика СГД-0704	...	
			...		
QM Управление качеством	QM_PTC_1 Операционный контроль	...			
...	...				

Рис. 1. Организация архива инструкций по работе пользователей в BAAN на ОАО «УМПО»

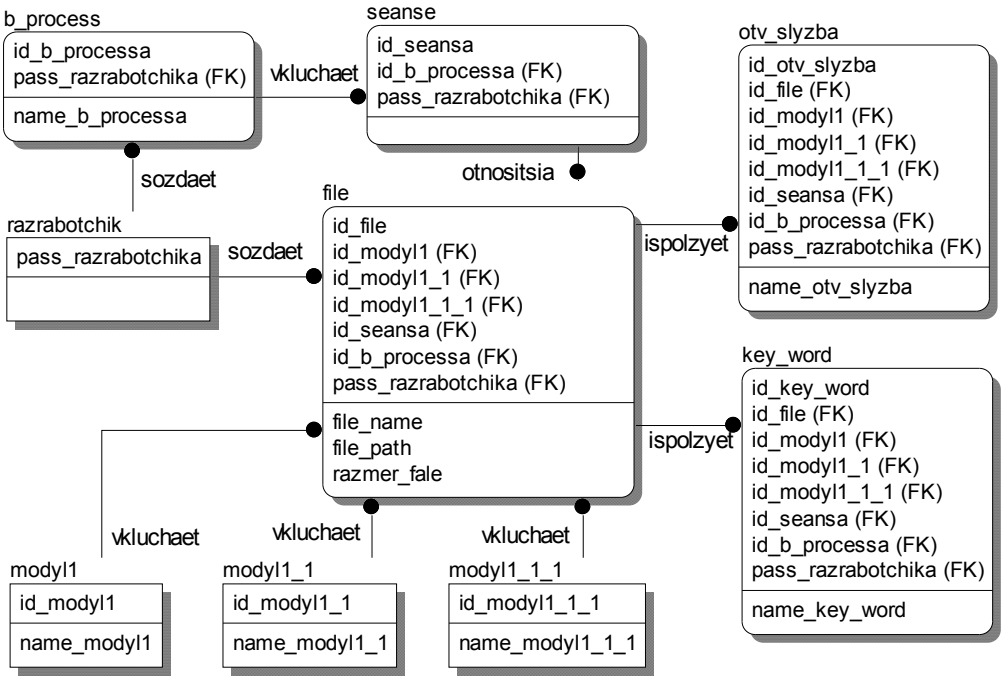


Рис. 2. Информационная модель службы поддержки пользователей по работе в BAAN

Так, для организации выполнения запросов пользователей в системе управления знаниями (далее СУЗ), каждому файлу инструкции по работе в BAAN соответствует свой список ключевых слов, ответственных служб и информация о разработчике данной инструкции. А для интеграции системы непосредственно с КИС BAAN, прописана информация о наименованиях, кодах сеансов и бизнес-процессов, к которым имеет отношение конкретная инструкция.

Отметим, что связь с разрабатываемой СУЗ осуществляется как с Web-портала предприятия, так и непосредственно из определенного сеанса BAAN с выдачей

информации по данному сеансу, включая как инструкции по работе в выбранной области, так и справочную информацию о разработчиках данного сеанса и связи с ними.

Основной результат

Составляющие разрабатываемой службы поддержки пользователей:

- авторизация пользователей;
- поиск инструкций по реквизитам: модулям и подмодулям, отделам и ключевым словам;
- наличие глоссария BAAN;
- организация «горячей линии»;
- доступ из системы поддержки пользователей к демоверсии сеансов BAAN;
- доступ из сеансов BAAN в систему управления знаниями;
- доска объявлений (информация об обучении пользователей BAAN).

Так же планируется реализация наиболее важного раздела для дальнейшего развития системы управления знаниями – раздела часто задаваемых вопросов, как основы развития экспертной системы по поддержке работы пользователей как в BAAN, так и на предприятии в целом. Таким образом, будет достигнут максимальный вывод из процесса обучения дополнительных пользователей работников ОРИТ.

Для реализации системы выбрано следующее программное обеспечение: средствами SQL разработана база данных (архив инструкций) [6], на языке PHP реализована поисковая система в интранете предприятия [7], а так же ведутся работы по интеграции созданного средствами SQL архива с КИС BAAN, написанной на языке программирования 4GL.

Преимуществом такого подхода является динамический характер разработанной справочной системы. Тесно взаимодействуя с пользователями BAAN, учитывая часто задаваемые вопросы, которые, в свою очередь, фиксируются на Web-портале разрабатываемой справочной системы, а так же изменения бизнес-процессов на предприятии, отделом разработки информационных технологий инструкции по мере необходимости дорабатываются, изменяются и создаются новые, заставляя тем самым «дышать» базу архива инструкций в SQL.

Заключение

Таким образом, при помощи СУЗ достигается:

– эффективное удовлетворение информационных потребностей пользователей BAAN;

– развитая организация динамической справочной системы, позволяющая выполнять разнообразные запросы;

– снижение затрат не только на хранение данных, но и на их поддержание в актуальном состоянии;

– уменьшение потоков данных, циркулирующих в системе, сокращение их избыточности и дублирования;

– значительное уменьшение временных рамок поиска необходимой информации.

По окончанию внедрения данной системы реализуется возможность доступа к справочной системе как посредством интеграции системы BAAN с архивом инструкций, так и с помощью доступа к системе с web-сервера ОАО «УМПО» с возможностью изучения новой информации, используя демонстрационный пример работы в системе, а так же с возможностью получения информации о специалистах-разработчиках.

В целях усовершенствования системы управления знаниями, планируется разработка экспертной системы на основе раздела «часто задаваемые вопросы» созданной справочной системы.

Отметим так же, что данная справочная система может быть использована как в BAAN, так и в иных корпоративных информационных системах для поддержки работы пользователей в среде конкретной КИС.

Таким образом, положено начало развития системы управления знаниями на ОАО «УМПО», что, несомненно, является выгодным, ведь не секрет, что таким образом упрощается повторное использование имеющихся знаний и создаются новые знания, позволяющие заметно усовершенствовать процессы принятия решений, что в свою очередь повышает конкурентоспособность предприятия в целом!

Литература

1. ИТ в промышленности. Управление знаниями [Электронный ресурс]/ Игорь Бойцов– Москва, 2003. – Режим доступа: http://www.ci.ru/inform15_04/p_22.htm, свободный. – Загл. С экрана. – Яз. рус., англ.
2. Вендров А.М. Проектирование программного обеспечения экономических информационных систем. – М., Финансы и статистика, 2002. – 352 с.
3. Дресвянников В.А. Управление знаниями организации: учебное пособие / В.А. Дресвянников. – М.: КноРус, 2008. – 344 с.
4. OLAP.RU. Управление корпоративными знаниями [Электронный ресурс]/ Дэниэл Е. О'Лири (Daniel E. O'Leary) – Москва, 2001. – Режим доступа: http://www.olap.ru/basic/k_management.asp, свободный. – Загл. С экрана. – Яз. рус., англ.
5. BAAN ERP.Учебные материалы по программе «Основы использования BAAN ERP» /Компания Альфа-Интегратор – М. – 2003. – 86 с.
6. Плю Р. Освой самостоятельно SQL за 24 часа: Учеб.пособие / Пер. с англ. – 2-е изд. – М.: Вильямс, 2000. – 352 с.
7. Гутманс Э. PHP 5. Профессиональное программирование / Э. Гутманс, С. Баккен, Д. Ретанс; пер. с англ. А. Киселева. – М.: СПб: Символ: Символ Плюс, 2006. – 701 с.

УДК 681.3

РЕАЛИЗАЦИЯ СИСТЕМЫ ВЫДАЧИ ПАСПОРТОВ С ПОВЫШЕННОЙ ЗАЩИЩЕННОСТЬЮ ОТ ПОДДЕЛКИ

Н.А. Аль-Маджмар
(Санкт-Петербургский государственный электротехнический университет, ЛЭТИ)
Научный руководитель – д.т.н., профессор Н.А. Молдовян
(Санкт-Петербургский государственный электротехнический университет, ЛЭТИ)

Рассматривается разработка системы изготовления и выпуска документов и ценных бумаг с повышенной защищенностью от подделки на основе алгоритмов электронной цифровой подписи. Показано, что введение алгоритмов электронной цифровой подписи в такие системы позволяет обеспечить повышенная защищенность от подделки.

Ключевые слова: электронная цифровая подпись, аутентификация информации, подделка документов

Введение

Алгоритмы электронной цифровой подписи (ЭЦП) [1, 2] могут быть положены в основу разработки систем изготовления и выпуска документов и ценных бумаг с повышенной защищенностью от подделки. Построение таких систем рассмотрим на основе примера построения системы выдачи паспортов повышенной защищенности от подделки.

Основная часть

В основе построения такой системы лежит техническое решение, связанное с применением ЭЦП для связывания конкретного бланка документа с конкретными данными, содержащимися в документе. Идея такого технического решения опирается на уникальности микротекстуры (микроструктуры) бумаги, из которой изготовлен конкретный бланк документа. При этом может быть использована технология изготовления бумаги для документов, такая, что в текстуру вносятся устойчивые случайные включения со случайным технологически невоспроизводимым распределением. (Этот факт важен для предлагаемой ниже технологии и системы, поскольку она требует стабильности уникальной микроструктуры бумаги).

Таким образом, предполагаем использование бумаги со стабильными случайными микровключениями и наличием портативного сканера с достаточной разрешающей способностью. Также предполагается, что на бланке наносится специальная метка, по которой сканер автоматически определяет положение площадке, подвергаемой сканированию для выявления уникального цифрового образа бланка, на котором изготавливается паспорт или другой документ.

Практическая невозможность подделки документа связана с формированием ЭЦП к сообщению, которое формируется как объединение цифрового образа конкретного бланка с конкретным содержанием документа, серией и номером документа [3] (а в случае паспортов сюда может быть включена также биометрическая информация о владельце паспорта). В результате появляется возможность проверить подлинность документа по ЭЦП, для чего используется коллективный открытый ключ одного, двух или более органов, подтверждающих своими подписями правомерность выпуска данного конкретного экземпляра документа и его подлинность.

ЭЦП наносится на документ в одном или двух заданных местах документа (возможно использование разных форматов фиксирования на бумаге значения ЭЦП), что обеспечивает ее постоянное наличие в документе. При проверке подлинности докумен-

та, например паспорта на границе, осуществляется сканирование цифрового образа документа, считывание информационного содержания документа (а если надо, то и биометрических данных владельца) составляется контролируемое сообщение и проверятся подлинность ЭЦП к этому контрольному сообщению. Эта технология делает практически невозможным подделку документов. При использовании этой технологии в области паспортизации возможности криминальных и террористических групп и элементов по их вредоносной скрытной деятельности значительно сужаются, что в целом будет благоприятствовать правопорядку в обществе.

Наличие нескольких органов, легализирующих выпуск документа, будет способствовать значительному снижению вероятности участия лиц, уполномоченных осуществить легализацию документов, в незаконном оформлении документов. Это обусловливается резким уменьшением вероятности того, что неблагонадежные должностные сотрудники получат одновременно полномочия по выпуску документов. Таким образом, в рассматриваемой технологии требуется наличие двух и более цифровых подписей к контролируемому сообщению. Ввиду того, что ЭЦП физически должна присутствовать на документе, то актуален вопрос о снижении суммарного размера всех ЭЦП. Это делает весьма перспективным разработанный протокол коллективной ЭЦП для применения в такой технологии [4]. Как было показано выше размер коллективной ЭЦП не зависит от числа подписывающих, поэтому число органов участвующих в процессе легализации документов может быть достаточно большим и позволить сделать практически невероятным неправомерный выпуск документов (например, выдача подлинных паспортов с нарушением принятых правил и процедур недобросовестными работниками официальных органов паспортно-визовой службы) рис. 1.

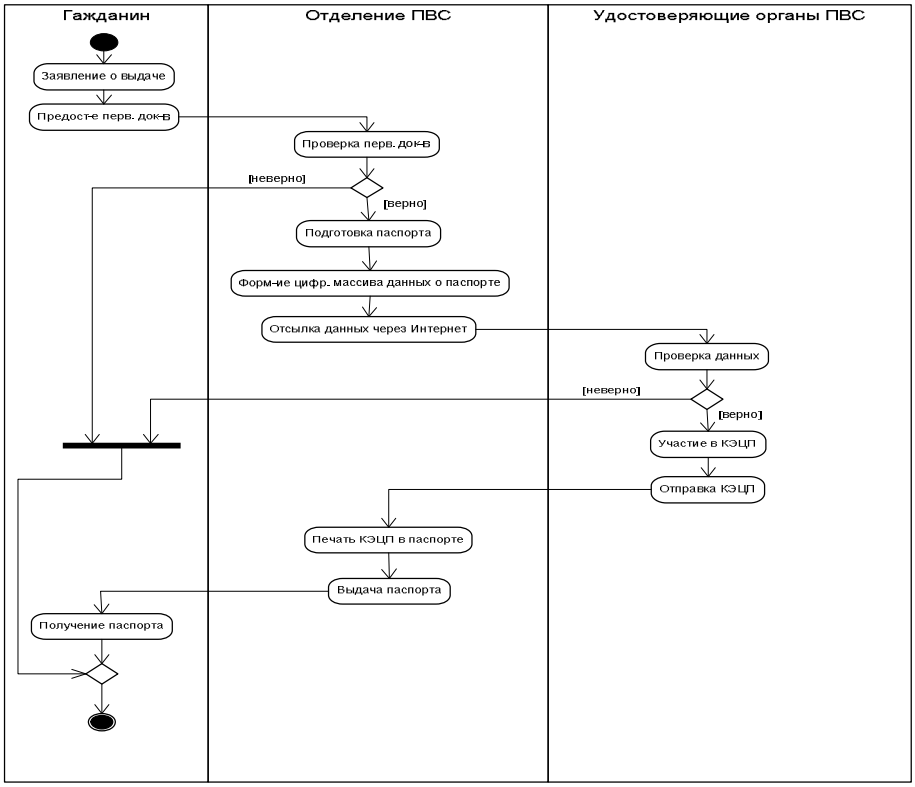


Рис. 1. Алгоритм процедуры изготовления и выдачи паспорта

Процедура выдачи паспорта реализуется в виде следующих шагов.

1. Обращение гражданина с заявлением о выдаче паспорта с предоставлением требуемого перечня первичных документов.
2. Проверка первичных документов.

3. Подготовка паспорта – внесение всех необходимых данных в виде текста и в кодированном виде для автоматического чтении данных при процедуре паспортного контроля. В кодированном виде также вносится контрольная информация о цифровом образе использованного бланка паспорта. Контрольная информация считывается специальными сканерами с заданного места в бланке.

4. Данные по гражданину и параметры контрольной информации о данном уникальном экземпляре паспорта объединяются по установленному правилу, в результате чего формируется единый цифровой массив данных о паспорте.

5. Данные по гражданину и указанный цифровой массив высылаются через Интернет (используется защищенный режим передачи данных) в удостоверяющие органы паспортно-визовой службы.

6. В паспортно-визовой службе осуществляется проверка данных и каждый из уполномоченных органов подтверждает правомерность выдачи паспорта путем участия в коллективной ЭЦП к цифровому информационному массиву.

7. Коллективная ЭЦП сформированная всеми уполномоченными органами отправляется в отделение ПВС, в которое обратился гражданин.

8. Полученная ЭЦП печатается в оговоренных местах паспорта, а паспорт выдается гражданину.

В эту достаточно схематично изложенную процедуру можно внести необходимую детализацию (снятие биометрических данных пользователя, занесение данных в чип паспорта и т.п.) каждого из шагов при разработке конкретной практической системы выдачи паспортов по данной технологии. Однако, эта схема процедуры выдачи паспортов достаточно ясно показывает использование уникального цифрового образа конкретного образца документа в сочетании с коллективной ЭЦП, что обеспечивает надежную защиту от подделки.

Процедура проверки подлинности паспорта включает:

1. сканирование образа паспорта и его оцифровывание;
2. формирование контрольного массива данных;
3. проверку подлинности коллективной ЭЦП с использованием открытого коллективного ключа уполномоченных органов ПВС, подтверждающих подлинность паспорта.

Заключение

Современные устройства сканирования достаточно надежны, миниатюрны и доступны по цене, поэтому предложенная технология защиты материальных документов от подделки перспективна для массового применения.

Литература

1. Молдовян А.А., Молдовян Н.А. Введение в криптосистемы с открытым ключом. – СПб. БХВ-Петербург, 2005. – 286 с.
2. Венбо Мао. Современная криптография. Теория и практика.– М., СПб, Киев. Издательский дом «Вильямс», 2005. – 763 с.
3. Молдовян Д.Н. Схема ЭЦП с проверкой подлинности по длине // В кн. Инновационная деятельность в вооруженных силах Российской Федерации. Труды всеармейской научно-практической конференции. СПб, 17–18 ноября 2005 г. СПб. – 2005. С. 196–199.
4. Аль-Маджмар Н.А., Гортинская Л.В., Щербаков В.А. Способ сокращения размера подписи в алгоритмах аутентификации, основанных на сложности факторизации. // Вопросы защиты информации. Москва, 2008. – №4. – С. 8–11.

УДК 004.738.52

АВТОМАТИЧЕСКАЯ ИНДЕКСАЦИЯ ТЕКСТОВЫХ ДОКУМЕНТОВ

Ю.А. Чернятина
Научный руководитель – к.т.н., доцент И.А. Бессмертный

В статье рассматриваются вопросы автоматического поиска, основанные на статистике используемых слов. Часто встречающиеся пары слов соединяются в цепи и строят «псевдосемантическую сеть». Граф псевдосемантической сети позволяет определить тематику документа на первый взгляд. Более или менее детальный граф делает содержание документа визуальным. Та же самая техника может быть применена к отдельному слову. Наличие компаньонов слова в предложениях во многих документах позволяет нам строить «портрет слова». Выбирая ветви графа, мы легко строим запрос поиска.

Ключевые слова: статистика слов, псевдосемантическая паутина, сетевая информация

Введение

Задача информационного поиска существовала с тех пор, как появились хранилища документов и библиотеки. В докомпьютерную эру идентификация документов была обязанностью авторов и библиотекарей. В настоящее время только научные бумаги помечаются ключевыми словами и лишь потому, что авторы заинтересованы в индексе цитирования. Все другие документы пополняют информационную среду без какой-либо разметки, облегчающей их поиск. Интернет-эра сделала доступными в он-лайн режиме миллиарды документов, в связи с этим задача информационного поиска приобрела особую актуальность. До появления мощных поисковых серверов (15–20 лет назад) популярностью пользовались Желтые страницы Интернета – напечатанные справочники сетевых ресурсов, упорядоченные по темам. Следующие 10 лет – это время поисковых серверов. История успеха Google – хороший тому пример. И последние (но не в последнюю очередь) 5 лет являются временем ожидания Семантической паутины.

Существующие методы маркировки

Ключевая идея Семантической паутины была объявлена 7 лет назад, и сразу же претерпела изменения, даже не успев быть реализованной в полной мере [1]. Основной проблемой развертывания Семантической паутины является необходимость смысловой идентификации документы вручную, причем без извлечения мгновенной выгоды.

В то время как ожидание Семантической паутины затягивается, мы можем попытаться улучшить разметку документов. Могут использоваться два подхода к идентификации документов: ручной и автоматический. Ручная разметка ключевыми словами весьма надежна, так как ключевые слова-признаки назначаются самим автором, если не принимать во внимание фактор субъективности; кроме того, документы иногда содержат скрытый смысл, не выраженный устно. Определенные ключевые слова отражают стилистическое предпочтение автора, которое может не соответствовать словарю поисковой машины.

Автоматическая индексация базируется на статистике используемых слов и словосочетаний. Типичный автоматически построенный индекс – это матрица размерностью M×N, где M – номер документов, N – размер словаря. Ячейки матрицы отражают использование слова в документе. Самый простой индекс хранит двоичные значения ячеек. Поиск документов в индексе заключается в нахождении отличных от нуля ячеек для задаваемых в поисковом запросе слов. Этот подход не применим к очень большим хранилищам документов, потому что релевантность документов будет также двоичной, что не позволит ранжировать выборку. Более сложные индексы учитывают

как частоту использования слова в документе, так и его редкость среди всех документов.

Наиболее известные неудобства этих автоматических методов индексации – синонимия и полисемия (многозначность). Синонимия приводит к потерям релевантных документов; многозначность наоборот возвращает нерелевантные. Некоторые вычислительные методы помогают частично устранить эти проблемы. Один из известных методов – латентный семантический анализ (Latent Semantic Analysis) и сингулярное разложение (Singular Value Decomposition) [2]. Это метод размывает индексную матрицу и сглаживает негативный эффект полисемии и синонимии.

Псевдосемантические сети

Выше мы рассмотрели способы неявного извлечения смысла документа на основе статистики встречаемости слов. Но при этом все слова рассматриваются по отдельности. Мы попытаемся связать слова в пары, если они часто встречаются вместе в предложениях. Каждая такая пара слов будет похожа на элемент семантической сети, показанной в рис. 1, но без предиката, который в семантических сетях определяет тип отношения между субъектом и объектом. Таким образом, мы только предполагаем наличие связи между словами, если они встречаются в одном предложении, но не можем определить тип связи (рис. 2).

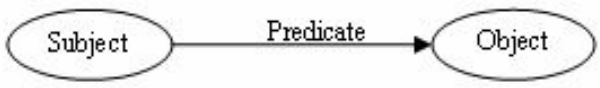


Рис. 1. Элемент семантической паутины

Рис. 2. Слова-компаньоны

Очевидно, такие пары могут образовать сеть, которую мы будем называть «Псевдосемантической Сетью». Таким образом, процесс маркировки (то есть создание псевдосемантической сети) состоит из следующих трех шагов.

1. Вычисление частотности слова в документе. Очевидно, предлоги и другие общие слова должны быть исключены. Кроме того, вариации слова (единственное / множественное числа, времена и т.д.), должны быть устранены.
2. Усечение (отбрасывание) малозначащих слов в списке. Проведенный анализ текстов показал, что здесь может быть применен принцип Парето (20% слов формируют 80% текста) и таким образом можно отбрасывать большую часть слов.
3. Вычисление статистики пар слов и построение индекса как множество триплетов (слово, слово, номер), где номер отражает частоту пар

После того, как псевдосемантическая сеть сформирована, мы можем построить граф. В принципе не имеет значения, с которого узла начинать развертывать граф, но опыт показывает, что использование наиболее встречаемого слова в качестве стартового узла позволяет размещать граф в двумерном пространстве более рационально. Иллюстрация 3 – скриншот программы.

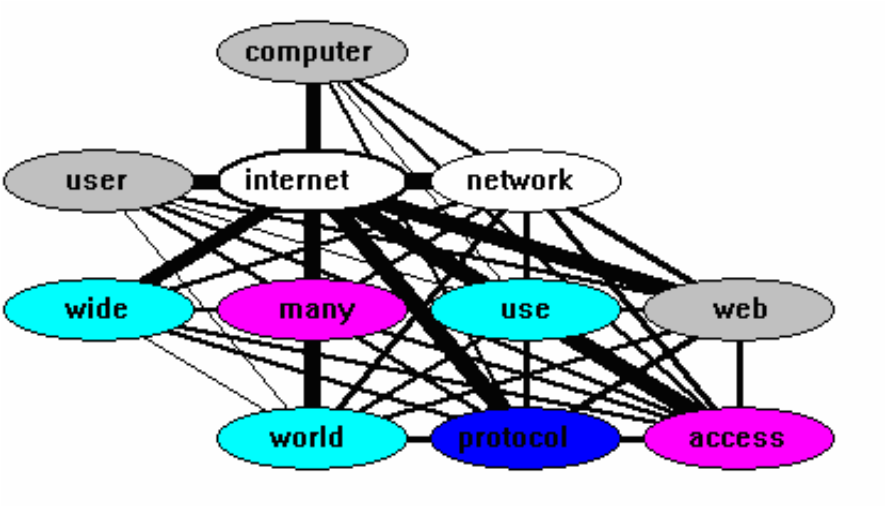


Рис. 3. Связь между словами

Представленный граф отображает статью "Internet" в Wikipedia. На этой картине различные цвета эллипсов кодируют различную частотность слова, и толщина линий отражает мощность связей. Этот пример демонстрирует, что некоторые слова образуют устойчивые (часто встречаются) пары, которые позволяют нам предполагать присутствие значащих связей. Преимущество визуального представления сети – быстрое распознавание семантики документа (если существует) на первый взгляд. Внутреннее представление индекса – множество триплетов (в примечании ПРОЛОГА) как это:

пара ("internet", "network ", 16).
пара ("work", "internet ", 7).
пара ("internet", "connect ", 6).
пара ("network", "user ", 5).
пара("internet", "user",4).
пара("network", "work",3).
…

Третий член каждого списка – встречаемость пары в документе.

Поиск документов

После того, как индекс построен, возникает другая проблема: как использовать индекс для поиска документов? Самый простой запрос поиска – ряд пар слов как это:

(internet, network), (internet, world), (world, wide), (wide, web)

Очевидно, написание такого запроса гораздо сложнее, чем просто указание списка ключевых слов. Кроме того отрицательный эффект синонимии в этом случае будет усилен. Следовательно, мы нуждаемся в поддержке процесса построения поискового запроса.

Статистика слов может также здесь помочь. На основе глобальной статистики пар слов, полученной на массе документов, можно построить портрет слова, выбранного как главное слово запроса поиска. Рис. 4 показывает часто используемые слова вместе с главным словом «network».

Для формирования запроса нам необходимо выбрать, какое слово должно быть поставлено в соответствие слову «network». Например, если нас интересуют сети передачи данных, то мы выбираем слово «data», которое гарантированно будет присутствовать в индексах документов, относящихся к сетям передачи данных. Далее мы должны получить портрет слова «data» и выбрать связи данного слова. Подобный подход используется в поисковом командном процессоре quintura.com. Отличие

заключается в том, выбранные слова в Quintura только пополняют список ключевых слов запроса без учета встречаемости пар слов.

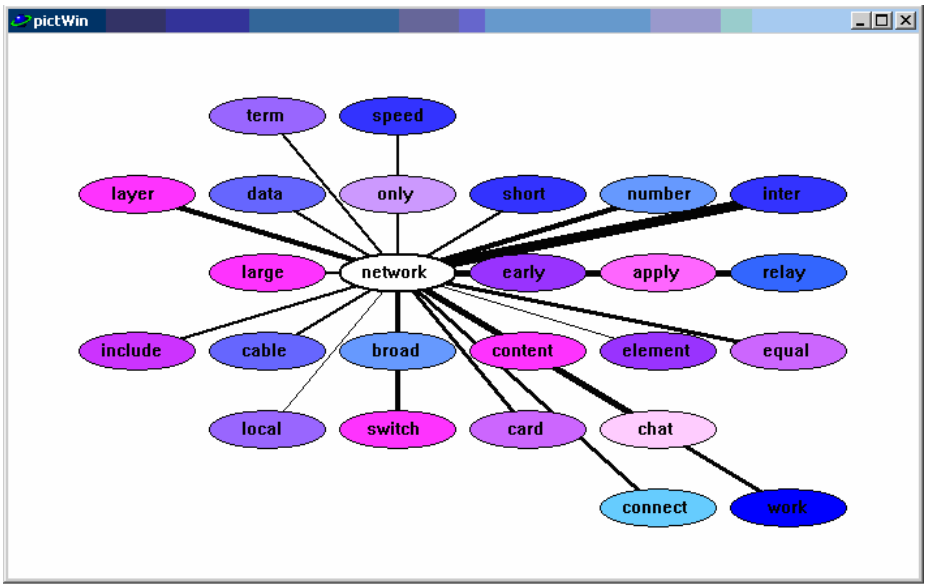


Рис. 4. Связь слов-компаньонов с главным словом

Исследовательский прототип программы индексации и поиска, использованной здесь для иллюстрации предлагаемых методов, написан в Visual Prolog 7.0. Основная цель этой программы – изучение поисковых методов в учебном курсе «Искусственный интеллект» на кафедре вычислительной техники СПбГУ ИТМО.

Литература

1. Nigel Shadbolt, Wendy Hall, Tim Berners-Lee. The Semantic Web Revisited. IEEE Intelligent Systems. – 2006.
2. S. Deerwester, Susan Dumais, G. W. Furnas, T. K. Landauer, R. Harshman (1990). "Indexing by Latent Semantic Analysis". Journal of the American Society for Information Science 41 (6): 391–407.

УДК 004.021

РЕАЛИЗАЦИЯ ПАРАЛЛЕЛЬНОГО АЛГОРИТМА ДЛЯ РЕШЕНИЯ ЗАДАЧИ О РАЗВОЗКЕ ГРУЗОВ С ПРИМЕНЕНИЕМ КЛАСТЕРИЗАЦИИ

В.Н. Поляков, Е.В. Болгова
(Оренбургский государственный университет)
Научный руководитель – к.п.н., доцент А.Е. Шухман
(Оренбургский государственный университет)

В данной статье рассматриваются методы решения задачи о развозке грузов, основанные на кластеризации и последующем приближенном решении задачи коммивояжера. Рассмотрены различные методы кластеризации, а так же методы оптимизации алгоритма с целью повышения эффективности работы параллельной программы. Проведен анализ реализации алгоритмов с использованием технологий OpenMP и MPI и приведены результаты сравнения эффективности работы алгоритмов.

Ключевые слова: задача коммивожера, методы кластерзации, параллельный алгоритм, граф, OpenMP

Введение

Рассмотрим практическую задачу со следующей постановкой: некая фирма по доставке питьевой воды обслуживает *n* потребителей. Для доставки воды используется *m* машин. Фирма предполагает улучшить качество обслуживания клиентов, для чего предполагается разработать информационную систему составления маршрута и графика доставки воды клиентам. Фактически, данная задача представляет собой задачу о развозке грузов.

Задача развозки – это транспортная задача по доставке мелкопартионных грузов из распределительного центра (базы, склада и пр.), множеству получателей, расположенных в районе развозки [1]. Отличительной чертой задачи развозки является движение транспортных средств по радиальным и кольцевым маршрутам.

Существует достаточно большое количество методов решения задачи развозки. Одним из наиболее популярных итерационных методов является метод Кларка-Райта. Суть метода заключается в том, чтобы, отталкиваясь от исходной схемы развозки, по шагам перейти к оптимальной схеме развозки с кольцевыми маршрутами. С этой целью вводится такое понятие, как километровый выигрыш. Результатом таких расчетов является матрица расстояний между объектами [1].

Однако этот метод не всегда обеспечивает требуемую точность расчетов, так как он базируется на предположении, что длина пути между объектами пропорциональна расстоянию между объектами. Иными словами, в их основе лежит принцип аппроксимации расстояний [1].

Для решения задачи о развозке грузов с учетом вышеперечисленных факторов используются методы расчета расстояний на сети: метод потенциалов, метод «мельницы». Эти методы позволяют обеспечить высокую точность расчетов. Результатом расчетов являются две матрицы – матрица расстояний и матрица указателей [2].

Приведенные выше методы для расчетов используют матрицы, что при увеличении количества вершин приводит к значительному увеличению требуемого объема оперативной памяти и, как следствие, либо к переполнению стека, что не позволит получить решение, либо к замедлению работы программы.

Задачу о развозке грузов можно также свести к задаче коммивояжера, так как необходимо осуществить доставку и вернуться на базу, то есть посетить каждый пункт только один раз. Применение высокопроизводительный вычислений позволит увеличить скорость работы, а использование других способов представления графов – уменьшить объем памяти.

Задача коммивояжера относится к классу NP-полных задач, и точное ее решение находится методом полного перебора, который для графов с большим количеством вершин занимает много времени [3]. Поэтому целесообразнее воспользоваться известными приближенными методами решения задачи: методом Кристофидеса [3] и методом Эйлера [3].

Разработка параллельного алгоритма

Основная идея решения поставленной задачи заключается в том, что множество всех пунктов назначения делится на некоторое количество частей (кластеров). Полученные части содержат примерно одинаковое количество пунктов назначения. Затем для каждого кластера рассчитывается маршрут с помощью решения задачи коммивояжера. Распараллеливание проведем с помощью библиотек OpenMP и MPI. Можно с уверенностью утверждать, что точность расчетов на сети напрямую зависит от точности расчетов на отдельных участках сети.

Набор входных данных

Определим набор входных данных и основные понятия, которыми будем пользоваться. Мы будем рассматривать город как ориентированный взвешенный граф (граф перекрестков), в котором вершинами являются перекрестки дорог, а ребра с весами – непосредственно дороги с указанными расстояниями.

Множество пунктов назначения представляется как список вершин с координатами. Каждая вершина характеризуется парой чисел, соответствующими географическими координатами.

Методы кластеризации

Рассматриваемый граф является плоским, следовательно, деление на подграфы можно осуществлять относительно положения вершин на плоскости. Метод основан на делении плоскости на четыре части по вертикали и горизонтали, каждая из которых при необходимости так же разбивается на части. Получившиеся кластеры представляют собой непересекающиеся множества вершин.

Другой метод основан на применении поиска в ширину. После выбора начальной вершины осуществляется поиск в ширину до тех пор, пока количество выбранных вершин не достигнет определенного числа. Это число определяется как отношение общего числа вершин к количеству машин.

Схема алгоритма

После применения метода кластеризации мы получаем некоторое число непересекающихся множеств вершин, следовательно, можно применить параллельные алгоритмы. Рассмотрим подробнее параллельную реализацию расчета маршрутов коммивояжера с использованием библиотеки MPI [4].

Так как вычисления производятся с несвязанными между собой матрицами большой размерности, то очевидно, что необходимо выполнить распараллеливание по данным, следовательно, выбрать модель SPMD [4].

Суть параллельного алгоритма заключается в следующем.

Нулевым процессом осуществляется считывание исходных данных. После чего выполняется расчет весов графа перекрестков и заполнение весов графа пунктов назначений, основанное на поиске кратчайших путей между каждой парой вершин с помощью алгоритма Дейкстры [5]. Далее осуществляется кластеризация графа перекрестков, и полученные кластеры пересылаются незанятым работающим процессам.

Каждый работающий процесс, получая данные, производит поиск маршрута коммивояжера по одному из методов и полученный результат выводит в файл. После завершения работы последнего процесса работа программы прекращается.

На рис. 1 приведена схема работы параллельного алгоритма.

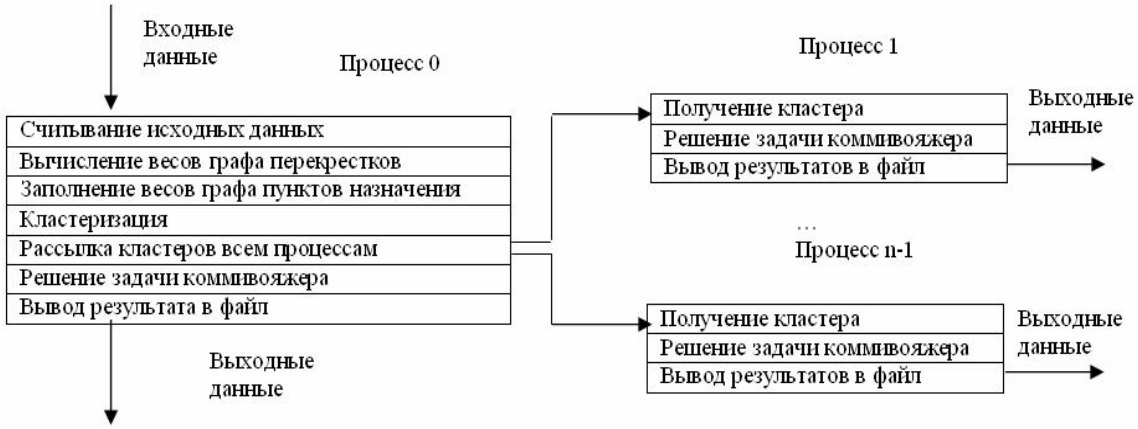


Рис. 1. Схема работы параллельного алгоритма

Для теоретической оценки эффективности распараллеливания воспользуемся законом Амдала [4]. В нашем случае доля последовательных операций f=0,55. Рассчитаем теоретическую эффективность распараллеливания для p=2 и p=8 по формуле. Таким образом, теоретически ожидаем получить ускорение производительности для двух процессоров 1,29, а для восьми – 1,65.

Оптимизация алгоритма

В первоначальной версии алгоритма в качестве структуры представления графов использовались матрицы смежности. Однако матрица смежности графа перекрестков является сильно разреженной и поскольку количество вершин графа велико, это приводит к нецелесообразному использованию памяти. Также в этом случае пересылка кластеров пусть и меньших размеров значительно замедляет работу алгоритма. Этот недостаток может быть устранен в случае использования списков смежности для графа перекрестков, что значительно сокращает объем используемой памяти. С другой стороны, списки смежности нецелесообразно использовать для полносвязного графа, так как объем используемой памяти практически не изменяется (в сравнении с использованием матрицы смежности), а работа алгоритмов даже замедляется. Это связано со сложностью операции поиска для матриц ($\Theta(n)$) [5] и списков($\Theta(\log m)$) [5]. Поэтому для представления графа пунктов назначений использовалась матрица весов.

В процессе работы алгоритма приходится сохранять и читать данные с жесткого диска. Как известно, эти операции замедляются, если данные являются текстовыми. Чтобы уменьшить время работы алгоритма некоторые данные хранятся в бинарных (двоичных) файлах. Работа с такими файлами осуществляется быстрее.

Анализ результатов

Тестирование проводилось на следующем наборе данных: ориентированный граф перекрестков с числом вершин 20000; граф пунктов назначения с числом вершин 100. Результаты представлены на рис. 2–5 в виде графиков зависимостей.

Зависимость времени работы алгоритмов с использованием библиотеки OpenMP от количества процессоров представлена на рис. 2.

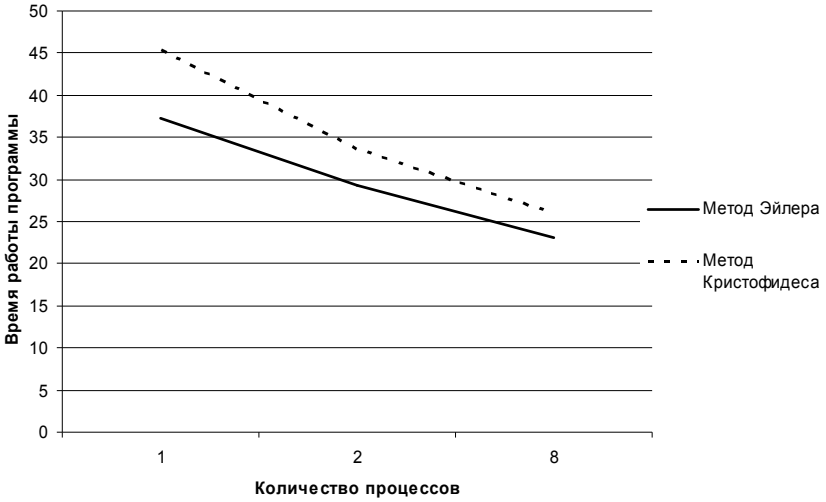


Рис. 2. График зависимости времени работы алгоритмов с использованием библиотеки OpenMP от количества процессоров

Зависимость времени работы алгоритмов с использованием библиотеки MPI от количества процессоров представлена на рис. 3.

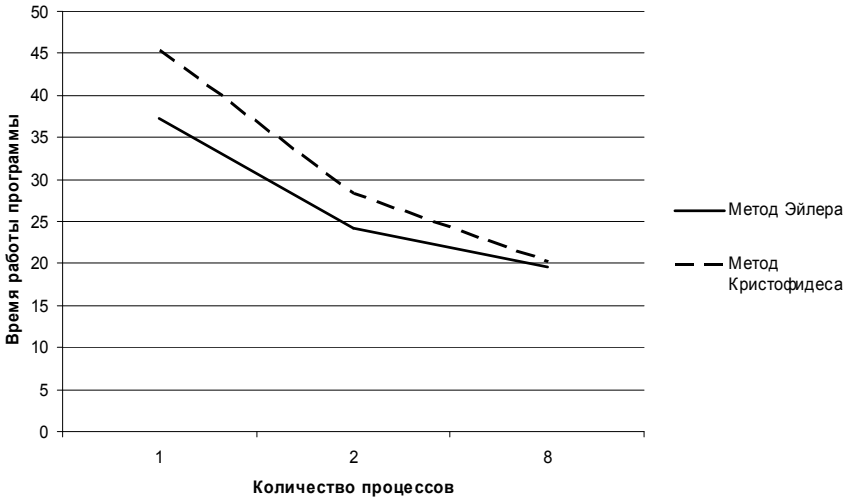


Рис. 3. График зависимости времени работы алгоритмов с использованием библиотеки MPI от количества процессоров

После применения оптимизации, описанной в пункте 2.4, удалось достичь следующих результатов: для метода Эйлера ускорение получилось $S_2 \approx 1{,}12$ $S_8 \approx 1{,}24$, а для метода Кристофидеса – $S_2 \approx 1{,}27$ $S_8 \approx 1{,}59$. Для более наглядного представления результатов на рис. 4 и 5 представлены графики зависимости теоретической оценки, рассчитанной по закону Амдала, эффективности работы программы без применения оптимизации и эффективности работы программы с применением оптимизации от количества процессоров.

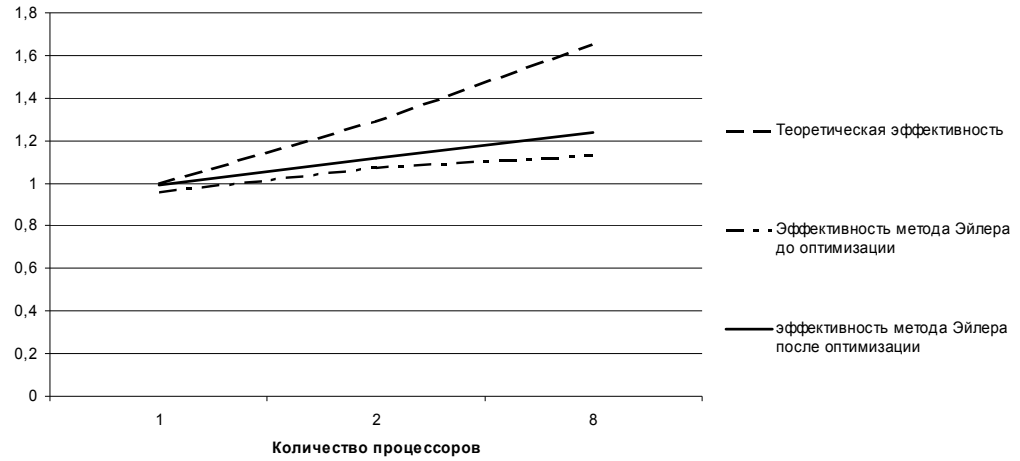


Рис. 4. Сравнительные графики зависимости эффективности работы метода Эйлера

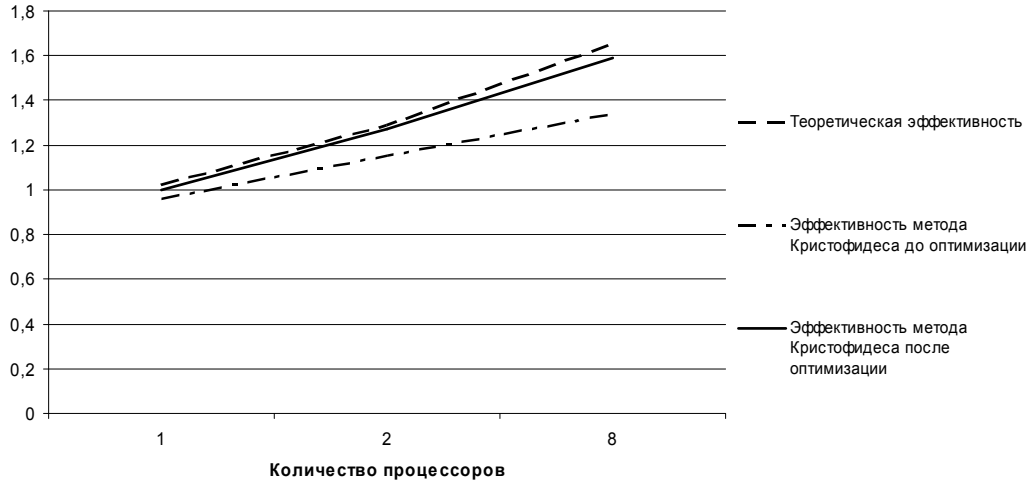


Рис. 5. Сравнительные графики зависимости эффективности работы метода Кристофидеса

Заключение

Анализ эффективности алгоритма показывает, что для решения задачи о развозке грузов следует использовать метод Кристофидеса, так как он имеет более высокий порядок точности по сравнению с алгоритмом Эйлера и эффективность работы алгоритма максимально приближена к теоретической. Следует отметить, что полученные результаты не являются окончательными и могут быть улучшены.

Итак, в данной статье был разработан параллельный алгоритм решения задачи о развозке грузов путем сведения ее к задаче коммивояжера. Так же были приведены примеры методов кластеризации и способы оптимизации самого алгоритма.

В дальнейшем предполагается модифицировать алгоритм для использования гибридной модели распараллеливания, уменьшить долю последовательных операций, реализовать графическую оболочку для наглядного представления результатов решения.

Литература

1. Бауэрсокс Д. Логистика: интегрированная цепь поставок. – М. – 2001 – 640 с.
2. Борю С.Ю., Каштанова И.А., Курапов С.В. Автоматизация решения задач на графах. – М. – 2002 – 10 с.
3. Кристофидес Н. Теория графов. Алгоритмический подход. – М. – 1978 – 432 с.

4. Антонов А.С. Параллельное программирование с использованием технологии MPI. Учебное пособие – М. – 2004. – 71 с.
5. Седжвик Р. Фундаментальные алгоритмы на C++. Алгоритмы на графах. СПб. – 2002. – 496 с.
6. Антонов А.С. Введение в параллельные вычисления: методическое пособие. – М.: Изд-во МГУ, 2002. – 69 с.

УДК 371.398

ОСОБЕННОСТИ АРХИТЕКТУРЫ ОБУЧАЮЩИХ СИСТЕМ ДЛЯ УЧЕНИКОВ МЛАДШИХ КЛАССОВ

А.А. Ахмадеева
Научный руководитель – к.т.н., доцент Н.Н. Горлушкина

Особенности архитектуры обучающих систем для учеников младших классов в соответствии с требованиями современного санитарного законодательства. Структура компьютерной обучающей системы с учетом характерных особенностей обучения учеников младших классов.
Ключевые слова: обучающая система, ученики, младшие классы

Введение

С каждым днем компьютеры все больше используются в различных сферах деятельности человека, образование не стало исключением. Создаются многочисленные обучающие компьютерные программы и приложения, предназначенные для обучения как взрослых, так и детей. Все больше создается обучающих программ для домашнего использования и интернет-ресурсов для самообучения или для обучения без прямого контакта с преподавателем.

Компьютерная обучающая система должна включать три основных блока:

- информационно-справочный блок;
- блок управления процессом обучения;
- блок контроля.

Все блоки должны учитывать характерные особенности учеников младших классов, то есть должно учитываться допустимое время пребывания ребенка за компьютером, индивидуальные особенности каждого ученика, также обучающая информация должна привлекать внимание детей и должна быть изложена в простой, понятной для ученика форме.

Большинство интернет-ресурсов, например, http://www.wunderkinder.narod.ru, http://children.kulichki.net, http://detskiy.nm.ru, http://novakovskiy.narod.ru/kids/kid.html, http://vip.km.ru/vschool, http://www.solnet.ee, ориентированных на младших школьников включают в себя информационно-справочный блок, некоторые из них также содержат блок самоконтроля, но отсутствует блок управления процессом обучения, который следил бы за последовательностью прохождения заданий и за временем занятия. Последнее условие очень важно, так как время пребывания за компьютером ограничено требованиями современного санитарного законодательства, следовательно, компьютерная обучающая система, а также ее содержание должны быть построены с учетом этих требований.

Информационно-справочный блок

Информационно-справочный блок можно представить в виде обучающей подсистемы, которая состоит из программ формирующих знания, умения и навыки. При заполнении информационно-справочного блока для учеников младших классов необходимо учитывать их особенности, связанные с потерей внимания к предмету, и формировать информацию таким образом, чтобы она давалась небольшими порциями.

Программы **формирующие знания** делятся на информационно-справочные и поисковые. Информационно-справочная система представляет собой программную оболочку, хранящую организованный набор теоретических сведений, терминов, развернутых пояснений к ним, обеспечивающая возможность поиска и выборки необходимой тематической информации и реализации запросов. Поисковой системой называется

программная оболочка, обеспечивающая возможность поиска необходимой информации в процессе обучения. Теоретические сведения информационно-справочной системы для учеников младших классов должны быть представлены в красочной форме в виде картинок и описаны простыми, короткими предложениями, понятными для данной аудитории, некоторая информация должна иметь звуковое сопровождение для повышения восприятия информации. Переход по информационно справочной системе должен осуществляться либо родителями, либо блоком управления процессом обучения.

Программы, **формирующие умения и навыки,** для учеников младших классов представляют собой генераторы заданий определенного типа по заданной теме, которые представлены в форме компьютерной игры. Они позволяют провести контрольную или самостоятельную работу, обеспечив каждому учащемуся отдельное задание, соответствующее его индивидуальным возможностям. Для учеников младших классов данные программы целесообразно представлять в **тренировочном типе**, когда за один из ведущих принципов берется подкрепление правильного ответа. Принцип заключается в том, что когда ученик отвечает на вопрос правильно, ему сообщается об этом, для учеников младших классов данное сообщение может быть представлено в виде красивой картинки и положительного звукового сигнала. Если ответ не правильный, ученику сообщается о том, что он ответил не правильно, в зависимости от формы задания сообщается, к какой категории относится выбранный ответ, и уточняется вопрос.

Блок управления процессом обучения

В блок управления процессом обучения входит тренирующая подсистема и подсистема, управляющая процессом чередования режимов обучения и перерывов.

Программы тренировочного типа предназначены преимущественно для закрепления умений и навыков. Предполагается, что теоретический материал уже усвоен. Тренирующая программа случайным образом генерирует задания по пройденным темам. Когда ученик отвечает на задание правильно, ему сообщается об этом, и в систему поступает сообщение, что тема пройдена успешно. Когда ученик отвечает не правильно, то ему даются ещё попытки до тех пор, пока он не найдет правильный ответ, при этом в базу данных поступает информация о количестве попыток, на основании которой, принимается решение о повторении проблемной темы. В следующий раз информационно-справочный блок начнется с повторения плохо изученной темы.

Создание подсистемы, управляющей процессом чередования режимов обучения и перерывов, может стать решением основной проблемы, связанной с определением промежутка времени, нахождения ребенка за компьютером.

Известно [1], что рекомендуемая непрерывная длительность работы, связанной с фиксацией взора непосредственно на экране монитора, на уроке не должна превышать:

- для обучающихся в I–IV классах – 10–15 минут;
- для обучающихся в V–VII классах – 15–20 минут;
- для обучающихся в VIII–IX классах – 20–25 минут;
- для обучающихся в X–XI классах на первом часу учебных занятий – 30 минут, на втором – 20 минут.

Оптимальное количество занятий с использованием компьютера в течение учебного дня для обучающихся I–IV классов составляет 1 урок, для обучающихся в V–VIII классах – 2 урока, для обучающихся в IX–XI классах – 3 урока.

В дошкольных образовательных учреждениях (ДОУ) рекомендуемая непрерывная продолжительность работы с компьютерами на развивающих игровых занятиях для детей 5 лет не должна превышать 10 минут, для детей 6 лет –15 минут.

Игровые занятия с использованием компьютеров в ДОУ рекомендуется проводить не более одного в течение дня и не чаще трех раз в неделю в дни наиболее высокой работоспособности детей: во вторник, в среду и в четверг. После занятия с детьми проводят гимнастику для глаз [1].

Основываясь на [1], в управляющей подсистеме через определенные промежутки времени, отведенные на обучение, проводятся перерывы. Во время перерывов компьютер, выступая в роли ведущего, озвучивает упражнения для глаз или физические упражнения. Экран во время перерыва становится темным, что позволяет гарантировать то, что ребенок отвернется от экрана.

Блок контроля

Контролирующий блок может состоять из программ с контролем в экспертной системе, тестирующих программ и программ, организующих самоконтроль. Контролирующие программы специально рассчитаны на проведение текущего или итогового опроса учащихся. Они позволяют установить необходимую обратную связь в процессе обучения, способствуют накоплению оценок, дают возможность проследить успеваемость каждого учащегося, соотнести результаты обучения с трудностью предлагаемых заданий, индивидуальными особенностями обучаемых, предложенным темпом обучения, объемом материала, его характером. В условиях компьютерного обучения, за счет систематической и продуктивной обратной связи, появляется возможность построения индивидуальной программы обучения для отдельного ученика, которую легко корректировать.

Исследованию проблемы обратной связи посвящена работа [2]. Опираясь на [2], в обучающей системе для учеников младших классов обратная связь осуществляется с помощью тренирующих и контролирующих тестов в игровой форме, а также с помощью веб-камеры.

Для тех, у кого есть веб-камера, существует возможность «контролировать» поведение ребенка во время перерыва. Пока ребенок не встанет из-за компьютера занятие в перерыве не начнется. Также не начнется занятие после перерыва, если ребенок сел за компьютер раньше положенного срока или ещё не успел подойти к компьютеру после перерыва, что позволит гарантировать, что обучение не начнется без учащегося.

Во время обучения некоторые тестовые занятия могут проводиться с помощью веб-камеры. Например, ребенку сначала показали цвета и как они называются, затем предлагают походить по комнатам и принести предмет указанного цвета. Ребенок показывает этот предмет камере, она устанавливает правильного цвета предмет или нет. Ещё один пример, урок был посвящен геометрическим фигурам, ребенку предлагается пойти, поискать предметы, которые похожи на определенную фигуру, или нарисовать на листке бумаги и показать камере.

Заключение

Компьютерные обучающие системы для учеников младших классов должны быть построены таким образом, чтобы информационно-справочный, тренирующий и контролирующий блоки были представлены в интересной для детей, непринужденной игровой форме.

Обратная связь и блок управления обучением должны быть построены таким образом, чтобы процесс обучения корректировался для каждого ученика индивидуально, в зависимости от его успеваемости, индивидуальных особенностей, реакций на трудность предложенных задач, темп обучения, объем и характер материала.

В блоке управления обучением обязательно должно учитываться время непрерывного нахождения обучающегося за компьютером, должны проводиться перерывы в обучении, а также количество обучающих сеансов в день должно быть ограничено в соответствии с [1].

Литература

1. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы: Санитарно-эпидемиологические правила и нормативы СанПиН 2.2.2 / 2.4.1340-03 // Безопасн. жизнедеятельности. – 2005.
2. Лукьяненко О.Д. Технологическое обеспечение обратной связи в дидактическом информационном взаимодействии педагога с детьми 6–7 лет: Диссертация... кандидата педагогических наук. – Армавир. – 2007. – 199 с.
3. Горлушкина Н.Н. Педагогические программные средства. Учебное пособие. Под ред. М.И. Потеева. – СПб: СПб ГУ ИТМО, 2003. – 136 с.

УДК 004.627

СЖАТИЕ ИЗОБРАЖЕНИЙ С ПОТЕРЕЙ КАЧЕСТВА С ПРИМЕНЕНИЕМ АДАПТИВНОГО КВАНТОВАНИЯ

Ю.В. Лужков

Научный руководитель – д.т.н., профессор А.Ю. Тропченко

Исследована проблема квантования спектральных коэффициентов в схемах сжатия изображений с потерей качества. Предложен метод вычисления значений коэффициентов вектора квантования, основанный на использовании весового критерия. Проведено сравнение базовой схемы JPEG и ее модификации на основе разработанного метода. Данная модификация превосходит схему JPEG на 10–20%.

Ключевые слова: сжатие изображений, адаптивное квантование, весовой критерий, JPEG

Введение

Среди наиболее эффективных схем сжатия изображений – схемы, использующие спектральные преобразования исходного сигнала. К таким преобразованиям можно отнести дискретное косинусное преобразование (ДКП), дискретное вейвлет-преобразование (ДВП), преобразование Карунена-Лоэва и некоторые другие. Схемы сжатия на их основе включают процедуру скалярного квантования спектральных коэффициентов. В связи с этим актуальной становится проблема адаптивного выбора шага квантования. В простейшем случае исходный сигнал разбивается на блоки одинакового размера, и для квантования всего сигнала используется вектор квантования, совпадающий по размерности с окном сканирования. Такой подход используется, в частности, в JPEG (Joint Photographic Experts Group) [1].

На сегодняшний день известно несколько методов определения векторов квантования коэффициентов спектра. С. Ву и А. Гершо в работе [2] предлагают метод на основе пошагового изменения его значений. Изначально все коэффициенты инициализируются максимальными значениями. На каждом шаге производится уменьшение одного из коэффициентов на некоторую величину. Поскольку оптимизация вектора проводится только в направлении уменьшения коэффициентов, ее можно назвать *однонаправленной*.

Х. Фунг и К. Паркер в работе [3] предлагают *двунаправленный* метод оптимизации. Его основное отличие от метода Ву-Гершо заключается в том, что на очередном шаге коррекция коэффициента может производиться как в сторону уменьшения его значения, так и в сторону увеличения.

В работе [4] предлагается метод вычисления вектора квантования, основанный на RD-оптимизации. Схема имеет принципиальное отличие от пошаговых однонаправленных и двунаправленных схем: вычисление значений вектора квантования проводятся сразу для многих значений битрейта R или значений искажения D, а выбор нужного набора коэффициентов осуществляется в самом конце из множества вариантов.

Все описанные схемы используют в качестве оценки битрейта *энтропийную функцию*, аппроксимирующую результат сжатия. Поскольку битрейт в значительной степени зависит от применяемых методов вторичного сжатия (например, статистического кодирования или кодирования длин серий), энтропийная функция не является универсальной и должна определяться для конкретной схемы сжатия.

В данной работе предлагается метод вычисления вектора квантования, не использующий энтропийные оценки. Он основан на сборе статистической информации о сигнале, которая оценивается с помощью специального критерия. Коэффициенты вектора квантования вычисляются в соответствии со значениями данного критерия. Благодаря

этому, алгоритм вычисления вектора является универсальным и может быть использован во многих схемах компрессии без существенных изменений.

Вычисление вектора квантования на основе весового критерия

Известно, что энергия сигнала распределяется между спектральными коэффициентами неравномерно. Более того, существует выраженная зависимость распределения энергии от номера спектральной позиции в окне сканирования. Идея предлагаемого метода заключается в том, чтобы квантовать коэффициенты на данной спектральной позиции *n* с *шагом квантования* Δ, значение которого зависит от степени значимости этой спектральной позиции с точки зрения распределения энергии спектра. Таким образом, необходимо определить функцию шага квантования $\Delta(\vec{z},n)$, где $\vec{z}$ – вектор спектральных коэффициентов.

Чтобы оценить значимость каждой спектральной позиции *n* для всех *M* блоков с номерами $m = 0,1,\ldots M-1$, вводится специальный весовой критерий *T*. В работе [5] рассмотрено несколько способов его задания и отмечено, что в ряде случаев выгоден способ вычисления критерия на основе максимальных амплитуд спектральных коэффициентов $z_{n,m}$:

$$T_n = \max\left|z_{n,m}\right|. \qquad (1)$$

Пример зависимости величины критерия *T* (его значения упорядочены по убыванию) от номера позиции *n* приведен на рис. 1. Сплошная линия соответствует составляющей яркости Y, пунктир – хроматическим составляющим Cb и Cr.

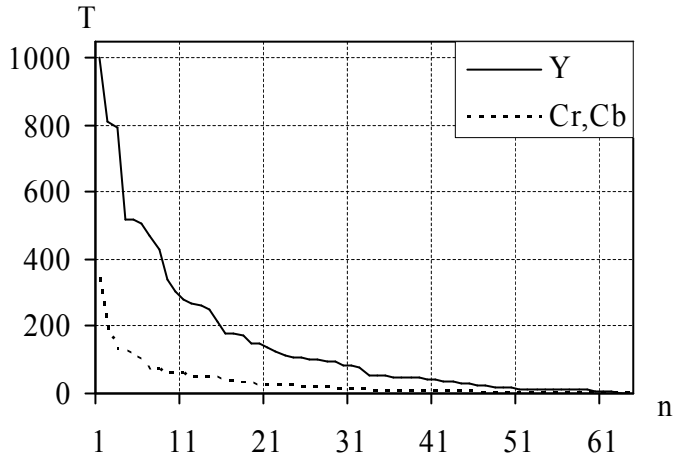


Рис. 1. График зависимости $T(n)$

Рассмотрим вопрос определения функции шага квантования $\Delta(\vec{z},n)$. Пусть её значения должны быть ограничены диапазоном $[a_1,a_2]$, $0 \le a_1 < a_2$. Введём функцию от *T*:

$$E(\hat{T}) = a_1 + \frac{\hat{f}(T_{\max}) - \hat{f}(T_n)}{\hat{f}(T_{\max}) - \hat{f}(T_{\min})}(a_2 - a_1), \qquad (2)$$

где $\hat{f}$ – корректирующая функция.

Поскольку любой T_n в общем случае зависит от всех элементов исходного спектрального вектора $\vec{z}$, функция *E* также зависит от $\vec{z}$. Фактически, это есть функция шага квантования сигнала $\Delta(\vec{z},n)$. Введем обозначение $f(\vec{z},n) = \hat{f}(T_n)$. Тогда формула (2) окончательно принимает вид:

$$\Delta(\vec{z},n) = \Delta(T) = a_1 + \frac{f(\vec{z},n_{\max}) - f(\vec{z},n)}{f(\vec{z},n_{\max}) - f(\vec{z},n_{\min})}(a_2 - a_1). \qquad (3)$$

Результаты сжатия тестовых изображений «Baboon» и «Peppers» представлены на рис. 2. Сплошные линии соответствуют базовой схеме JPEG, пунктир – модифицированной схеме, шаг квантования в которой вычисляется по формуле (3) с использованием критерия максимальных амплитуд (1).

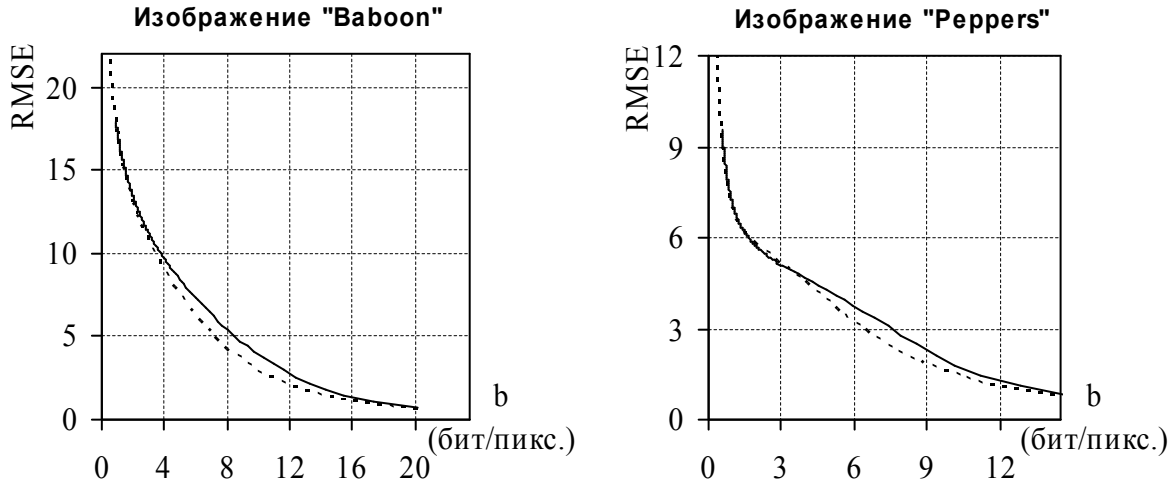
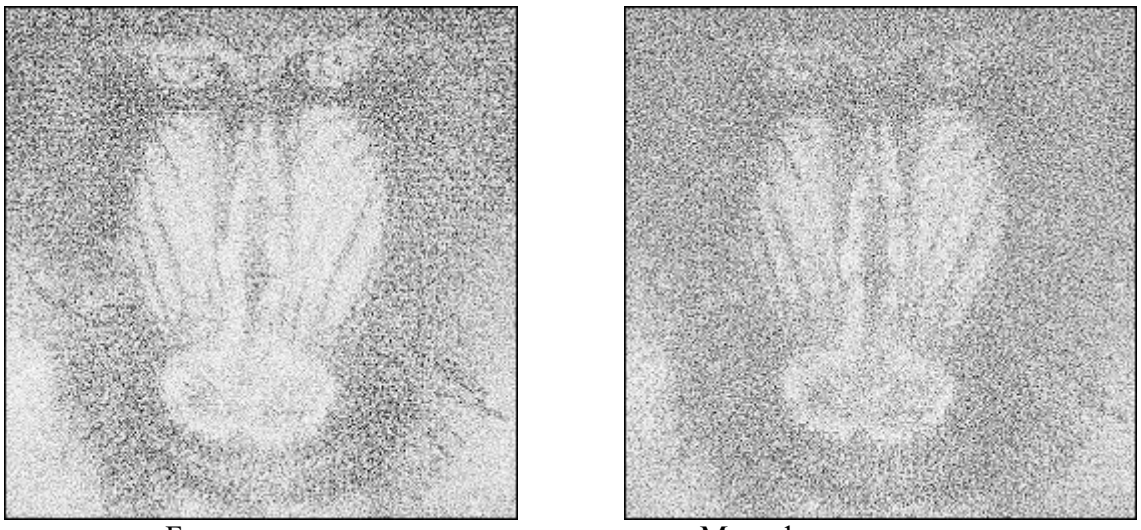


Рис. 2. Результаты компрессии тестовых изображений

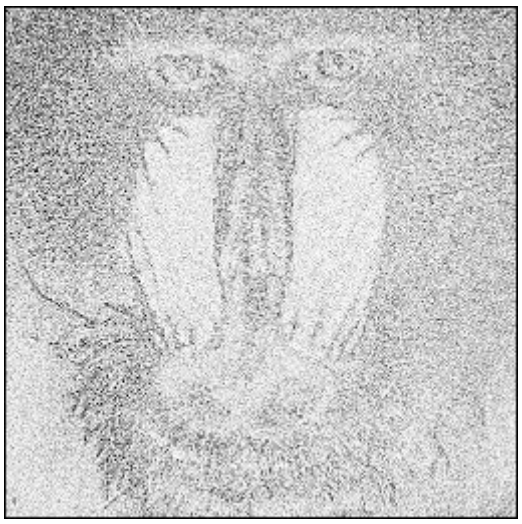
Для визуальной оценки качества сжатия рассмотрим разностные изображения. На рис. 3 и рис. 4 приведены разностные изображения для двух цветовых плоскостей. Изображения слева соответствуют стандартной схеме JPEG, справа – модифицированной схеме на основе весового критерия.



Базовая схема Модифицированная схема

Рис. 3. Разностные изображения для цветовой плоскости Y

Разностные изображения получены вычитанием восстановленного рисунка Q из исходного изображения P для каждого i-го пикселя: $D_i = 255 - a|P_i - Q_i|$, где a – коэффициент масштаба. При этом чем темнее пиксель разностного изображения, тем больше ошибка. Как видно, высокочастотные области изображений, сжатых по модифицированной схеме, искажены незначительно, что обусловлено адаптивным выбором шага квантования для разных частот.



Базовая схема

Модифицированная схема

Рис. 4. Разностные изображения для цветовой плоскости Cb

В таблице приведены численные результаты сжатия для четырех тестовых изображений. Как видно из представленных данных, при использовании модифицированной схемы размер файла сокращается до 15%.

Таблица. Результаты экспериментов

Изображение	Базовая схема JPEG		Модифицированная схема		Сокращение размера файла, %
	Размер файла, байт	RMSE	Размер файла, байт	RMSE	
«Lena»	131246	3.449	127745	3.436	3
«Baboon»	303617	4.399	263066	4.382	15
«Peppers»	223219	3.33	195510	3.321	14
«Oldman»	14150	2.668	12178	2.67	16

Выигрыш в сжатии особенно значителен для изображений, на которых присутствуют разные, не всегда однородные участки, соответствующие различным частотным составляющим.

Основные результаты и выводы

Предложен метод вычисления векторов квантования на основе весового критерия. Представлены экспериментальные данные для ряда тестовых изображений, также приведены разностные изображения для визуальной оценки ошибки компрессии, проведен анализ полученных результатов. Показано, что наибольший выигрыш при использовании предложенного метода в схеме JPEG может быть получен для коэффициентов сжатия от 2 до 10. Предложенный метод позволяет сократить размер сжатого файла в среднем на 10-15 % по сравнению с неадаптивными схемами. При использовании разработанного метода в схеме JPEG необходимо внести изменения только в программу сжатия. Для декомпрессии изображений достаточно использовать стандартный JPEG-декомпрессор.

Литература

1. Wallace G.K. The JPEG still picture compression standard // IEEE Trans. Consumer Electronics. – 1992. – Vol. 38, N 1. – P. 18–34.
2. Wu S.W., Gersho A. Rate-constrained picture-adaptive quantization for JPEG baseline coders // IEEE International Conference on Acoustics, Speech, and Signal Processing. – 1993. – Vol. 5. – P. 389–392.
3. Fung H.T., Parker K.J. Design of image-adaptive quantization tables for JPEG // J. of Electronic Imaging. – 1996. – Vol. 4, N 2. – P. 144–150.
4. Ratnakar V., Livny M. RD-OPT: an efficient algorithm for optimizing DCT quantization tables // Proceedings of the Conference on Data Compression. – 1995. – P. 332–341.
5. Лужков Ю.В. Метод адаптивного скалярного квантования в схемах необратимого сжатия изображений // Известия вузов. Приборостроение. – 2009. – Т. 52, Вып. 3. – С. 12–16.

УДК 004.434

ОБЗОР МЕТОДОВ ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ, ОСНОВАННЫХ НА ОБМЕНЕ СООБЩЕНИЯМИ

Р.И. Попов
Научный руководитель – к.т.н., доцент А.Е. Платунов

Альтернативой потоковой модели с общей памятью является модель параллелизма, основанная на обмене сообщениями. В статье рассмотрены современные языки и методы программирования, ориентированные на обмен сообщениями. В качестве примера используются функциональный язык Erlang, разработанный для использования в телекоммуникационных системах и более традиционный (императивный) язык Scala, предназначенный для Java платформы.

Ключевые слова: параллельное программирование, обмен сообщениями, надежность, erlang, scala

Введение

Традиционно, в программировании существуют две модели параллелизма: с общей памятью (shared memory) и основанная на обмене сообщениями (message passing). Большинство существующих языков используют модель с общей памятью, как более близкую по своей семантике к машинным инструкциям. Лишь некоторые языки построены на основе обмена сообщениями, к этой группе относятся Erlang, Scala, Occam и Oz.

В модели параллелизма, основанной на обмене сообщениями, постулируется: общей памяти нет, все вычисления должны производятся в изолированных процессах. Единственный способ обмена информацией – асинхронный обмен сообщениями. Такой подход избавляет разработчика от трудно обнаруживаемых ошибок: взаимных блокировок и состояний гонок, свойственных потоковой модели. Помимо этого, обмен сообщениями между процессами дает дополнительные возможности для увеличения надежности и масштабируемости разрабатываемых систем.

На сегодняшний день разработано множество способов борьбы с взаимными блокировками и гонками в приложениях с общей памятью. Наверное, лучший и наиболее широко используемый из них – транзакционная память, и её современная реализация в виде популярных систем управления базами данных. Специалистами по параллельному программированию предложены множество паттернов и программных каркасов, решающих традиционные задачи распараллеливания вычислений. Тем не менее, общая память остается узким местом, ограничивающим производительность основанных на ней систем.

Уже сейчас становятся актуальными задачи создания распределенных систем, не попадающих под существующие шаблоны. Наш мир параллелен, и эта параллельность не основана на общей памяти. Мы обмениваемся сообщениями: звуковыми и световыми сигналами, обновляем наше внутреннее состояние и принимаем решения к действию на основе полученных данных. Природа – живой пример сложной распределенной системы, построенной на принципах обмена сообщениями. Муравейник и пчелиный рой, являются образцами систем, где множество достаточно простых организмов коллективно решают сложные задачи, не прибегая при этом к использованию общей памяти. Инженерам уже сейчас приходится решать подобные задачи, а с развитием искусственного интеллекта, сенсорных сетей, нанотехнологий их доля будет только увеличиваться.

Обзор языка Erlang

Язык, ориентированный на параллельное программирование (в том числе для распределенных систем) и реализующий модель обмена сообщениями должен отвечать следующим требованиям [1]:

- На уровне языка должна быть реализована модель управления процессами. Под процессом можно понимать программу, исполняющуюся в независимой виртуальной машине.
- Несколько процессов, выполняющихся на одном компьютере, должны быть строго изолированы. Ошибка в одном процессе не должна влиять на работу других процессов, только если это не предусмотрено явно.
- С каждым процессом должен быть связан уникальный идентификатор, используя который можно обращаться к данному процессу. Между процессами не должно быть общей памяти. Единственный способ взаимодействия – обмен сообщениями.
- Передача сообщений между процессами считается ненадежной, нет гарантии доставки сообщения.
- Если один из процессов прекращается с ошибкой, другие процессы должны иметь возможность получать уведомления об этом событии и причинах возникновения ошибки.

Разработчики языка Erlang называют подход, отвечающий этим требованиям, параллельно-ориентированным программированием (Concurrency Oriented Programming, COP). Математическая модель, основанная на этих положениях, называется *акторной моделью* [2]. Под актором понимается универсальная единица параллельных вычислений: в ответ на полученное сообщение актор принимает решения, создает другие акторы, посылает сообщения. Впервые акторная модель предложена в 1973 году Карлом Хьюиттом, профессором Массачусетского технологического института [3].

Сложные системы, реализованные в рамках этой парадигмы, могут состоять из тысяч параллельно выполняющихся процессов. Программистам, знакомым с параллельным программированием, известно, что создание процессов операционной системы дорого, также значительного времени требует переключение контекста процессов. Решение этой проблемы предложено в функциональном языке Erlang. Одна из основных концепций функционального программирования – неизменяющиеся данные. Переменная, назначенная один раз, уже не может быть переопределена. Таким образом, сама семантика функционального программирования защищает данные разных процессов, следовательно, несколько процессов могут работать в одном контексте. Создание процессов в Erlang очень дешево. На моем компьютере (Intel Core 2 Duo 2.3Ghz, 3Gb ОЗУ) в случае создания 200000 процессов, создание одного процесса занимает 2.7 мкс процессорного времени.

Язык Erlang поддерживает механизмы обмена сообщениями на уровне синтаксиса, что делает его использование гораздо более удобным, чем использование библиотечных реализаций обмена сообщениями, таких как MPI [4]. У каждого процесса в Erlang есть буфер (mailbox) для хранения принятых сообщений. Для отправки сообщения используется конструкция:

Pid ! Message

где Message – отправляемое сообщение, а Pid – идентификатор процесса, которому предназначается данное сообщение. Для приема сообщений используется следующая конструкция:

receive ... end

Для выборки сообщений из буфера используется проверка на соответствие шаблону. На рис. 1 процесс C принимает сообщения от процессов A и B. Сообщение типа 'foo' обладает приоритетом над сообщениями типа 'bar'.

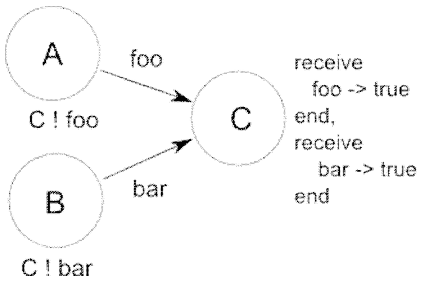


Рис. 1. Прием сообщений в соответствии с приоритетом

Чтобы процесс имел возможность ответить на сообщение, сообщение нужно снабжать адресом отправителя. На рис. 2 процесс A отправляет сообщение процессу B, процесс B передает сообщение от A процессу C. Процесс C отвечает процессу A.

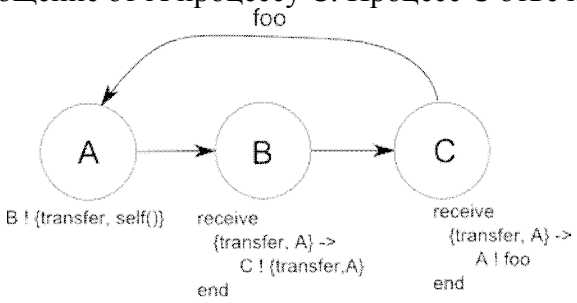


Рис. 2. Передача сообщений с адресом отправителя

В качестве примера программирования на Erlang рассмотрим решение «Santa Concurrency Problem» [5] предложенное Ричардом А. О'Кеффи [6].

Санта Клаус спит в своем доме на северном полюсе, и может быть разбужен, только если все девять северных оленей вернуться из своего отпуска с тропических островов в Тихом океане, или, если нескольким эльфам потребуется помощь с изготовлением игрушек. Если проблемы возникнут только у одного эльфа, тогда это не достаточно серьезная причина, чтобы будить Санту, поэтому эльфы всегда приходят к дому Санты втроем. В то время, пока трое эльфов решают вместе с Сантой свои проблемы, любые другие эльфы, которым также требуется помощь от Санты, должны ждать, пока вернуться предыдущие трое. Если Санта просыпается и обнаруживает, что три эльфа ждут его у двери, но в то же время последний из оленей вернулся из отпуска, он решает, что эльфы могут и подождать, ведь гораздо важнее приготовить сани к наступлению Рождества. (Предполагается, что олени не хотят покидать тропики, и пытаются оставаться там до последнего момента. Они бы рады совсем не возвращаться, но Санта оплачивает все их счета...)

Архитектура решения задачи на Erlang выглядит следующим образом:

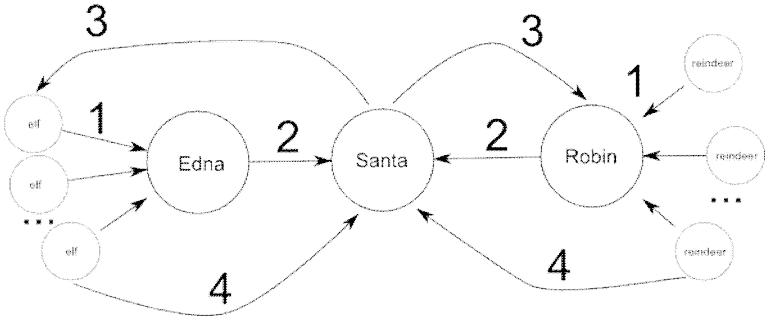


Рис. 3. Последовательность передачи сообщений в решении «Santa Concurrency Problem»

- Создается процесс Santa, который ожидает, пока кто-нибудь пришлет ему сообщение со списком оленей {reindeer,[R1,...,R9]} или эльфов {elves,[E1,E2,E3]}, собравшихся в группу. Используются две вложенных конструкции receive: первая принимает группу оленей, не зависимо от числа ожидающих эльфов, вторая, вложенная, принимает группы любого типа, т.к. может возникнуть такая ситуация, что сразу две группы оленей ожидают Санту. Санта ничего не знает о других процессах; он может только посылать сообщения оленям или эльфам, т.к. их идентификаторы находятся в принимаемых им сообщениях. После получения списка группы он отправляет свой идентификатор каждому члену группы и ждет от них ответа (барьерная синхронизация), после этого процесс повторяется.
- У Санты есть два секретаря (отдельные процессы). Эдна – секретарь, занимающийся эльфами. Когда она собирает группу из трех эльфов, она отправляет их список Санте. Робин, секретарь занимающийся оленями, собирает аналогичный список из девяти оленей.
- Каждый эльф это тоже процесс. Он посылает свой идентификатор Эдне и затем ожидает приглашения от Санты. После получения приглашения он совершает требуемые ему действия и отправляет Санте сообщение о том, что закончил. Эльф знает только идентификатор Эдны, остальные идентификаторы ему не известны.
- Олени отличаются от эльфов только тем, что знают идентификатор Робина, но не знают идентификатор Эдны.

Решение проблемы на Эрланге не требует никаких экзотических управляющих структур и структур данных, используется только простой обмен сообщениями. Для сравнения, решение в рамках потоковой модели, требует использования как минимум 10-ти семафоров.

Методы увеличения надежности

Первая версия языка Эрланг была разработана 1986–87 годах сотрудниками фирмы Ericsson для использования в телекоммуникационных системах. Телекоммуникации – одна из областей промышленности, где предъявляются повышенные требования к надежности систем. Коммуникационное оборудование должно годами работать без сбоев и дополнительного обслуживания. Поэтому, в язык Erlang изначально закладывались требования, характерные для телекоммуникационных систем:

- Необходимость обработки очень большого числа параллельных процессов.
- Некоторые действия должны выполняться точно в заданный момент времени, или за определенный временной промежуток. (Мягкое реальное время).
- Системы могут быть распределены на несколько вычислителей.
- Системы используются для управления аппаратурой.
- Очень большие объемы программного кода.
- Системы реализуют комплексную функциональность, существуют зависимости между функциями.
- Непрерывная работа в течение многих лет.
- Обслуживание программного обеспечения (обновление, конфигурирование) должно осуществляться без остановки системы;
- Устойчивость, как к аппаратным сбоям, так и к ошибкам в программном обеспечении.

На сегодняшний день, один из самых больших проектов, реализованных с использованием Erlang – ATM-коммутатор Erricson AXD301 (более миллиона строк кода). Разработчикам удалось достигнуть девяти девяток надежности (99.999999999%) [1]. Основной механизм надежности в Erlang – процессы супервизоры. Рассмотрим схему его работы.

Пары процессов в Erlang могут быть связаны вместе. Если один из процессов в паре погибает, тогда другой получит сообщение, содержащее причины гибели первого. На основании полученного сообщения оставшийся процесс может принять решения по восстановлению системы после случившегося сбоя. Хороший стиль программирования на Erlang предполагает разделение процессов на два класса: рабочих и супервизоров. Процессы-рабочие выполняют основную функциональность системы, супервизоры следят за состоянием системы и перезапускают процессов-рабочих после сбоев. При использовании кэширования данных становится возможным восстановление процесса без потерь. Для достижения максимальной надежности разработчик может строить иерархии (деревья) супервизоров, которые могут восстанавливать после сбоев целые подсистемы.

Реализация обмена сообщениями в императивных языках

В своей статье «Problem with threads» Эдвард А. Ли отмечает, что, несмотря на существование в течении долгого времени моделей альтернативных потокам, программисты раз за разом выбирают именно потоки для решения своих задач [7]. Прежде всего, это связано с тем, что сам дух программирования, все ключевые абстракции программирования связаны с парадигмой последовательных вычислений. Большинство используемых сегодня языков программирования реализуют именно эту парадигму. Синтаксически потоки являются незначительным расширением для таких языков, или даже могут быть реализованы в виде отдельных библиотек. При этом, к сожалению, семантически потоки полностью разрушают детерминизм последовательных вычислений.

Другая причина популярности императивных языков заключается в высокой эффективности их исполнения в рамках существующих архитектур микропроцессоров. Хотя, по своей природе функциональные (декларативные) языки, такие как Erlang, значительно ближе к семантике модели дискретных событий, в рамках которой разрабатывается современная цифровая аппаратура, прямой аппаратный синтез с таких языков остается невозможным, из-за невыполнимых требований к емкости кристаллов микросхем. Другой вариант – разработка архитектуры микропроцессоров, оптимизированных для исполнения функциональных программ. Такие процессоры находят свое применение в специальных областях.

Эдвард Ли видит решение проблемы в использовании координационных языков, как надстройки над существующими широко применяемыми языками. Задачей координационного языка является организация обмена данными между модулями (акторами), описанными на традиционных императивных языках, таких как Си или Java. Реализацией такого подхода является язык Scala и построенный на базе него координационный язык Reo [8].

Scala – мультипарадигменный язык программирования, сочетающий в себе возможности объектно-ориентированного и функционального программирования. Программы, разработанные на Scala, компилируются в код виртуальной машины JVM, что позволяет использовать в разработке существующие классы Java платформы. Одной из особенностей Scala является то, что в отличие от Java, он не использует потоки и общую память для организации параллельных вычислений. Вместо этого в Scala используется механизм обмена сообщениями, аналогичный используемому в Erlang'e. Аналогом потока в Scala является актор. Каждый актор реализует конструкции для отправки и получения сообщений и буфер для принятых сообщений. На базе библиотеки акторов Scala можно легко реализовывать координационные языки для Java платформы.

Выводы

Модель параллелизма, основанная на обмене сообщениями, обладает большими перспективами в области построения надежных и высокоэффективных распределенных систем. Уже сейчас, такие проекты как yaws и ejabberd доказывают состоятельность этого подхода. С развитием многоядерных процессоров и SMP систем, интерес разработчиков к языкам, ориентированным на эту парадигму, будет расти. В области распределенных встраиваемых систем популярность могут завоевать специализированные процессоры и SoC, аппаратно поддерживающие методы обмена сообщениями между процессами.

Литература

1. Armstrong Joe. Making reliable distributed systems in the presence of software errors.// Ph.D. Dissertation, 2003. The Royal Institute of Technology, Stockholm, Sweden.
2. Gul Agha. Actors: A Model of Concurrent Computation in Distributed Systems. // Doctoral Dissertation. – 1986. MIT Press.
3. Carl Hewitt; Peter Bishop; Richard Steiger. A Universal Modular Actor Formalism for Artificial Intelligence. // 1973. – IJCAI, Stanford.
4. William Gropp; Ewing Lusk; Anthony Skjellum. Using MPI, 2nd Edition: portable Parallel Programming with the Message Passing Interface. // 1999, MIT Press In Scientific And Engineering Computation Series, Cambridge, MA. – USA. – 395 pp.
5. J.A. Trono. A new exercise in concurrency // SIGCSE Bulletin. – 1994. – Vol. 26. – PP. 8–10.
6. Richard O'Keefe Solving the Santa Claus problem in Erlang.// http://www.cs.otago.ac.nz/staffpriv/ok/santa/index.htm
7. Edward A. Lee. Problem with Threads // 2006, Technical Report No. UCB/EECS-2006-1, EECS Dept. University of California Berkeley.
8. Philipp Haller; Martin Odersky, Actors that Unify Threads and Events. // 2007, Technical report LAMP-REPORT-2007-001. École Polytechnique Fédérale de Lausanne.
9. Edward A. Lee. Disciplined Message Passing // 2009, Technical report No. UCB/EECS-2009-7, EECS Dept. University of California Berkeley.

УДК 685.618:629.488.27

ОСНОВНЫЕ ТРЕБОВАНИЯ К СТЕНДАМ ДЛЯ КОНТРОЛЯ ИЗМЕРИТЕЛЬНЫХ РУЛЕТОК

Л.А. Хамитова
Научный руководитель – С.С. Гвоздев

Цель исследования – выявление требований к стендам для контроля измерительных рулеток. В статье перечислены главные характеристики, лежащие в основе классификации рулеток, а также показано, какие параметры классификации необходимо учесть в конструкциях стендов.
Ключевые слова: рулетка, стенд, контроль, требования, блок

Введение

Рулетка – инструмент для измерения длин в виде металлической или полотняной (лакированной) ленты с делениями, сворачиваемой в рулон в футляре [1].

Рис. 1. Измерительная рулетка

Рулетки служат для измерения расстояний от одной точки до другой. Рулетка – самый распространенный и один из самых дешевых измерительных инструментов, неизменный атрибут геодезистов и строителей [2].

Как любое измерительное средство, рулетка должна быть поверена. Для создания стендов для поверки или контроля рулеток необходимо классифицировать рулетки и их узлы, и все параметры классификаций учесть в конструкциях стендов и методиках поверки. Основы классификации рулеток были представлены в докладе автора [3].

Основные требования к стендам

Основными составными частями рулетки являются:

– лента с нанесенной шкалой;

– катушка;

– корпус;

– дополнительные приспособления.

Рекомендуется ленту рулетки нагружать в процессе контроля. Поэтому в составе стенда должен присутствовать блок натяжения.

Ленты рулеток в соответствии с ГОСТ 7502-98 могут быть следующих длин: 1 метр, 2 метра, 3 метра, 5 метров, 10 метров, 20 метров, 30 метров, 50 метров, 100 метров (или иной длины, если они изготовлены по заказу потребителя). Длина стенда зависит от длины ленты рулетки [4].

Самые ходовые на сегодняшний день рулетки – «короткие». Длина их полотна – от 2 до 10 м, а ширина – от 12,5 мм до 25 мм. Оба этих показателя определяются задачами, для которых прибор приобретают [5]. Отсюда можно предположить, что стенды для контроля таких рулеток наиболее востребованы.

Шкалы рулеток могут быть следующих видов:

– метрическая шкала;

– дюймовая шкала;

– футовая шкала;

– смешанная шкала.

Шкала на ленте может быть нанесена как с одной стороны, так и с двух сторон. В зависимости от типа шкалы рулетки стенд должен быть приспособлен к контролю шкал ленты с разных ее сторон.

Точность измерений рулеткой определяется классом точности. Например, для класса точности 2 – самого распространенного для рулеток – показания при длине 1 м должны иметь абсолютную погрешность не более 0,5 мм, а при 10 м – не более 2,3 мм [6].

Точность измерительного органа стенда должна соответствовать указанным в таблице 1 параметрам (табл. 1).

Корпус рулетки может быть:

– по типу материала: пластмассовый, металлический, обрезиненный корпус;

– по возможности разборки: разъемный, неразъемный;

– по конструкции: открытый и закрытый.

а) б)

Рис. 2. Рулетки в закрытом корпусе (а) и открытом корпусе (б)

Поэтому в состав стенда может входить блок, обеспечивающий фиксацию корпуса.

В составе рулетки можно выделить дополнительные приспособления, такие как: механизм сматывания, крючок, кольцо, груз, зацеп, ручка, механизм фиксации [7]. Блок, выполняющий фиксацию корпуса, в каждом конкретном случае должен обеспечивать его установку вне зависимости от дополнительных приспособлений.

Конструкция начала ленты рулетки непосредственно влияет на конструкцию блока установки ленты.

Наименование интервала	Допускаемое отклонение действительной длины, не более, для класса точности, в мм	
	2	3
Миллиметровый	±0,15	±0,20
Сантиметровый	±0,20	±0,30
Дециметровый	±0,30	±0,40
Отрезок шкалы 1 м и более	± [0,30+0,15(L-1)]	± [0,40+0,20(L-1)]
Примечание – L – число полных и неполных метров в отрезке		

Таблица 1. Классы точности рулеток и отклонение действительной длины

Заключение

Таким образом, на базе рассмотренной классификации измерительных рулеток можно сделать вывод о том, что:

– в составе стенда для контроля измерительных рулеток должны присутствовать: блок натяжения ленты; блок, обеспечивающий фиксацию корпуса рулетки; блок, предназначенный для фиксации крючка ленты рулетки; блок снятия информации, одной из частей которого должен быть измерительный орган;

– от параметров рулетки зависят такие характеристики стенда как: длина, ширина, класс точности.

Литература

1. Рулетки: [Электронный ресурс]: Большая советская энциклопедия. – Издание 1969–1978 гг. – Режим доступа: http://slovari.yandex.ru/dict/bse/article/00067/39200.htm
2. Рулетки: [Электронный ресурс]: Сайт ЗАО НПФ Белко-М. – Режим доступа: http://www.belkom.ru/products/building/index.html
3. Лучко С.С., Хамитова Л.А., Гвоздев С.С. Основы классификации механических рулеток. – XXXVIII научная и учебно-методическая конференция СПбГУ ИТМО, посвященная 100-летию со дня рождения выдающегося ученого и талантливого педагога М.М. Русинова, 3–6 февраля 2009 года. – Программа. – СПб: СПбГУ ИТМО. – 2009. – С. 44.
4. ГОСТ 7502-98 Рулетки измерительные металлические [Текст]. – Взамен ГОСТ 7502-89; введ. 1998-05-28. – Межгос. совет по стандартизации, метрологии и сертификации; М.: Изд-во стандартов, cop. 1998. – 23 с.
5. Рулетки: [Электронный ресурс]: Современная рулетка. Подготовка, проведение и описание испытаний. Евгений Коноплев, 2002 г. – Режим доступа: http://www.mastercity.ru/cgi-bin/ml.cgi?test&17
6. Рулетки: [Электронный ресурс]: Современная рулетка. Подготовка, проведение и описание испытаний. Евгений Коноплев, 2003 г. http://www.mrtools.ru/tape-line.htm
7. Рулетки: [Электронный ресурс]: Википедия. Свободная энциклопедия, 2008. – Режим доступа: http://ru.wikipedia.org/wiki/Рулетка (инструмент).

УДК 519.71

СИНТЕЗ УСТОЙЧИВЫХ РАССИНХРОНИЗОВАННЫХ ИТЕРАЦИОННЫХ ПРОЦЕССОВ МЕТОДОМ ПРЕ- И ПОСТ-КОДИРОВАНИЯ

Н.Г. Рябых
(Московский физико-технический институт (государственный университет))
Научный руководитель – д.т.н., академик Н.А. Кузнецов
(Институт радиотехники и электроники им. В.А. Котельникова РАН)

В последние годы все более «очевидной» для специалистов в области теории управления, передачи информации и др. становится идея применения асинхронных систем вместо традиционных «синхронных» систем. Применение идеологии асинхронных процессов часто «упирается» в вопрос том, может ли асинхронная система, отвечающая своему синхронному прообразу, быть устойчивой при произвольном срабатывании ее подсистем. Ответ на поставленный вопрос в общем случае отрицателен, но преодоление данной, казалось бы, неразрешимой ситуации возможно, если обратиться к идее кодирования и декодирования информации.

Ключевые слова: рассинхронизованные системы, устойчивость, спектральный радиус, кодирование

Введение

Одним из важных разделов теории управления является анализ работы систем с дискретными элементами. Если в системе имеются дискретные элементы (ключи, элементы памяти, микропроцессоры и др.), которые могут изменять свое состояние (переключаться, подвергаться коррекции, срабатывать) лишь в некоторые определенные дискретные моменты времени, то в общем случае момент срабатывания одного элемента системы не совпадает с моментами срабатывания других элементов. Поэтому большое значение имеет вопрос влияния на динамику системы синхронности (или наоборот – асинхронности) изменения состояния различных ее элементов.

Обеспечивать синхронность работы элементов системы чаще всего приходится инженерным или программным путем (реже она возникает естественно). Иногда она достигается сравнительно просто, но чаще для синхронизации работы элементов приходится либо вводить дополнительные устройства, либо разрабатывать сложные процедуры обмена информацией между компонентами. Это, разумеется, усложняет конструкцию систем, повышает их стоимость и приводит к непроизводительным затратам времени при работе. Кроме того, в некоторых типах систем (экологические и нейронные системы, системы коллективного поведения) несинхронность работы элементов вызвана внешними причинами. Также надо учитывать такие особенности поведения, как сбои в процессорах, дрейф параметров, старение элементов, что также влияет на несинхронность работы системы. На эти причины человек повлиять не в состоянии, но их необходимо учитывать в проектировании и работе.

Указанные особенности систем с синхронно работающими элементами побудили исследователей обратиться к системам, элементы которых могут работать несинхронно друг с другом. Из-за интенсивного развития в последнее время многопроцессорных вычислений и сетей ЭВМ усилился интерес к вопросам влияния синхронности работы технических, биологических и других объектов на их функциональность (см., например [1] и библиографию там).

В данной работе анализируются системы, состоящие из нескольких компонент (элементов, подсистем). Состояние каждой компоненты может изменяться лишь в дискретные моменты времени по некоторому функциональному закону. Если все компоненты системы изменяют свои состояния одновременно, то система называется син-

хронизованной. Однако различные причины могут привести к тому, что некоторые компоненты будут изменять свое состояние неодновременно с другими. Такие системы называются рассинхронизованными.

Системы, построенные по синхронным моделям, обладают рядом недостатков: усложняется структура систем вследствие появления большого количества устройств синхронизации, таймеров; увеличивается трудоемкость и уменьшается надежность программного обеспечения и др. Эти проблемы можно решить, если разработать модель функционирования систем с асинхронным режимом обмена информацией между их частями и исследовать работу таких систем.

Кроме того, зачастую бывает необходимо намеренно перевести систему в рассинхронизованный режим работы – например, при многопроцессорных параллельных вычислениях. Как оказывается, переход от состояния «синхронизованности» к состоянию «рассинхронизованности» и наоборот может привести к качественным изменениям поведения системы. Многие вопросы и задачи, которые в случае синхронизованных систем решены или ответы на которые могут быть получены довольно легко, в случае рассинхронизованных систем становятся весьма трудными и для своего решения требуют развития новых математических подходов.

Одной из основных задач теории рассинхронизованных систем является на хождение условий, при которых система будет устойчивой. Для синхронизованных систем такие критерии устойчивости существуют и доказаны. Кроме того, для некоторых типов систем (например, системы, в которых переход от одного состояния к другому описывается матрицей с неотрицательными коэффициентами) устойчивость рассинхронизованного процесса следует из устойчивости синхронизованного. Но может возникнуть ситуация, в которой синхронизованный процесс будет сходиться, а соответствующий ему рассинхронизованный расходиться. В этой работе описывается метод, который позволяет обойти эту проблему и расширить класс систем, к которым применимы процессы рассинхронизации.

Постановка задачи

Пусть имеется некоторая система W, состоящая из подсистем $W_1, \ldots, W_N$ (рис. 1).

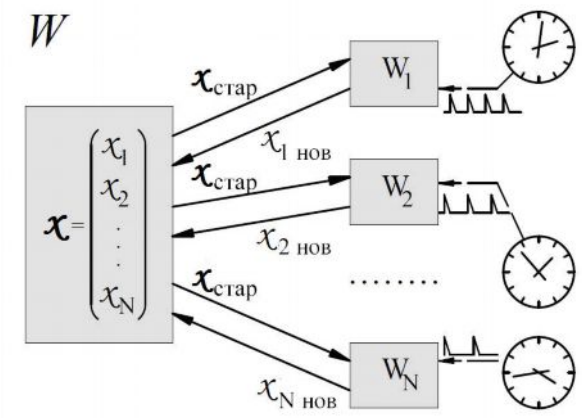


Рис. 1. Рассинхронизованная система

Тогда в общем виде состояние синхронизованной системы (все компоненты переключаются одновременно) записывается в виде

$$x_{n+1} = Ax_n + f_n, \qquad (1)$$

где x_n, x_{n+1} – векторы состояния системы в моменты времени T_n и T_{n+1} соответственно; A – матрица перехода системы; f_n – вектор внешних воздействий.

Если одновременно переключаются не все компоненты, то динамика системы описывается уравнением

$$x_{n+1} = A_{\omega_n} x_n + f_{\omega_n}, \qquad (2)$$

где ω_n – множество номеров переключаемых в момент времени T_n компонент; A_{ω_n} – матрица, строки которой с номерами $i \in \omega_n$, совпадают с соответствующими строками матрицы $A = (a_{ij})$, а строки с номерами $i \notin \omega_n$ совпадают со строками единичной матрицы соответствующего размера.

Применение идеологии асинхронных процессов упирается в вопрос о том, может ли асинхронная вычислительная схема (2), отвечающая своему синхронному прообразу (1), сходиться к решению линейного уравнения

$$x = Ax + f$$

при произвольном выборе индексных последовательностей $\{\omega_n\}$.

Ответ на поставленный вопрос в общем случае отрицателен. Вместе с тем существуют классы матриц *A*, для которых сходимость синхронной процедуры влечет сходимость и ее асинхронного аналога. Так, такие классы образуют симметричные матрицы и матрицы с неотрицательными элементами [1], спектральный радиус которых строго меньше единицы ($\rho(A) < 1$). Таким образом возникает идея некоторым преобразованием привести исходную матрицу *A* к «хорошему» виду. Это становится теоретически возможным, если воспользоваться предложением Даймонда-Опойцева [2]: *если спектральный радиус* $\rho(A)$ *матрицы A размерности* $n \times n$ *строго меньше единицы, то для некоторого натурального* N $(N > n)$ *найдется такая* $N \times n$ *матрица L и* $n \times N$ *матрица P, а также* $N \times N$ *матрица с неотрицательными элементами B, что справедливы следующие соотношения*

$$LA = BL,\ AP = PB,\ \rho(B) < 1.$$

Результат

Разработан алгоритм работы с синхронным итерационным процессом (1), позволяющий применить асинхронную схему вычислений. Разработана методика получения матриц B, P, L из матрицы *A* (кодирование), а также обратный переход (декодирование). Подробное описание алгоритма можно найти в [3].

Составлена программа на языке *C#*, иллюстрирующая работу алгоритма на примере матрицы поворота со сжатием (размерность 2×2).

Алгоритм работы с итерационным процессом (1)

1. Подготовка процедуры. Имея матрицу *A*, спектральный радиус которой строго меньше 1, находятся число *N*, а также матрицы L, P, B.

2. Пре-кодирование. Для нахождения решения уравнения

$$x = Ax + f$$

производится замена переменных $y = Lx$, $\tilde{f} = Lf$ (здесь векторы *y* и $\tilde{f}$ оказываются принадлежащими пространству достаточно большой размерности R^N).

3. Асинхронные вычисления с кодированными данными. Для построения последовательных приближений рассматривается асинхронная процедура

$$y_{n+1} = B_{\omega_n} y_n + \tilde{f}_{\omega_n}$$

Эта итерационная процедура в силу построения матрицы *B* будет сходящейся при любом выборе индексных последовательностей $\{\omega_n\}$ (см. [1]).

4. Пост-кодирование (декодирование). Для нахождения приближений к решению исходного уравнения достаточно произвести замену переменных $x_n = Py_n$.

Результаты работы программы

Рассмотрим итерационный процесс:

$$x_{n+1} = Ax_n + f_n$$

где

$$A = \lambda \cdot \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix},$$

$$\lambda = 0.9,\ \alpha = \frac{2\pi}{3},\ x_0 = f = \begin{pmatrix} 0.5 \\ 0.5 \end{pmatrix}.$$

Синхронный процесс (одновременный пересчет всех координат) сходится к точке:

$$x_* = \begin{pmatrix} 0.12372 \\ 0.41133 \end{pmatrix}.$$

Асинхронный процесс (последовательный пересчет каждой координаты) без кодирования:

$$x_{45} = \begin{pmatrix} -294.7804 \\ 253.43553 \end{pmatrix},\ x_* = \begin{pmatrix} \infty \\ \infty \end{pmatrix}$$

Процесс расходится, как и ожидалось.

Асинхронный процесс с кодированием:

$N = 11$

B – матрица размерности 11×11.

$$\rho(B) \le \|B\| = \max_j \sum_i \left|b_{ij}\right| = 0.94868 < 1$$

Результат после декодирования (количество итераций = 1000):

$$x_* = \begin{pmatrix} 0.12372 \\ 0.41133 \end{pmatrix}.$$

Скорость сходимости для синхронного и кодированного процессов можно наглядно сравнить на следующих графиках:

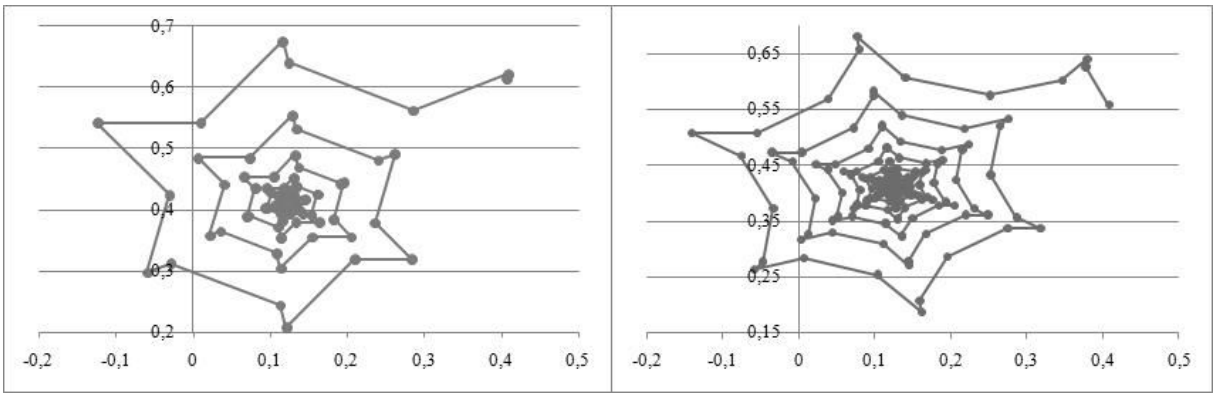


Рис. 2. Ход приближений к решению для синхронного процесса и асинхронного процесса с кодированием

Из рис. 3 видно, что подбором параметров кодирования можно добиться того, что кодированный асинхронный процесс будет довольно близок по сходимости к синхронному процессу.

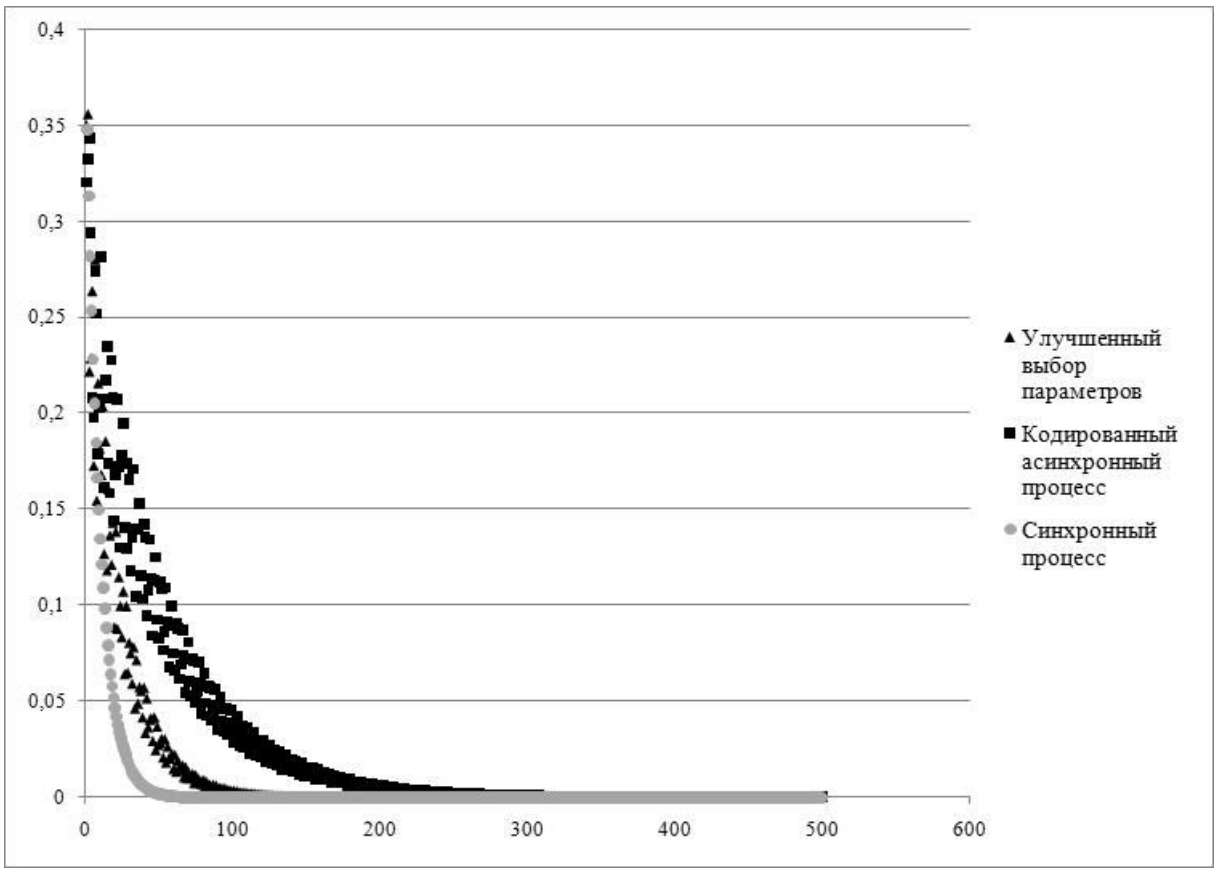


Рис. 3. Скорость сходимости для разных процессов

Заключение

Основным достоинством предлагаемой схемы является тот факт, что она доказывает принципиальную возможность для произвольной матрицы со спектральным радиусом, не превосходящим 1, применить асинхронную процедуру вычисления решения уравнения $x = Ax + f$.

Другим возможным достоинством предлагаемой процедуры является тот факт, что клиенты вычислительной процедуры – то есть процессоры, осуществляющие обработку векторов y_n – будут работать с «кодированными» данными, а их начальное кодирование и последующее декодирование будут осуществляться «постановщиком» задачи. В ряде случаев такая «скрытность» для клиентов вычислительного процесса реальных данных может оказаться существенной.

Основным недостатком предлагаемой схемы является факт существенного роста размерности N матрицы B по сравнению с размерностью n матрицы A. Грубая оценка показывает, что

$$N \approx \frac{1}{(1-\rho(A))^{\frac{n-1}{2}}}.$$

В то же время следует отметить, что матрица B оказывается так называемой «разреженной» матрицей – каждая ее строка и столбец содержат не более $n+1$ ненулевых элементов. Как известно, это существенно упрощает работу с такими матрицами. Кроме того, есть основания полагать, что более «интеллектуальные» процедуры построения матрицы B могут существенно понизить значение размерности N.

Описанный метод перехода к асинхронным гарантированно сходящимся процедурам далек от совершенства. Однако он показывает, что, по крайней мере, теоретиче-

ски построение гарантированно сходящихся асинхронных процедур возможно в достаточно широких ситуациях. Это означает, что необходимы интенсивные исследования в данном направлении, так как не исключена ситуация, что возможны и более простые методы синтеза гарантированно сходящихся асинхронных процедур.

Литература

1. Асарин Е.А., Козякин В.С., Красносельский М.А., Кузнецов Н.А. Анализ устойчивости рассинхронизованных дискретных систем. – М.: Наука, 1992. – 408 с.
2. Даймонд Ф., Опойцев В.И. Устойчивость линейных и разностных дифференциальных включений // Автоматика и телемеханика. – 2001. – № 5. – С. 22–30.
3. Рябых Н.Г. Синтез устойчивых рассинхронизованных итерационных процессов методом пре- и пост-кодирования: Диссертация на соискание степени магистра. – МФТИ, 2008.

УДК: 004.416.6

КОНКУРЕНТНАЯ БОРЬБА ОПЕРАЦИОННЫХ СИСТЕМ НА РЫНКЕ МОБИЛЬНЫХ УСТРОЙСТВ

Н.С. Токалов
Научный руководитель – А.П. Ищенко

В статье рассмотрена динамика структуры российского рынка трех наиболее распространенных операционных систем для мобильных устройств, включая Palm ОС, Symbian ОС и Windows Mobile а также приводятся из основные характеристики и наиболее значительные вехи их становления.
Ключевые слова: рынок, операционная система, ОС, становление, Windows Mobile, Symbian, Palm

Введение

В мобильном обществе возникает потребность эффективно работать даже в дороге, появляется необходимость в полнофункциональных мобильных устройствах. В результате продажи мобильных устройств в России за последние десять лет возросли более чем сто раз. При этом совершенно очевидно, что рыночным спрос обуславливается не мобильным устройством как таковым, хотя дизайн имеет тоже огромное значение, а его свойствами, т.е. программным обеспечением: дорогим или бесплатным, мощным комплексом программ или набором легковесных утилит, являющихся продуктом крупной фирмы, или разработанных самостоятельно. Операционные системы (ОС) это особый вид программного обеспечения, который являются главным отличительным признаком и в значительной степени определяет приоритеты на рынке мобильных устройств. Наиболее распространенными на Российском рынке мобильным устройств являются ОС Palm, Symbian и Windows Mobile (рис. 1). Остановимся подробнее на этих ОС.

Основная часть

У ОС Palm есть одно огромное преимущество перед ОС Symbian и Windows Mobile – Palm был первым. С большой степенью уверенности можно сказать, что большая часть того, что сейчас есть на мобильных устройствах, впервые увидела свет именно на мобильных устройствах фирмы Palm или под управлением ОС Palm. С самого начала в эту ОС была заложена простота и максимальная эффективность имеющихся ресурсов. Положительными сторонами являлось максимальное использование экрана, наличие рукописного ввода, невероятное время работы без подзарядки (от 30–40 часов на ранних моделях, до 6–12 на более новых), компактность, надёжность, отличная синхронизация с ПК, невысокая цена, огромное количество настроек и программного обеспечения [1, 2]. В результате вплоть до 2003 года устройства на базе Palm OS безраздельно царствовали на рынке Российском рынке мобильных устройств, обеспечивая более половины всех продаж (рис. 1).

А в наиболее популярном и продаваемом КПК, работающий на Palm OS – Handspring Treo 600 были настолько удачно объединены функции КПК и телефона, что с момента его создания (2003 г.) и до сих пор – он лучший в своем классе. К минусами можно назвать отсутствие полноценной многозадачности, недостаточной «мультимедийности» и постоянные запоздания с выпусками версий. Из-за большого количества версий рассмотрим лишь две последние, как наиболее возможные для использования в настоящее время. Palm OS версия 4 – 16-битная однозадачная ОС с процессорами серии Motorola DragonBall 68000. С предыдущими версиями разработчики обеспечили

полную совместимость. Была встроена система защиты, которая обеспечивает запрос пароля при включении устройства, а также скрытие записей в базах данных. Встроены драйверы и API с поддержкой соединений по протоколам Bluetooth, GSM, CDMA, а также 2.5G/3G сетей. Максимальное разрешение экрана составляло 160×160, а 320×320 стало результатом доработок других компаний. Не лучшая, но приемлемая работа со звуком и изображениями. Palm OS версия 5 – мультизадачная, 32-разрядная ОС на основе ARM-процессоров стала более надежной плане безопасности. Были введены не только более эффективные системы шифрования, но произошло разграничение пользователей по уровню доступа к различной информации. Появилась авторизация по голосу, отпечаткам пальцев и даже смарт-картам. Ко всему прочему в пятой версии Palm OS поддерживается работа в 802.11b (Wi-Fi) беспроводных сетях. Также поддерживаются экраны с большим разрешением 320x320, произошли заметные изменения в сторону повышения качества графики и звука, что значительно улучшило мультимедийные функции устройств на Palm OS. В то же время приложения предыдущих версий не поддерживаются [1, 2]. Разработчики добавили в эту версию Web-браузер. В начале 2009 г. была представлена новая версия Palm ОС, основанная на ядре Linux, названная Palm WebOS. Перспективы объединения платформ представляются в самом радужном свете. Еще бы, потрясающая мощность и универсальность Unix с простотой использования Palm ОС [12].

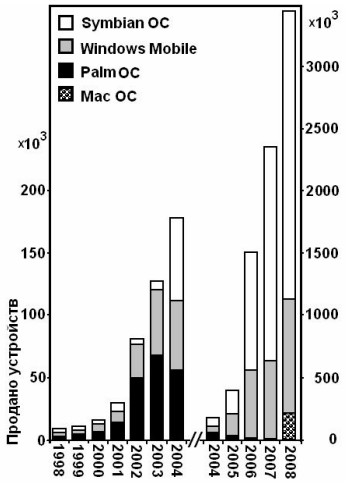


Рис. 1. Динамика и структура Российского рынка годового объема продаж мобильных устройств: смартфонов, коммуникаторов и КПК [3–11]

В середине 90-х годов, когда необходимость в переходе к 32-разрядным архитектурам окончательно сформировалась, началась разработка Symbian ОС [13–15]. В 1997 г. Psion Software представила Symbian OS Release 1. Серия обновлений, вышедшая в течение 1997 года, включала исправление ошибок, приложения для работы с электронной почтой и Web, ПО для синхронизации с настольным компьютером. Пятый релиз Symbian (EPOC 32), анонсированный в 1999 году, включал поддержку цветных дисплеев, Java, улучшенные коммуникационные возможности. Широкие возможности Symbian ОС заинтересовали производителей мобильных устройств. Компания Psion Software была окончательно отделена от Psion Group, превратившись в Symbian Ltd. Задачей компании стала разработка универсальной ОС для мобильных устройств. К 2000 году был готов Release 6. Новая версия ОС Symbian получилась полностью несовместимой со старым ПО, но проработанный набор приложений и ошеломляющий набор функций сгладили этот недостаток. Модульная конструкция позволяла создавать сборку ОС под конкретную аппаратную базу, и, в отличие от ОС Windows или Palm, производителю устройства предоставлялась полная свобода действий. В качестве примера обычно приводят Nokia 9120, Nokia 7650 и SonyEricsson P800 – все эти устройства работают под

управлением ОС Symbian. Первое использует модификацию Crystal (для клавиатурных устройств), второе – Pearl (смартфоны), третье – MediaPhone (Quartz, бесклавиатурные коммуникаторы). Результатом этого является неуклонный рост как абсолютного числа, так и процентного содержания ОС Symbian структуре рынка годового объема продаж мобильных устройств (рис. 1). В настоящее время наиболее распространённой версией ОС является Symbian OS Series 60 (S60).

Отличительной особенностью платформы S60 является её мультимедийная направленность и максимальная телефонная функциональность – можно даже не задумываться о том, что в телефоне есть операционная система. Уже в стандартной поставке имеются отличные редакторы для фотографий и видео, предусмотрены Real Player и Flash Player. Все программы для S60 пишутся с использованием языков программирования C++ и Java MIDP. Однако Symbian все-таки не обладает такой расширяемостью и надстраиваемостью, как Windows Mobile, что делает её более стабильной платформой. Дополнительным бонусом платформы S60 является огромное количество разнообразных игр, написанных специально под неё.

Компания Microsoft на рынок мобильных устройств заглядывалась с самого его появления [16–18]. Уже к 1995 году были готовы промежуточные версии Windows Pegasus. Интересно, что Windows Pegasus получилась более «продвинутой», чем многие ОС для настольных компьютеров, вышедших позже! Чего стоит встроенная поддержка Unicode, потребовавшаяся Microsoft для продвижения продукта на международном рынке. В 1996 году разработка получила название Windows CE 1.0, а в 1997 году была опубликована версия Windows CE 2. Вторая версия являлась полноценной ОС для встраиваемых устройств, тогда как Windows CE 1 предназначалась только для клавиатурных КПК. Модульная конструкция ОС позволяла удалять отдельные части в определенных конфигурациях. Windows CE 2.0 можно было использовать как для установки на мобильные компьютеры, так и в автомобильных навигационных системах, промышленных встраиваемых устройствах и программируемых кофеварках. ОС умела работать с сетевыми адаптерами, модемами, VGA-экранами, разъемами расширения с интерфейсом PCMCIA и CompactFlash и другой периферией. Заметные изменения претерпело комплектное ПО: появились Pocket Access и PowerPoint. С версией 2.10 появилась поддержка TCP/IP, файловой системы FAT32, fast infra-red, шины USB. Обновление 2.11 для Handheld PC привнесло одну интересную возможность: работа на КПК с файлами Microsoft Word и Excel без дополнительных преобразований. Эта функциональность исчезнет из дальнейших выпусков ПО для Windows CE, но появится у основного конкурента – Palm OS (в виде Documents To Go). В 2000 г. Microsoft представила Windows CE 3.0. Без преувеличения, выход Windows CE 3.0 стал переломным моментом в развитии рынка КПК. Безраздельному властвованию Palm появилась серьезная угроза (рис. 1). Функциональность ОС от Microsoft во многом превосходила Palm OS. Среди недостатков, как всегда, числились высокие требования к аппаратной базе и неумеренное энергопотребление. Но маркетинговая машина набрала обороты, и покупатели были готовы платить за возможности проигрывания mp3 и просмотра фильмов на КПК. Версия 4.0 содержала заметную часть проверенного кода. Внушительный список изменений большей частью коснулись поддержки 802.1x, IPSec/L2TP, Bluetooth, IPv6, USB host и других подсистем. Windows Mobile 5.0 была специально разработана для мобильных устройств в 2005 г. и включала новые возможности: Office Mobile, с PowerPoint Mobile, Windows Media Player 10 Mobile, Photo Caller ID, поддержка клавиатуры QWERTY, ActiveSync 4.0, с AKU 3.2 поддержка .NET Compact Framework 2, интерфейс работы с GPS, поддержка Persistent Storage, а также возможность работы по четырём видам беспроводного подключения – 3G, Wi-Fi, WAN, Bluetooth. В ОС Windows Mobile 6.1 добавлено «Карусельное» меню, приложение One Note Mobile для создания голосовых, текстовых и графических заметок, в Internet Explorer включена функ-

ция «Zoom Out», «Managed Programs», улучшена работа по Wi-Fi и Bluetooth с поддержкой Bluetooth 2.1, добавлена поддержка MS Exchange Server 2007. В ОС Windows Mobile 7 (третий квартал 2009 года) будут поддерживаться жесты – новейший способ управления устройством.

Основными особенностями ОС семейства Windows Mobile являются: гибкая настройка практически любых параметров, поддержка тем оформления интерфейса, установка программ сторонних разработчиков (плееры, игры, навигационный софт, калькуляторы, словари и многое другое), что значительно расширяет возможности устройства с Windows Mobile. Сама ОС уже содержит в себе множество возможностей – это работа с сообщениями (SMS, электронная почта), медиаплеер, Internet Explorer, календарь, заметки, адресная книга – т.е. стандартный телефонный и КПК функционал. По дизайну ОС напоминают настольную Windows, однако имеют с ней мало общего, впрочем, тем, кто привык к домашней Windows будет психологически приятно видеть знакомые цвета и логотип. Наследственная черта Windows Mobile, взятая от Windows CE – открытая архитектура. Это открывает небывалые возможности установки дополнительных программ, можно даже заменять и надстраивать стандартные программы Windows Mobile. Однако эта особенность делает систему менее стабильной – чем больше программ установлено, тем больше вероятность конфликта. Конечно же, Windows Mobile обладает многозадачностью – т.е. на таком устройстве можно запустить одновременно несколько программ и работать с ними.

Заключение

Прогнозы, которые можно сделать на основании сложившейся ситуации, обрадуют сторонников продукции Microsoft. Перечисленные выше особенности ОС в сочетании с агрессивной маркетинговой политикой, проводимой корпорацией, неуклонно ведет к увеличению объемов продаж устройств с предустановленной Windows Mobile.

Нет поводов для беспокойства и у пользователей Symbian. Отличные коммуникационные возможности, непревзойденный уровень реализации энергосберегающих технологий, модульная конструкция и другие немаловажные особенности позволяют назвать Symbian лучшей ОС для коммуникаторов/смартфонов.

К сожалению, не смотря на все свои многочисленные достоинства, операционная система Palm проигрывает сейчас более современным ОС. На рынке КПК активно продвигаются, и что важно, стремительно завоевывают популярность устройства с Windows Mobile. Производители же смартфонов всё больше предпочитают устанавливать Symbian, что также сильно теснит Palm. И если разработчики этой операционной системы не сделают каких-то революционных шагов в сторону расширения её возможностей, подобно выпуску новой ОС – Palm webOS – первой многозадачной ОС компании Palm, то мобильные устройства с предустановленной Palm OS уйдут в историю.

Литература

1. Всё о Palm OS, http://mirsovetov.ru/a/hi-tech/pocket-computer/palm-os.html
2. Бережная Т. (2007) Palm OS – операционная система для мобильных устройств, http://mobil.km.ua/articals/mobileos/palmos.php
3. Басина Н. (2001) Российский рынок карманных компьютеров: Состояние. Особенности. Развитие, ИнфоБизнес, N1 (146), 16 января 2001, http://offline.ibusiness.ru
4. Хавжу Д. (2002) Несколько поправок к маркетинговому исследованию, http://www.hpc.ru/lib/arts/1821/printable.shtml

5. Итоги исследования российского рынка КПК за 2002 г., http://www.handy.ru/a/2003/03/25/1003.html
6. Итоги исследования российского рынка КПК за 2003 г., http://www.handy.ru/a/2004/01/19/1799.html
7. Российский рынок КПК и смартфонов в 2004 году, http://www.handy.ru/a/2004/12/22/2416.html
8. SmartMarketing объявляет оценки рынка КПК и смартфонов за 2005 г, http://www.smartmarketing.ru/pda_smartphone_y2005
9. Российский рынок смартфонов, коммуникаторов и КПК в 2006 г., http://www.handy.ru/a/2007/03/06/6750.html
10. КПК, коммуникаторы и смартфоны в России. 2007 год, http://www.handy.ru/a/2008/03/20/7277.html
11. Рынок смартфонов и коммуникаторов в России: 3,4 млн. проданных устройств в 2008 году http://rumetrika.rambler.ru/publ/article_show.html?article=3639
12. Palm анонсировала новую ОС и первый коммуникатор на ее основе, http://www.mobiletm.ru/blog/2009/01/12/palm_webos_i_palm_pre/
13. История развития Symbian OS, http://mazur.3dn.ru/publ/1-1-0-1
14. Все о Symbian OS, http://dvj92.ucoz.ru/forum/73-56-1
15. Все о Symbian OS, http://advices.com.ua/vse_o_symbian_os.html
16. История развития Windows Mobile, http://3gplist.ru/publ/6-1-0-2
17. Все о Windows Mobile, http://moikompas.ru/compas/wmobile
18. Все о Windows Mobile, http://mirsovetov.ru/a/hi-tech/cellular-phone/windows-mobile.html

УДК 004.052.42

КОНТРОЛЬ РАБОТЫ АВТОМАТНЫХ ПРОГРАММ С ИСПОЛЬЗОВАНИЕМ АППАРАТА ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ

В.О. Клебан
Научный руководитель – д.т.н., профессор А.А. Шалыто

В статье ставится задача динамического контроля работы автоматных программ и предлагается решение данной задачи с применением аппарата цифровой обработки сигналов.
Ключевые слова: автоматное программирование, верификация программ

Введение

В настоящее время получает распространение проверка свойств программ на моделях. Однако такая мера не является достаточным средством для обеспечения надежности программного обеспечения, в силу того, что это не более чем проверка выполнения лишь *некоторых* свойств программы. Полноту такой проверки следует также доказать, что является также нетривиальной задачей. Таким образом, программа остается бесконтрольной *в процессе работы*. Кроме того утверждение о текущем состоянии программы может зависеть от всей истории исполнения – описания последовательности всех предшествующих переходов и всех промежуточных состояний. Это означает, что доказательство свойств такой программы не может быть статическим и его следует вести динамически – параллельно с ее исполнением при конкретных исходных данных.

Постановка задачи динамического контроля

Можно поставить задачу динамического контроля работы автоматных программ [1]. Для решения этой задачи предлагается динамически измерять значения некоторых параметров работающей автоматной программы. Измеренные значения параметров могут использоваться, к примеру, как аргументы правил поведения контролирующей системы, для выработки управляющих воздействий по результатам измерений и т.д. Разработанный метод предоставляет возможность осуществлять контроль без введения каких-либо специальных состояний в автоматную программу, добавления (удаления) переходов, то есть фактически без изменения самой автоматной программы.

На практике это означает, что при контроле эффективности работы программы возможно использовать не только выходные параметры, генерируемые самой программой, но и некоторые показатели «поведения» программы [2].

Метод решения задачи

Метод состоит в следующем: процесс работы автоматной программы представляется в виде дискретной функции, пригодной для анализа средствами цифровой обработки сигналов.

Рассмотрим алгоритм преобразования процесса работы автоматной программы в дискретную функцию (рис. 1):

- перенумеруем состояния автоматной программы;
- будем осуществлять запись состояний в ходе работы программы;
- отложив по оси ординат номера состояний, а по оси абсцисс время (или такты работы автомата), получим дискретную функцию.

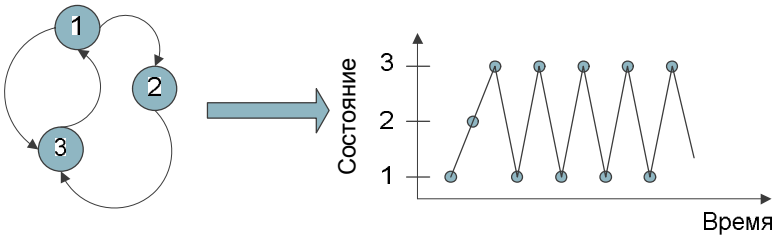


Рис. 1. Преобразование процесса работы автоматной программы в дискретную функцию

Можно рассмотреть полную четырехмерную модель: Время, состояние, вход и выход. Полученная дискретная функция – является *траекторией автомата* и может быть проанализирована средствами цифровой обработки сигналов. Следует отметить, что для наблюдателя не всегда становится возможным накопление полной траектории автомата, например в силу того, что подконтрольный автомат работает существенно быстрее контролирующего автомата. В этом случае могут наблюдаться явления сходные с наложением спектров при дискретизации непрерывных сигналов.

Пример работы системы предупреждения

Одним из наиболее интересных подходов к анализу является построение нейросетевой, либо иной обучающейся системы классификации. Классификатор обучается с помощью тех функций, которые были получены при штатной работе автоматной программы (либо использует самообучение). Обученный таким образом классификатор способен с некоторой вероятностью обнаруживать нештатную работу программы. Отметим, что данный подход позволяет не только контролировать работу автоматных программ, но и сравнивать автоматы между собой по поведению, а не по графу переходов, что необходимо для уменьшения пространства поиска при решении задач выращивания автоматных программ методами генетического программирования.

Рассмотрим автомат принимающий на вход отношения вида *a<>b;* в виде строк (рис. 2), где *a* и *b* – числа, <> – знаки отношения и символ окончания*;* (например “`10>9;`”, “`6<12;`”).

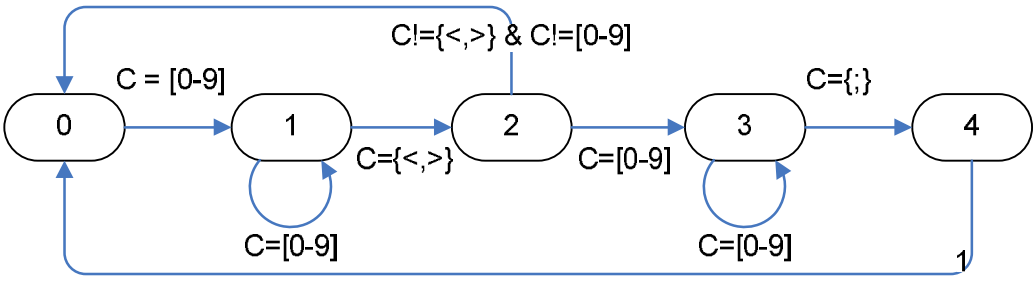


Рис. 2. Автомат обрабатывающий строки вида a<>b

На данном этапе функция выполняемая автоматом не имеет значения, достаточно лишь того, чтобы результаты ее работы выглядели правильно со стороны наблюдателя. Согласно предложенной концепции сформируем дискретную функцию описывающую работу автомата и подадим ее на вход нейронной сети.

В качестве нейронной сети используется персептрон с одним скрытым слоем состоящим из 21 нейрона и выходным слоем состоящим из 5 нейронов. Обучение производится методом обратного распространения в ручном или автоматическом режиме. В ручном режиме в качестве учителя выступает пользователь, который оценивает пра-

вильность работы по пятибалльной шкале. В автоматическом режиме система обучается в течение некоторого времени. При этом гарантируется, что в данный отрезок времени контролируемый автомат работает правильно.

Зависимость ошибки обучения нейронной сети от номера шага приведена на рис. 3. Из графика видно, что нейронная сеть обучилась всего за шесть шагов.

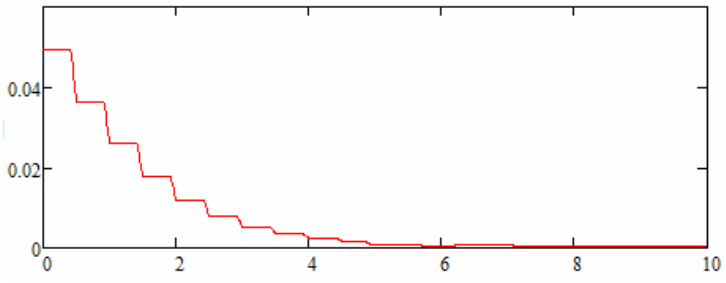


Рис. 3. Процесс обучения нейронной сети

В дальнейшем на обученную нейронную сеть оказывались следующие возмущающие воздействия (порядок соблюден):

- на вход поступаю правильные данные, и работает правильный автомат;
- на вход поступали зашумленные данные;
- на вход поступаю правильные данные, и работает правильный автомат;
- в наблюдаем автомате удален один из переходов.

Реакция нейронной сети представлена на рис. 4.

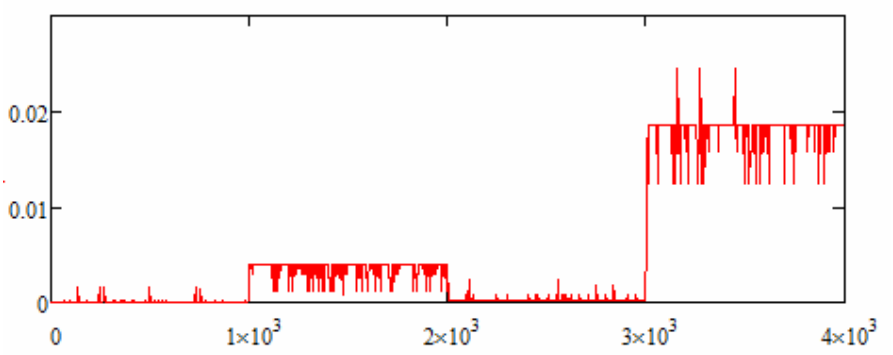


Рис. 4. Реакция нейронной сети на возмущение

Из графика видно, что нейронная сеть правильно сигнализировала об изменениях в поведении автомата. Безусловно, теоретические вопросы, связанные с настройкой сети и схемой ее построения, а также иные, связанные с предложенным методом требуют дальнейшей проработки.

Полученный способ решения задачи может быть применен (в случае его дальнейшей проработки) для контроля автоматных программ без изменения этих программ, что повышает инженерную привлекательность метода.

Литература

1. Шалыто А.А. Switch-технология. Алгоритмизация и программирование задач логического управления. СПб: Наука, 1998. http://is.ifmo.ru/books/switch/1
2. Сапожников В.В., Сапожников Вл.В. Дискретные автоматы с обнаружением отказов. Л: Энергоатомиздат. 1984.

УДК 004.052

МОДЕЛИРОВАНИЕ БИЗНЕС-ПРОЦЕССОВ С ИСПОЛЬЗОВАНИЕМ КОНЕЧНЫХ АВТОМАТОВ

В.О. Клебан, Л.Е. Стрюк
Научный руководитель – к.ф-м.н., доцент Ф.А. Новиков

В работе рассматривается задача построения системы автоматизации документооборота. Для построения системы автоматизации документооборота применяются конечные автоматы, так как такой подход имеет ряд преимуществ по сравнению с традиционным.

Ключевые слова: автоматное программирование, документооборот, автоматизация бизнес-процессов

Введение

Проблема автоматизации бизнес-процессов, на сегодняшний день, достаточно остро стоит перед предприятиями. Многие крупные предприятия уже обзавелись системами электронного документооборота, тогда как малые и средние – практически нет и продолжают использовать разрозненные документы Microsoft Office (в редких случаях с использованием распределенного хранилища Microsoft Groove).

Традиционный способ автоматизации бизнес-процессов – разработка прикладного программного обеспечения – постепенно вынужден отходить на второй план ввиду того, что внесение даже небольших изменений в схему бизнес-процесса означает необходимость перепрограммирования и большие затраты времени и средств. В результате прикладные программы не успевают обновляться в том темпе, который диктуют изменяющиеся условия бизнеса и потребности самого предприятия.

Активно развивающийся бизнес, связанный с автоматизацией предприятий, требует большого количества обученных кадров из-за больших объемов работ. При этом количество квалифицированных специалистов в области автоматизации растет недостаточно быстро.

Таким образом, стоит задача создания простого в освоении, надежного средства автоматизации, имеющее в своем арсенале не только средства описания документооборота, но и его исполнения. Возможность исполнения является ключевым моментом, ведь чисто описательное средство интересно только с точки зрения анализа бизнес-процессов и может быть применено при реализации конкретной модели документооборота лишь как часть технического задания. Во всех известных авторам случаях, «описательная» часть системы автоматизации документооборота оторвана от «исполнительной» части, что делает невозможным быстрый переход от спроектированной схемы к реализации.

Использование конечных автоматов

Наряду с описанием процессов в виде блок-схем, существует другой подход – автоматный [4].

Данный подход заключается в представлении процесса в виде системы взаимодействующих автоматов. Автоматы могут взаимодействовать по вложенности (один автомат вложен в одно или несколько состояний другого автомата), по вызываемости (один автомат вызывается с определенным событием из выходного воздействия, формируемого при переходе другого автомата), по обмену сообщениями (один автомат получает сообщения от другого) и по номерам состояний (один автомат проверяет, в каком состоянии находится другой автомат). Вложенность может рассматриваться как

вызываемость с любым событием. Ни число автоматов, вложенных в состояние, ни глубина вложенности не ограничены. Такое представление позволяет более компактно описывать поведение программы, модуля, а в нашем случае – жизненный цикл документа, либо бизнес-процесса. Компактное представление в свою очередь улучшает наглядность.

Конечный автомат может быть представлен в виде простейшей языковой конструкции, состоящей из одного или нескольких операторов `SWITCH`. Возможность такого подхода делает возможным формальное и изоморфное автоматическое преобразование автомата в код программы. Повышается наблюдаемость программы за счет сокращения количества наблюдаемых переменных.

Автоматные программы могут быть эффективно верифицированы методом проверки на моделях (Model Checking) [5], так как в таких программах управляющие состояния явно выделены, а их количество обозримо. Это позволяет строить компактные модели Крипке даже для программ большой размерности.

Автоматные программы показали свою эффективность при построении «реактивных систем» [6]. Документооборот, по сути, является такой системой. Документы реагируют на действия пользователей, а бизнес-процессы на изменения в документах, т.е. *система управляется событиями*.

В качестве примера использования данной технологии рассмотрим применение предлагаемого подхода к построению инструментального программного средства на базе Microsoft Office, которое предназначено для разработки и внедрения автоматизированной системы менеджмента качества (АСМК) в компаниях с *проектным* типом организации производства. В разработке также используется продукт Microsoft Groove, который позволяет организовать распределенное хранилище документов. При проектном типе организации производства *реализации* одного и того же бизнес-процесса могут отличаться в разных проектах в рамках одной организации. Автоматизированная система менеджмента качества – это частично или полностью программно реализованная система менеджмента качества определенная в стандарте ИСО 9001 : 2000.

Принципы работы и средства описания

Система представляет собой инструментальное программное средство (конструктор), предназначенный для разработки и внедрения АСМК.

Определим следующие роли пользователей системы:

- разработчик – изготовитель инструментария;
- инженер – пользователь инструментария, осуществляющий автоматизацию предприятия;
- пользователь – сотрудник предприятия, использующий систему для выполнения повседневных обязанностей.

Инструментарий состоит из следующих основных средств, которые обеспечивают базовую функциональность:

- система времени выполнения (клиент и сервер);
- транслятор моделей жизненного цикла бизнес-процессов;
- транслятор моделей жизненного цикла документов.

Используя средства инструментария, инженер определяет в графическом виде модели бизнес-процессов и модели жизненных циклов документов, а также производит их стыковку с системой времени выполнения.

Моделью жизненного цикла *активного* объекта (документа или бизнес-процесса) является конечный автомат, в котором определены состояния объекта, условия перехода из одного состояния в другое и выходные воздействия (эффекты). Условие перехода является булевой формулой, в которой участвуют *входные воздействия* и *события.*

Входное воздействие представляет собой функцию, как правило, оперирующую с записями о качестве (в терминах ИСО 9001) и возвращающую булево значение. Событие – это именованное сообщение, инициирующее переход автомата и поступающее на вход системы в произвольный момент времени. Событие может быть сгенерировано автоматом жизненного цикла документа, либо автоматом жизненного цикла бизнес-процесса, либо другим «поставщиком событий» в зависимости от задачи.

Рассмотрим в качестве примера процесс исправления ошибки в программном продукте, упрощенная модель которого представлена на рис. 1.

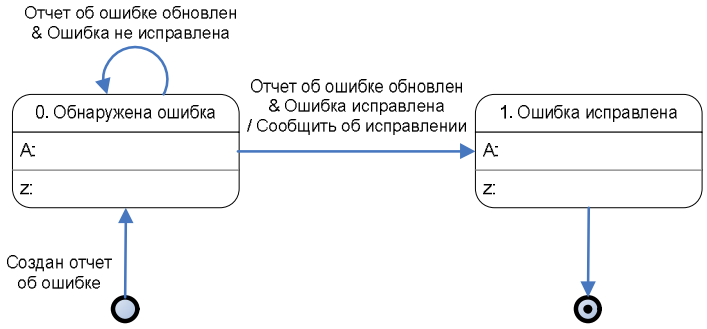


Рис. 1. Процесс исправления ошибки

На данной модели выделено два состояния: «Обнаружена ошибка» и «Ошибка исправлена». Используются два события, на которые реагирует модель: «Создан отчет об ошибке» и «Отчет об ошибке обновлен» и условия «Ошибка исправлена», «Ошибка не исправлена». Также используется выходное воздействие «Сообщить об исправлении». Стрелками показано направление перехода.

Переход из состояния «Обнаружена ошибка» в состояние «Ошибка исправлена» следует читать так: при наступлении события «Отчет об ошибке обновлен» и истинности условия «Ошибка исправлена» совершить действие «Сообщить об исправлении» и перейти в состояние «Ошибка исправлена».

Как было указано ранее, активный объект системы способен реагировать на события от других объектов, а также сам порождать события (в эффектах). Например, документ при переходе из одного состояния в другое порождает событие, которое передается бизнес-процессу. Важно, что жизненный цикл документа исполняется на стороне клиента, а жизненный цикл бизнес-процесса на стороне сервера. Процесс передачи события проиллюстрирован на рис. 2.

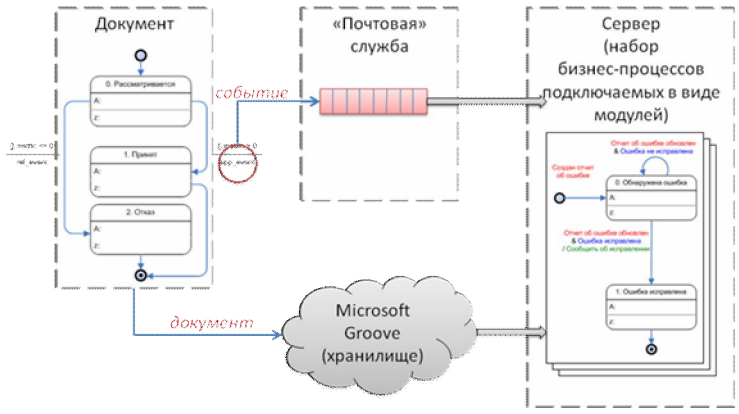


Рис. 2. Передача события из документа в бизнес процесс

Документ при переходе из состояния «Рассматривается» в состояние «Принят» генерирует событие, которое попадает в «Почтовую службу». Она является временным

хранилищем событий на стороне пользователя и сохраняет события (и порядок их следования), в том случае, если передача их на сервер затруднена или невозможна. Одновременно с отсылкой события на сервер происходит сохранение документа в распределенное хранилище Microsoft Groove.

Сервер, после получения события и соответствующего ему документа, действует в соответствии с заложенными в него моделями жизненных циклов бизнес-процессов, например, извлекает из хранилища необходимый документ и анализирует, изменяет его содержимое.

Заметим, что для обеспечения функционирования АСМК в рамках организации необходимо соблюдение следующих *условий функционирования*:

- бизнес-процессы организации, подпадающие под действие АСМК, определены и документированы;
- управление бизнес-процессами отражено в электронных документах;
- выполнение бизнес-процессов основано на обработке событий;
- обрабатываемыми событиями являются события документов: создание, удаление, изменение;
- записи о качестве (метрики) хранятся в специальных полях документов.

Некоторые из данных условий справедливы не только в рамках внедрения АСМК, но и для документооборота в целом.

Структура документа

Документ делится на две составляющие: «модель» и «представление», объединенные в один файл в соответствии со стандартом OpenXML, который реализован в Microsoft Office 2007. К документу Microsoft Office прикреплено XML-хранилище, в котором хранятся служебные данные и значения записей (метрик). Подчеркнем, что данные (записи о качестве) хранятся непосредственно в документе.

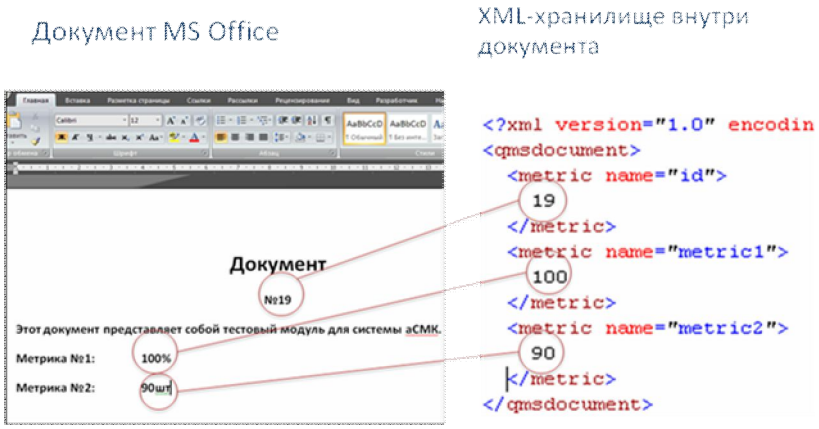


Рис. 3. Структура документа

Внутри документа также храниться его жизненный цикл, записанный в виде XML-представления (рис. 4).

Рис. 4. Модель жизненного цикла и его представление

Структура модуля бизнес-процесса

Модуль бизнес-процесса представляет собой динамическую библиотеку (plug-in), которая подключается сервером АСМК. Устройство такой библиотеки аналогично устройству документа, с той разницей, что в документе модель жизненного цикла интерпретируется и хранится в виде XML-модели, а в модуле бизнес-процесса модель жизненного цикла скомпилирована. Модель жизненного цикла бизнес-процесса описывается аналогичным образом, в качестве примера приведем упрощенную модель процесса исправления ошибки и соответствующее XML-представление.

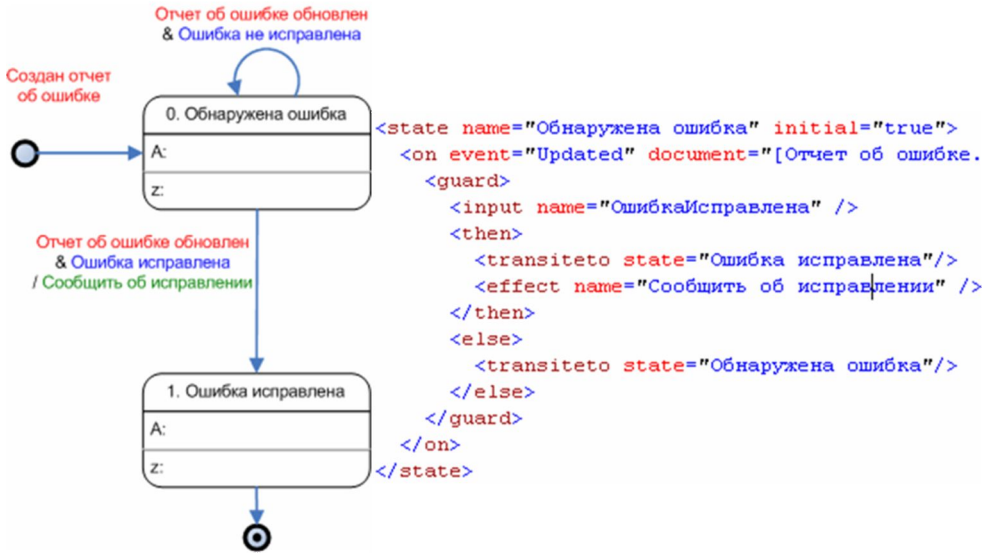


Рис. 5. Модель процесса исправления ошибки в графическом и XML представлениях

Описанные выше XML-модели, а в дальнейшем и исполняемый код, генерируются автоматически из графического представления конечных автоматов, созданных в редакторе Microsoft Visio, и текстовых описаний входных и выходных воздействий.

Полученная промежуточная XML-модель преобразуется в исходный код модуля на языке C# и компилируется соответствующим компилятором.

Входные и выходные воздействия описываются с помощью языка C# в следующем виде:

```
<input name="ОшибкаИсправлена">
  <![CDATA[
   public bool ОшибкаИсправлена(){
      int a = int.Parse([Отчет об ошибке.docx].metric1);
      int b = int.Parse([Отчет об ошибке.docx].metric2);
      return (a >= 100 && b >= 100);
   }
  ]]>
</input>
```

Для удобства инженера в язык введена операция доступа к документам `[]`. Для того чтобы считать запись с именем «`metric1`» из документа «`Отчет об ошибке.docx`», необходимо использовать следующую операцию:

```
[Отчет об ошибке.docx].metric1
```

Заключение

Применение конечных автоматов в документообороте уже находит поддержку: например, в Microsoft Workflow помимо представления документооборота в традиционной форме (в виде блок-схем), введено представление в виде конечных автоматов.

Использование конечных автоматов при автоматизации документооборота позволяет решить несколько важных задач:

– простота автоматной модели существенно снижает требования к разработчикам, которые занимаются автоматизацией предприятий, что очень важно при наблюдающемся дефиците специалистов;

– изменение модели жизненного цикла активного объекта (документа или процесса) не приводит к необходимости перепрограммирования, достаточно лишь изменить схемы, т.к. большая часть программного кода генерируется автоматически по моделям;

– наблюдаемость автомата и его обратимость позволяют совершать «откат» системы в предыдущие состояния, не прибегая к сложным алгоритмам;

– возможность верификации автоматной модели позволяет строить системы правил, которые будут отвечать за ключевые моменты документооборота, что в свою очередь позволит проверять построенные модели еще до внедрения;

– классический способ наблюдения за показателями бизнеса – по метрикам (количество продукции и т.д.) в случае использования автоматной модели может быть дополнен показателями, основанными на поведении моделей, а это означает, что повышается вероятность обнаружения «патологии» в работе предприятия.

Литература

1. Новиков Ф.А. Дискретная математика для программистов //СПб: Питер. – 2008.
2. Шеер А.-В. Моделирование бизнес-процессов. //Весть-Метатехнология. – 2000.
3. Марка Д., МакГоуэн К. Методология структурного анализа и проектирования. http://www.marathon.ru/~fedor/doc/IDEF/ooad.asf.ru/standarts/idef/sadt/index.shtml
4. Шалыто А.А. Switch-технология. Алгоритмизация и программирование задач логического управления. СПб: Наука, 1998. http://is.ifmo.ru/books/switch/1
5. Автоматное программирование (http://is.ifmo.ru). Раздел «Верификация».
6. Шалыто А.А., Туккель Н.И. SWITCH-технология – автоматный подход к созданию программного обеспечения «реактивных» систем //Промышленные АСУ и контроллеры. 2000. № 10. (http://is.ifmo.ru/works/switch/1).

004.514:681.3

ИСПОЛЬЗОВАНИЕ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА DISTTOOL СИСТЕМЫ MATLAB ПРИ СТАТИСТИЧЕСКОЙ ОБРАБОТКЕ ЭКСПЕРИМЕНТАЛЬНЫХ ДАННЫХ

Е.П. Дудьева, Л.А. Хамитова
Научный руководитель – д.т.н., профессор В.М. Мусалимов

В статье рассматриваются три способа обработки экспериментальных данных в системе Matlab, особое внимание уделяется графическому интерфейсу disttool. Описан метод работы с интерфейсом disttool, использованы результаты работы, полученные на лабораторных занятиях.
Ключевые слова: интерфейс, система, обработка, данные

Введение

Экспериментальные исследования событий и процессов основаны на наблюдениях, в ходе которых регистрируются различные факты искусственного и естественного происхождения. Источниками экспериментальных данных могут быть результаты наблюдения за реальными объектами и протекающими в них процессами. Наблюдения могут проводиться в ходе испытаний или в ходе обычной эксплуатации. Также источниками данных могут быть результаты моделирования объектов. Обработка экспериментальных данных, получаемых от различных источников, имеет много общего. Однако организация сбора и интерпретации экспериментальных данных специфична для конкретной предметной области [1].

Существуют различные подходы и методы построения алгоритмов оценивания экспериментальных данных, а также разные программные средства, позволяющие обрабатывать экспериментальные данные.

Одним из программных средств, при помощи которых можно обрабатывать экспериментальные данные, является система Matlab. В системе Matlab функции плотности распределения вероятностей и функции распределения вероятностей могут быть заданы следующими способами:

- вызовом m-функций в командное окно;
- вызовом функции «hist» в командное окно;
- при помощи m-функции «disttool».

m-функции

В командном окне системы Matlab набираются функции:

```
f=normpdf(x, 0.0549, 0.0687); plot(x, f)
f=weibpdf(x, 4, 3); plot(x, f)
f=exppdf(x, 0.1); plot(x, f)
f=raylpdf(x, 0.9); plot(x, f)
```

и получены функции распределений вероятностей (рис. 1).

Функция hist

Функции плотности распределения вероятностей и функции распределения вероятностей выводится в виде гистограмм (рис. 2).

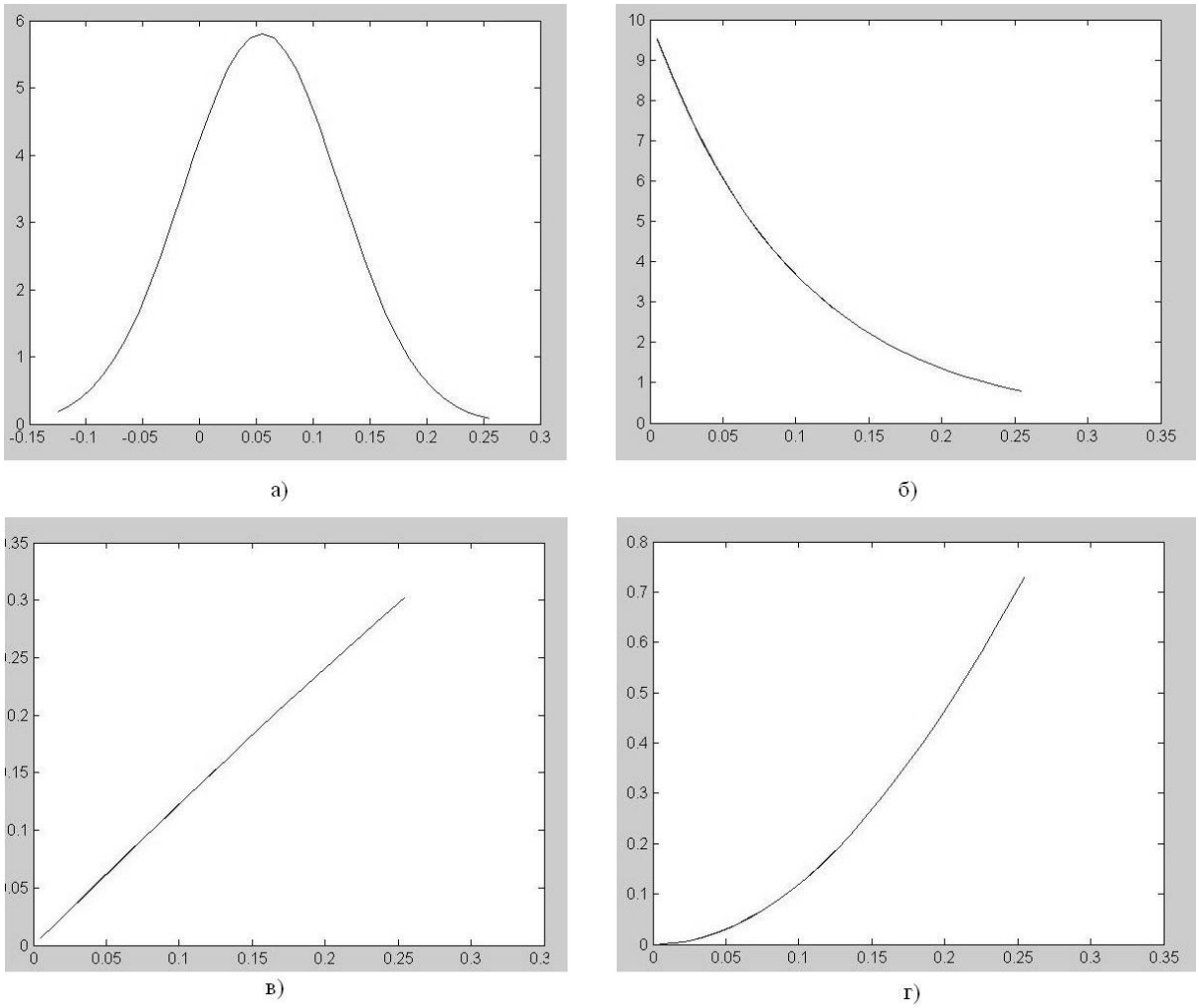


Рис. 1. Графики функций распределений вероятностей: а) – нормальный закон распределения; б) – экспоненциальный закон распределения; в) – закон распределения Рэлея; г) – закон распределения Вейбулла

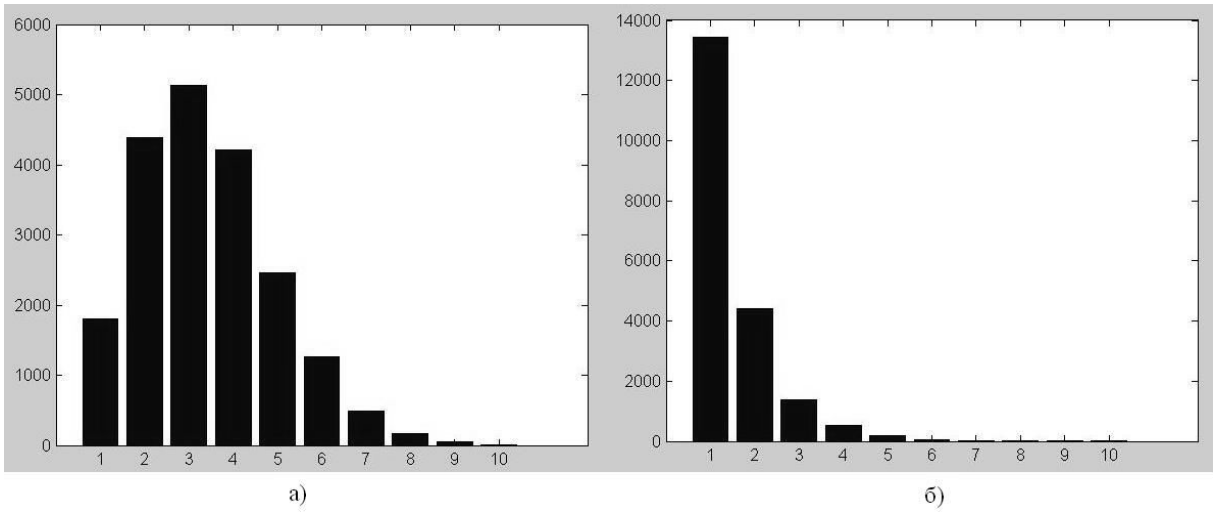


Рис. 2. Гистограммы функций распределения: а) – закон распределения Рэлея; б) – экспоненциальный закон распределения

m-функция disttool

Disttool представляет собой графический интерфейс для изучения влияния изменения параметров на участке ВПР (плотности распределения вероятностей) или PDF. Функция disttool отображает в графическом окне интерактивный график функции распределения. Вид закона распределения значений одномерной случайной величины выбирается пользователем. Кроме вида закона распределения пользователь может задать значения его параметров. Функция может быть выполнена при помощи команды: >> disttool + enter, которая вводится в командном окне [2].

Меню «Distribution» (рис. 3) предназначено для выбора закона распределения. В меню «Distribution» доступны все одномерные вероятностные модели, реализованные в соответствующем разделе Statistics Toolbox. По умолчанию при загрузке графика будет выбран нормальный закон.

Меню «Function type» позволяет выбрать вид функции распределения:

- CDF – функция распределения вероятностей;
- PDF – функция распределения плотности вероятности.

Значение функции распределения будет рассчитано для заданного значения случайной величины. Значение случайной величины может быть задано вводом числа в строку ввода или перемещением вертикальной штрихпунктирной линии на графике (рис. 3). После изменения значения случайной величины автоматически будет пересчитано значение функции распределения и отображено в строке ввода. Вводя значение вероятности в строку ввода «Probability» можно рассчитать соответствующее значение случайной величины. Значение функции распределения плотности вероятности будет отображено как текстовая метка, и не может быть изменено пользователем [3].

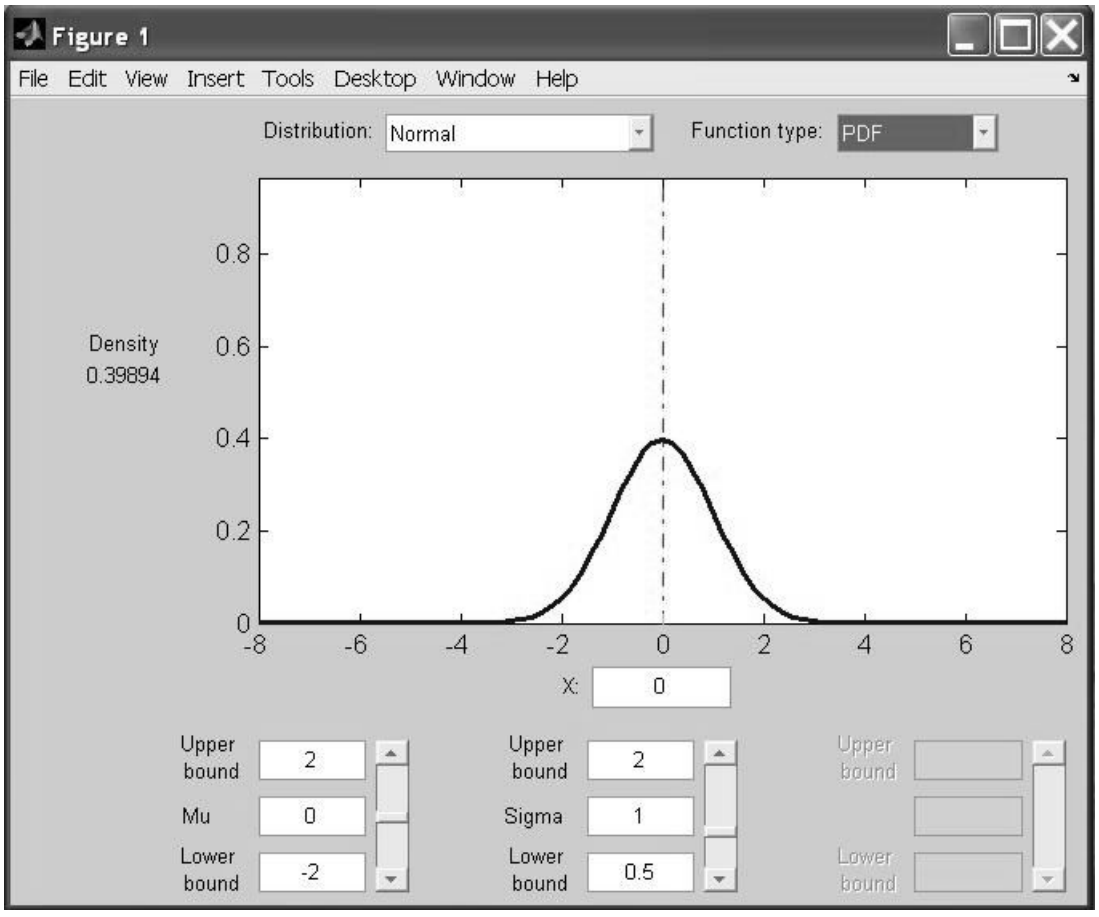


Рис. 3. Вид диалогового окна при работе с графическим интерфейсом disttool

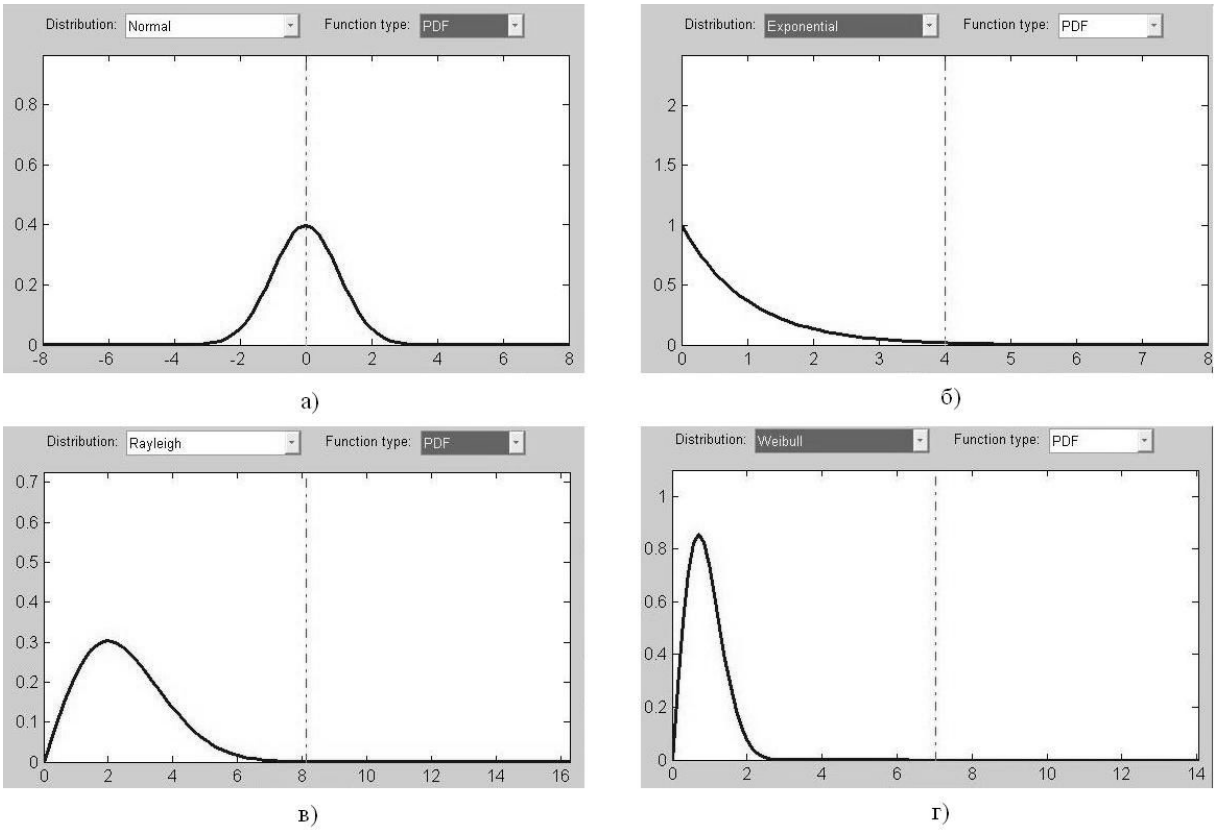


Рис. 4. Графики функций распределений плотностей вероятностей:
а) – нормальный закон распределения; б) – экспоненциальный закон распределения;
в) – закон распределения Рэлея; г) – закон распределения Вейбулла

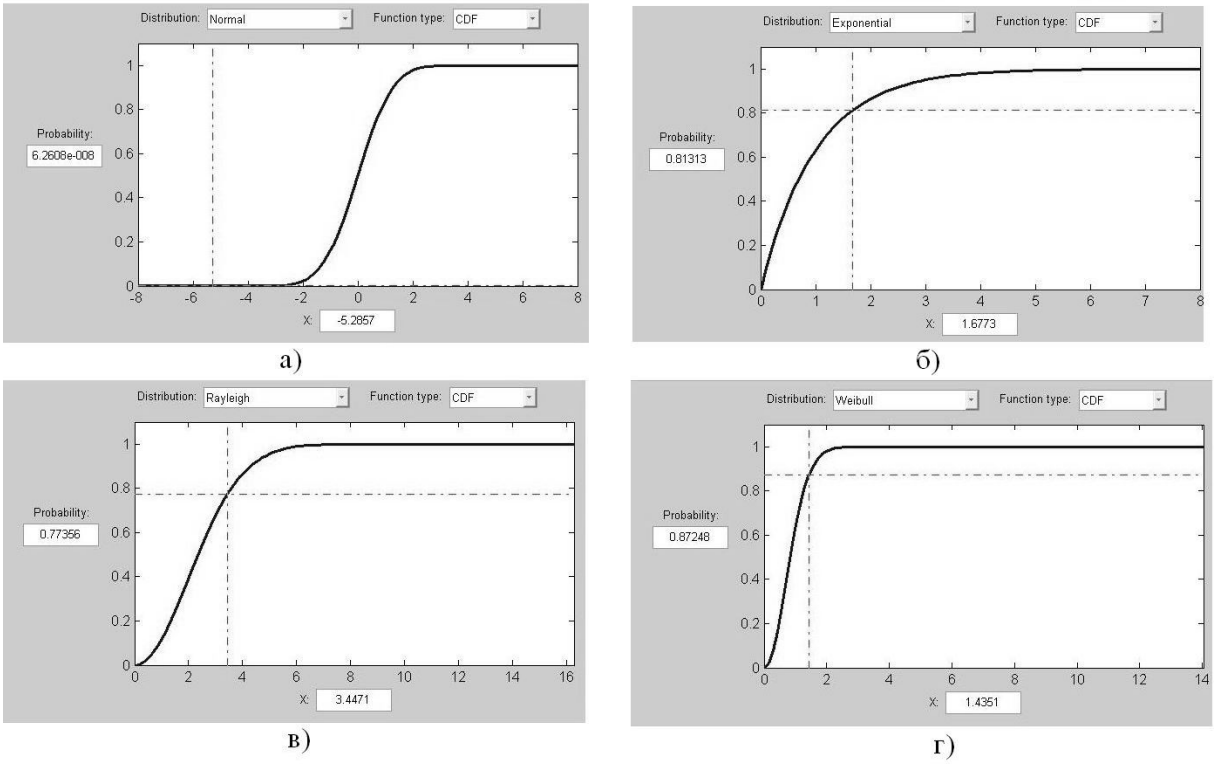


Рис. 5. Графики функций распределений плотностей вероятностей:
а) – нормальный закон распределения; б) – экспоненциальный закон распределения;
в) – закон распределения Рэлея; г) – закон распределения Вейбулла

Параметры закона распределения задаются при помощи вторых, в матрице нижних элементов управления, строк ввода или соответствующих им полос прокрутки. Для нормального закона строки ввода обозначены метками «Mu», «Sigma» (математическое ожидание, среднее квадратическое отклонение). Для остальных законов распределения метки строк ввода будут идентичны названиям параметров соответствующих законов распределения, приведенных в разделах системы помощи. Количество активных столбцов в матрице элементов управления будет соответствовать числу параметров распределения, выбранного в меню «Distribution». Строки ввода «Upper bound» и «Lower bound» предназначены для задания значений верхнего и нижнего пределов изменения параметров выбранного распределения при использовании полос прокрутки [4].

Примеры графиков функций распределения вероятностей (рис. 4) и функций плотностей распределения вероятностей (рис. 5), полученные в интерактивном окне disttool, приведены ниже.

Заключение

Был проведен обзор возможностей графического интерфейса disttool системы Matlab. В статье использовались результаты работы лабораторных занятий. Основным преимуществом графического интерфейса disttool является возможность изменения параметров функций распределения в интерактивном режиме. Такая возможность интерфейса позволяет моделировать процессы.

Литература

1. Степанов О.А. Элементы теории вероятностей: текст лекций. – СПб. – 2007. – 82 с.
2. Математика\Statistics Toolbox \Statistics Toolbox 5.0. Руководство пользователя \Графический анализ одномерных функций распределения [Электронный ресурс]. – Режим доступа: http://matlab.exponenta.ru, свободный. – Загл. с экрана. – Яз. рус.
3. Математика MATLAB Электронный учебник \Обработка данных [Электронный ресурс]. – Режим доступа: http://atomas.ru/mat/Matlab, свободный. – Загл. с экрана. – Яз. рус.
4. Раздел "Математика» \Statistics Toolbox \Список функций Statistics Toolbox \Оценка параметров закона распределения по экспериментальным данным [Электронный ресурс]. – Режим доступа: http://rrc.dgu.ru, свободный. – Загл. с экрана. – Яз. рус.

621.391.18:621.39:621.396.98

ИСПОЛЬЗОВАНИЕ ДИФФЕРЕНЦИАЛЬНЫХ НАВИГАЦИОННЫХ СИСТЕМ В ГБУ «ВОЛГО-БАЛТ»

Г.Б. Чистяков
(Санкт-Петербургский государственный университет водных коммуникаций)
Научный руководитель – д.т.н., профессор А.П. Нырков
(Санкт-Петербургский государственный университет водных коммуникаций)

Статья посвящена новому способу расстановки знаков навигационного ограждения на внутренних водных путях, используемому в ГБУ «Волго-Балт», с применением современных программно-аппаратных средств и дифференциальных навигационных систем.

Ключевые слова: навигация, дифференциальные системы, программные средства

Введение

Одним из ключевых факторов, обеспечивающих безопасность судоходства является непрерывность получения судоводителем информации об участке водного пути, по которому следует судно. А обеспечивается эта непрерывность, в первую очередь, знаками навигационного ограждения. Ежегодно вся навигационная обстановка снимается на зимний период и расставляется заново перед началом новой навигации. Обслуживанием внутренних водных путях (ВВП) Северо-Запада Российской Федерации занимается ГБУ «Волго-Балт». До недавнего времени расстановка знаков путевыми бригадами осуществлялась с помощью визуально-инструментального метода (рис. 1).

Рис. 1. Установка буя

При этом, в основном, использовались береговые отметки или засечки, то есть визуальные средства местоопределения, инструментальные измерения с использованием геодезических приборов применялись лишь изредка, в первую очередь, для установки или перемещения береговых объектов, в частности, створных знаков, не снимаемых на зимний период и требующих повышенного внимания. Указанный способ расстановки порождал как достаточно большую погрешность в расположении плавучих СНО, так и

затруднение в оперативном изменении их местоположения и доведении этих сведений до картографической службы с целью выпуска корректуры к картам.

Использование предлагаемого навигационного комплекса позволяет повысить точность проведения работ, снизить издержки, облегчить обработку и передачу информации между участниками процесса.

Основная часть

Для перехода на новый уровень производства работ в ГБУ «Волго-Балт» предлагается использовать навигационный комплекс, включающий ГЛОНАСС/GPS – приемник с функцией приема дифференциальных поправок и ноутбук с установленным программным обеспечением WayMaster («Путевой мастер»). Выбор данного комплекса обусловлен полным его соответствием требованиям, предъявляемым ГБУ, таким как, точность позиционирования, простота использования, возможность установки, как на судне, так и на оборудованном рабочем месте, реализация сквозной передачи информации в электронном виде в картографическую службу. С помощью данного комплекса оперативно проводится весенняя расстановка плавучих навигационных знаков, проверка и корректировка положения знаков относительно судового хода, постановка на штатное место знаков, сбитых судами и природными явлениями. Условия судоходства на внутренних водных путях требуют повышенный точности определения координат по сравнению, например, с морскими районами плавания. Для плавания по ВВП требуется высокая точность обсервации со среднеквадратической погрешностью (СКП) местоопределения 1–2 м (с вероятностью p=0,95) или не ниже 5–10 м для наиболее крупнотоннажных речных судов и судов класса «река-море». К точности установки навигационных знаков также предъявляются повышенные требования.

Точность, необходимая для морских районов с легкостью обеспечивается с помощью глобальных навигационных спутниковых систем (ГНСС). В случае использования совместно СРНС ГЛОНАСС и GPS точность определения координат (с вероятностью более 0,95) составляет от 2 до 10 м. На практике погрешность обычно не превышает 1..2 м. Но для выполнения условий по точности определения координат места для районов внутренних водных путей необходимо использовать специальные дополнения, такие как дифференциальные подсистемы ГНСС.

Рабочее окно программы представлено на рис. 2.

Рис. 2. Программа «Путевой мастер»

Основой рабочей области является электронная навигационная карта (ЭНК) того участка пути, на котором в данный момент выполняет работу путейская бригада. Местоположение судна отображается схематичным значком (размеры задаются пользователем в зависимости от габаритов реального судна) со стрелкой, обозначающей курс судна. Данные для своего местоопределения программа получает от спутникового навигационного приемника по протоколу NMEA. Благодаря наличию локальных контрольно-корректирующих станций (ККС) вдоль всего Волго-Балтийского водного пути (рис. 3) прием высокоточного навигационного сигнала с дифференциальными поправками обеспечивается на протяжении всей трассы.

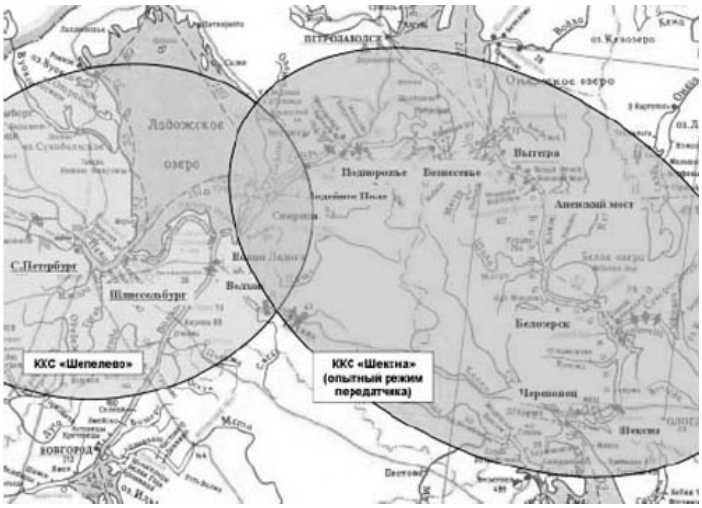


Рис. 3. ККС на трассе Волго-Балта

В режиме навигации программа автоматически перемещает электронную карту одновременно с перемещением судна, позволяя его отметке всегда находиться в центре экрана, для удобства восприятия информации. Масштаб изображения задается пользователем.

Для выполнения операций в программе предусмотрен планшет, который является как бы «верхним слоем» над электронной картой. Основными операциями, необходимыми пользователю, являются добавление нового объекта с заданными координатами, снятие координат вновь установленных или уже существующих объектов, запись трека судна. Например, при необходимости выставления нового плавучего знака (или переноса уже существующего на новое место) с помощью плана промера определяется требуемое место установки. Вычисляются координаты, и по ним на планшете в необходимой точке устанавливается отметка буя. Далее при работе на судне путейская бригада может в программе проложить себе курс к данной отметке и ориентироваться уже по электронной карте на экране, (пример выполнения данной операции приведен на рис. 4).

При использовании комплекса значительно упрощается задача контроля ранее установленных знаков, судну достаточно подойти к бую и по положению отметок судна и буя на экране будет видно, не смещен ли навигационный знак относительно своей первоначальной позиции.

Планшет и трек судна сохраняются в отдельный файл, который затем передается для анализа производителю работ в РВПиС и РГСиС , далее принятые изменения по установленной форме передаются в Службу пути ГБУ «Волго-Балт», где специалистами по навигационному ограждению и путевой информации проводится обработка дан-

ных и их дальнейшая передача в картографическую службу для внесения изменений в электронную базу ЭНК, для создания корректурных файлов ЭНК.

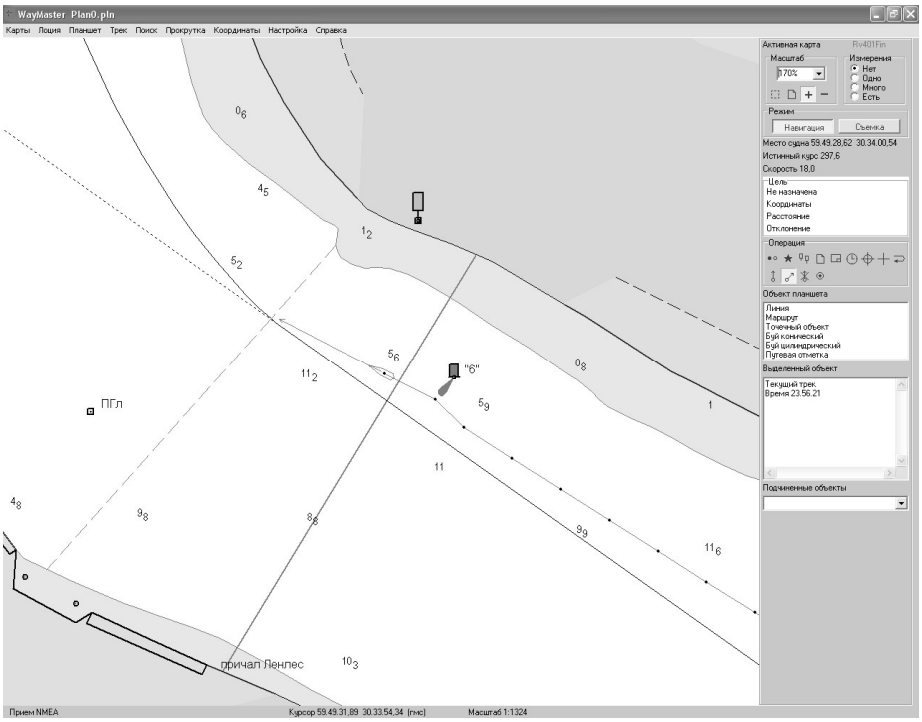


Рис. 4. Установка буя с помощью комплекса

Заключение

Во время проведенных ГБУ «Волго-Балт» испытаний система показала свою эффективность и реальную пользу для повышения безопасности судоходства на ВВП, позволив как повысить точность выставления навигационного ограждения до 8-10 м (учитывая точность показаний дифференциального навигационного приемника и перемещение путейского теплохода), так и упростить работу путейских бригад и повысить скорость прохождения оперативной информации до конечного пользователя.

Литература

1. Каретников В.В. Автоматизация судовождения: учебник / В.В. Каретников, В.Д. Ракитин, А.А. Сикарев. – СПб: СПГУВК. – 2007. – 265 с.
2. Бродский Е.Л., Ракитин В.Д., Сикарев А.А. О реализации концепции построения дифференциальных подсистем ГНСС на ЕГС европейской части РФ/Журнал Транспорт Российской Федерации. – 2006. – №5. – С. 37–38.
3. Соловьев Ю.А. Спутниковая навигация и ее приложения. – М.: Эко-Трендз. – 2003.

УДК 681.3

МЕТОДЫ СНИЖЕНИЯ ВЛИЯНИЯ ШУМА В ПОСЛЕДОВАТЕЛЬНОСТИ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ДВОЙНОГО ДЕРЕВА ВЕЙВЛЕТ ПРЕОБРАЗОВАНИЯ

П.С. Скаков
Научный руководитель – д.т.н., профессор И.П. Гуров

В работе рассматриваются применение двойного дерева вейвлет преобразования к задаче подавления шума видео. Описываются общие принципы использования двойного дерева и расширение их на двух- и трехмерные случаи. Предлагается комбинированный метод, призванный улучшить качество фильтрации быстро движущихся объектов.

Ключевые слова: шумоподавление, обработка видео, вейвлет преобразование

Введение

Дискретное вейвлет преобразование (ДВП) широко применяется для анализа и обработки изображений и видео. Основными недостатками наиболее часто используемого полностью прореженного (неизбыточного) ДВП являются сильная зависимость получаемых коэффициентов от сдвигов изображения и не различение деталей по некоторым направлениям. При выполнении шумоподавления видео с использованием ДВП следствием первого недостатка является нестабильность изображения между кадрами с небольшими перемещениями частей изображения, а второго – появление специфических искажений, наиболее заметных около резких границ и при агрессивном шумоподавлении (рис. 1.2).

Для снижения зависимости ДВП от сдвигов изображения возможно использование непрореженных его форм. Но такой подход существенно увеличивает вычислительные затраты и избыточность получаемых данных – в $(2^m)^n$ раз для n-уровневого преобразования в m-мерном пространстве.

Устранить оба недостатка при ограниченном увеличении необходимых вычислительных затрат и избыточности позволяет метод, предложенный в [1–3] – использование двойного дерева ДВП (рис. 1.3).

Рис. 1.1. Исходное изображение

Рис. 1.2. Неизбыточное ДВП

Рис. 1.3. Двойное дерево ДВП

Особенности двойного дерева ДВП

Одномерное неизбыточное ДВП хорошо сочетает локальность и разложение на частоты, что делает его очень удобным для большого класса реальных сигналов. К сожалению, это не верно для случаев большей размерности, например в двухмерном случае по-прежнему хорошо выделяются точечные особенности, но не диагональные линии или участки кривых, что приводит к специфическим искажениям, хорошо заметным на рис. 1.2.

Проблема состоит в том, что спектр вещественного вейвлета $\psi(x)$ содержит как положительные, так и отрицательные частоты, в результате чего построенный на его основе двухмерный вещественный неизбыточный вейвлет $\psi(x,y)=\psi(x)\psi(y)$ будет иметь частотный отклик вида «шахматная доска» и, соответственно, не будет различать диагональные направления.

Решить проблему можно использовав комплексный вейвлет вместо вещественного: $\psi(x)=\psi_h(x)+j\psi_g(x)$, в котором $\psi_h(x)$ и $\psi_g(x)$ являются преобразованиями гильберта друг друга с точностью до знака. В этом случае двухмерный вейвлет

$$\psi(x,y)=[\psi_h(x)+j\psi_g(x)][\psi_h(y)+j\psi_g(y)]=$$

$$\psi_h(x)\psi_h(y)-\psi_g(x)\psi_g(y)+j[\psi_g(x)\psi_h(y)+\psi_h(x)\psi_g(y)]$$

будет иметь частотный отклик только в одной четверти пространства, а его вещественная часть $\mathrm{Re}(\psi(x,y))=\psi_h(x)\psi_h(y)-\psi_g(x)\psi_g(y)$ – в двух противоположных четвертях, таким образом, по-прежнему обладая чёткой направленностью и отсутствием эффектов «шахматной доски».

Двойное дерево ДВП строится из двух деревьев обычных полностью прореженных ДВП (схема 1). Как было описано, в случае специально подобранных преобразований для каждого из деревьев коэффициенты одного дерева могут быть интерпретированы как вещественная часть, а другого – как мнимая часть единого комплексного вейвлет преобразования (рис. 1), обладающего свойствами чёткой направленности и инвариантности к сдвигу.

При обратном преобразовании на последнем этапе каждое дерево вносит одинаковый вклад в восстанавливаемое изображение.

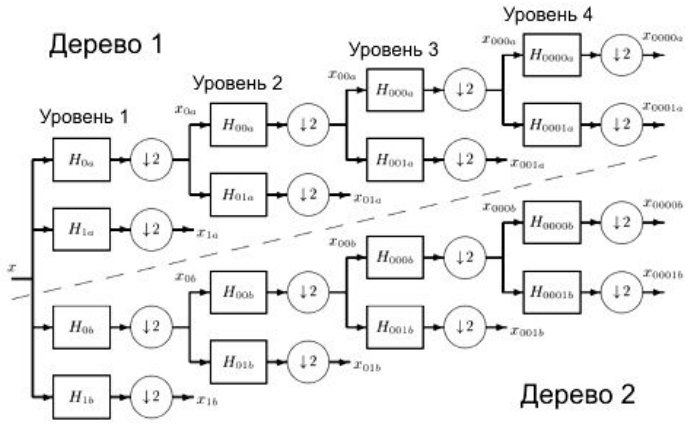


Схема 1. Двойное дерево фильтров дискретного вейвлет преобразования

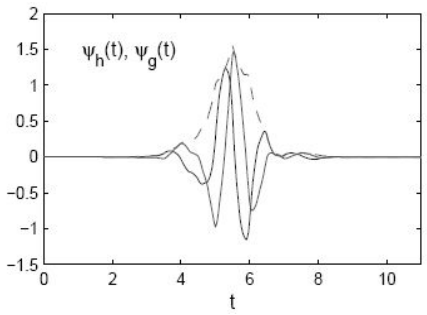


Рис. 2. Комплексный вейвлет (пунктиром) и его вещественная и мнимая части

В двухмерном случае возможно два варианта построения двойного дерева – вещественное и комплексное.

В вещественном случае дерево состоит из двух полностью прореженных деревьев с вещественными значениями:

$$\psi_{1,1}(x,y)=\phi_h(x)\psi_h(y) \qquad \psi_{2,1}(x,y)=\phi_g(x)\psi_g(y)$$

$$\psi_{1,2}(x,y)=\psi_h(x)\phi_h(y) \qquad \psi_{2,2}(x,y)=\psi_g(x)\phi_g(y)$$

$$\psi_{1,3}(x,y)=\psi_h(x)\psi_h(y) \qquad \psi_{2,3}(x,y)=\psi_g(x)\psi_g(y)$$

с которыми ассоциировано шесть вейвлетов (рис. 3):

$$\psi_i(x,y)=\frac{1}{\sqrt{2}}(\psi_{1,i}(x,y)+\psi_{2,i}(x,y))$$

$$\psi_{i+3}(x,y)=\frac{1}{\sqrt{2}}(\psi_{1,i}(x,y)-\psi_{2,i}(x,y))$$

Каждый их шести вейвлетов строго ориентирован в пространстве (по направлениям ±15°, ±45° и ±75°) в отличие от трёх вейвлетов обычного ДВП, где только два имеют строгую ориентацию по горизонтали и вертикали, а третий совмещает два диагональных направления (рис. 4). Избыточность преобразования равна 2.

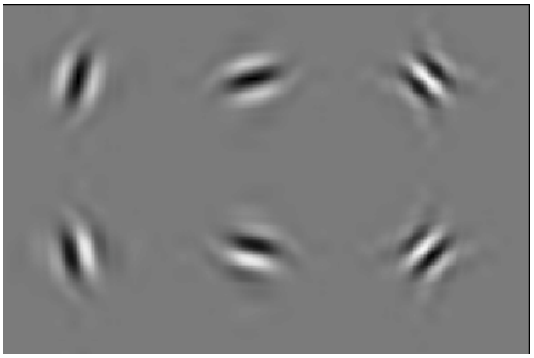


Рис. 3. Вейвлеты действительного двойного дерева

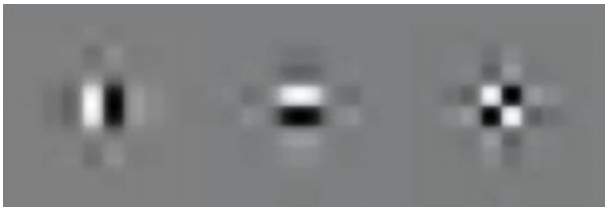


Рис. 4. Вейвлеты неизбыточного преобразования

В комплексном случае деревья содержат комплексные значения, с которыми ассоциировано 12 вейвлетов (рис. 5), ориентированных в пространстве по тем же направлениям, что и в вещественном случае, но здесь каждому направлению уже соответствует пара вейвлетов. Каждая такая пара вейвлетов может быть рассмотрена как вещественная и мнимая части одного комплексного вейвлета, модуль которого, в отличие от действительных вейвлетов, затухает без колебаний. Избыточность преобразования равна 4.

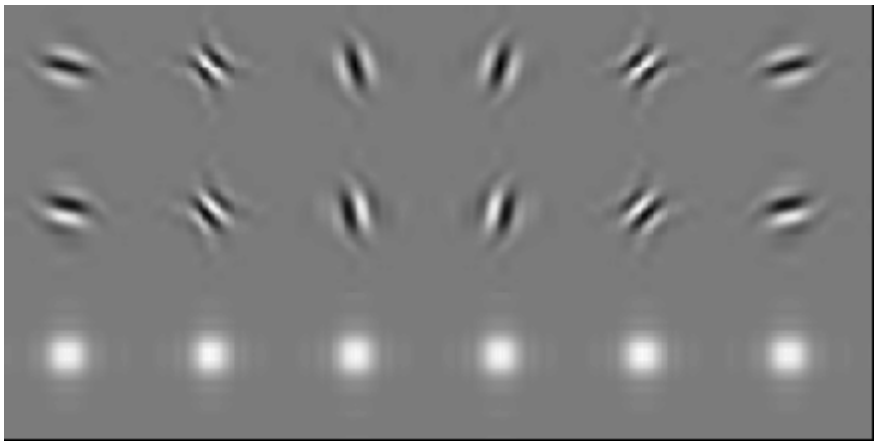


Рис. 5. Вейвлеты комплексного двойного дерева и модули комплексных пар

Трехмерный случай

Двойное дерево ДВП может быть прямо обобщено на случай трёх измерений, что представляет интерес для рассмотрения видеоданных как трёхмерного изображения. В этом случае порождается 28 различно направленных и по-прежнему чётко ориентированных вейвлетов, по одному на каждое направление для вещественного дерева и по паре для комплексного. Преобразование обладает 4-х кратной избыточностью в вещественном случае и 8-и кратной в комплексном.

Необходимо отметить, что ось времени видео обладает отличными характеристиками от пространственных осей изображения. Разрешение видео, частота кадров, угловая скорость перемещения и количество уровней декомпозиции определяют границы эффективного применения трёхмерного вейвлет преобразования видео. Так как при быстром движении объект находится совсем в разных частях изображения даже на соседних кадрах, то для выделения корреляции между такими фазами небольшого числа уровней разложения уже недостаточно, а при большом числе уровней не хватает разрешения для установления зависимостей.

Предлагается дополнить трехмерное двойное дерево ДВП компенсацией движения соседних кадров для более эффективного использования информации из них.

Пример практического использования

Для практической проверки эффективности применения двойного дерева ДВП для шумоподавления видео были выбраны вейвлеты, приведённые в таблице 1, и стандартное видео Flowers из набора «Tektronix test sequences». На изображение был наложен Гауссовый шум и отфильтрован несколькими способами. Были рассмотрены неизбыточное двухмерное ДВП, вещественное двухмерное и трехмерное двойное дерево ДВП, а также исследована комбинация блокового метода компенсации движения с логарифмическим поиском и перекрытием блоков с трёхмерным вещественным двойным деревом ДВП. В качестве оценки эффективности фильтрации использовалось пиковое отношение сигнала к шуму (PSNR).

Таблица 1. Коэффициенты вейвлетов

ϕ_h	ψ_h	ϕ_g	ψ_g
0	0	0.01122679215254	0
-0.08838834764832	-0.01122679215254	0.01122679215254	0
0.08838834764832	0.01122679215254	-0.08838834764832	-0.08838834764832
0.69587998903400	0.08838834764832	0.08838834764832	-0.08838834764832
0.69587998903400	0.08838834764832	0.69587998903400	0.69587998903400
0.08838834764832	-0.69587998903400	0.69587998903400	-0.69587998903400
-0.08838834764832	0.69587998903400	0.08838834764832	0.08838834764832
0.01122679215254	-0.08838834764832	-0.08838834764832	0.08838834764832
0.01122679215254	-0.08838834764832	0	0.01122679215254
0	0	0	-0.01122679215254

Рис. 6.1. Исходное изображение

Рис. 6.2. Изображение с наложенным шумом (PSNR 31.8)

Рис. 6.3. Двухмерное неизбыточное ДВП (PSNR 34.6)

Рис. 6.4. Двухмерное двойное дерево (PSNR 35.7)

Рис. 6.5. Трехмерное двойное дерево (PSNR 36.0)

Рис. 6.6. Трехмерное двойное дерево + компенсация движения (PSNR 36.2)

Заключение

Были рассмотрены отличительные особенности двойного дерева вейвлет преобразования в применении к задаче шумоподавления видео. Практическая проверка как подтверждает преимущество в данной задаче двойного дерева ДВП перед обычным неизбыточным ДВП, так и показывает эффективность комбинации различных методов, таких как трёхмерное ДВП и компенсация движения.

Литература

1. Kingsbury N.G. The dual-tree complex wavelet transform: A new technique for shift invariance and directional filters. / Proc. 8th IEEE DSP Workshop, Utah. – 1998. – Paper no. 86.
2. Kingsbury N.G. Image processing with complex wavelets. / Philos. Trans. R. Soc. – London: Math. Phys. Sci., Sept. 1999. – Vol. 357, no. 1760, pp. 2543–2560.
3. Kingsbury N.G. Complex wavelets for shift invariant analysis and filtering of signals. / Appl. Comput. Harmon. Anal. – May 2001. – Vol. 10, no. 3, pp. 234–253.
4. Borhani M., Sedghi V. 2-D Dual-Tree Wavelet Based Local Adaptive Image Denoising. / 12th State of Iranian Conference on Electrical Engineering, ICEE2004. – May 2004.
5. Selesnick I.W., Sendur L. Video denoising using 2D and 3D dual-tree complex wavelet transforms. / Proc. SPIE. – Aug 2003. – Vol. 5207.
6. Bo Chen, Zexun Geng, Yang Yang, Tianshuang Shen. Dual-tree Complex Wavelets Transforms for Image Denoising. / Proceedings of SNPD. – Aug. 2007. – Vol. 1, pp. 70–74.

УДК 004.382.73; 004.382.75

СРАВНИТЕЛЬНАЯ ОЦЕНКА ПОТРЕБИТЕЛЬСКИХ КАЧЕСТВ НОУТБУКОВ И ЭЛЕКТРОННЫХ КНИГ

Г.Я. Пантелеев
Научный руководитель – к.т.н., доцент Н.Ф. Гусарова

В мире предлагают много электронных книг и ноутбуков, в частности, «урезанная» версия ноутбука – нетбуки. В статье рассказано о категориях ноутбуков, преимуществах нетбуков и электронных книг. Также сделан краткий обзор двух доминирующих на рынке электронных книг.
Ключевые слова: ноутбук, классы ноутбуков, нетбуки, электронные книги, обзор, Amazon Kindle, Sony Reader PRS-700

Введение

Компьютерные технологии развиваются ускоренными темпами. С приходом нового тысячелетия настольные домашние компьютеры стали достаточно мощными, удобными, компактными. Ноутбуки тоже не стоят на месте. В настоящее время растет спрос на ноутбуки, а спрос на настольные компьютеры (десктоп) постепенно снижается. Есть дешевые и дорогие ноутбуки, есть большие и маленькие. Недавно появился новый класс ноутбуков – нетбук. Выбрать нужное для себя весьма не просто. Но не все задумываются о том, что для чтения книг в электронном виде ноутбук и нетбук – не лучшее решение. Читать на таких устройствах можно. Но для комфортного чтения электронной книги создано специальное устройство – E-book или попросту называется электронной книгой. О ноутбуках, в частности о нетбуках, и об электронной книге и пойдет речь.

Ноутбуки. Какие бывают и кому они нужны?

Все ноутбуки делятся на классы.

1. Ультрапортативные (например, Sony Vaio серии TT, [1]), или, как их называют, субноутбуки. Вес ~1,5 кг. Очень компактные. Это основные требования при построении ноутбуков такого класса. Все остальные характеристики подбираются в соответствии с этими требованиями. Такие составляющие, как винчестер, уменьшены до определенных пределов. Обычно в субноутбуках не ставят процессоры с большой тактовой частотой, т.к. они выделяют много тепла, а воздушного пространства очень мало. Субноутбуки имеют экран с диагональю 10″–12″. Не обладают рекордными характеристиками, стоят в 1,5–2 раза дороже систем с такими же основными характеристиками, но облаченными в массивные корпуса. Нужны деловым людям, которые постоянно работают в командировке.
2. Ноутбуки-трансформеры (например, ноутбуки-трансформеры от HP и Lenovo, [2]), у которых дисплей способен разворачиваться на 180° и размещаться поверх клавиатуры экраном кверху. В итоге превращается в миникомпьютер-планшет. Имеют примерно те же характеристики, что и субноутбук. На таком планшете можно рисовать пером поверх экрана. Перо может использоваться в качестве мыши-заменителя: достаточно касания пером к виртуальной кнопке. Прежде чем остановить выбор на таком ноутбуке, надо подумать сто раз, нужен ли он вам? Действительно ли актуальны его преимущества?
3. Класс «замена настольного компьютера» (desktop replacement, дескноуты – от слова ДЕСКтоп и НОУТбук). Вес – от 3 кг и выше. Это нечто среднее между компактным ноутбуком и десктопом. Отсутствие ограничений на размеры и массу

позволяет снабжать ноутбуки процессорами любой мощности, винчестерами большой емкости и большими дисплеями. Минимизация размера и веса отходит на второй план, а на первый план – улучшение других характеристик системы: производительность, мультимедиа-возможности, цены. Такие ноутбуки делятся на подклассы:

3.1. Бюджетные ноутбуки (офисные ноутбуки) (например, бюджетные ноутбуки Asus, [3]) – недорогие ноутбуки, способные справиться с задачами, не требовательными к ресурсам системы, например, MS Office, интернет-серфинг, простенькие игры типа пасьянса. Можно запускать более тяжелые программы, такие как Adobe Photoshop, Corel Draw, но работа будет некомфортной из-за недостаточной производительности. Преимущества: невысокая цена, продолжительное время работы от одной полной зарядки аккумулятора благодаря интегрированному видеоадаптеру.

3.2. Производительные ноутбуки апгрейдены по максимуму (например, производительные ноутбуки от Alienware, [4]). Они построены на базе процессора Core 2 Extreme, используются в качестве рабочих станций начального и среднего уровней. Наличие крупного экрана (от 17″ и выше) лучше подходят для отображения информации математического моделирования, проектирования и решения других тяжелых вычислительных задач. Стоимость, вес и цена отходит на последний план. Имеют внушительные размер и вес: 3 кг и выше.

3.3. Мультимедийные ноутбуки для использования в качестве развлекательного центра (например, Sony Vaio серии AW, [5]). Сейчас идет тенденция перехода на видео высокой четкости (Full HDTV, Full High-Definition Television, разрешение 1920 × 1080 пикселей) и на оптический носитель Blu-Ray. Для работы с такими данными, а также для запуска тяжелых 3D-игр нужны: очень мощный дискретный видеоадаптер и процессор, емкие накопители и ОЗУ, приличного качества экран и звуковая система (не заменят напольные колонки). В отличие от мультимедийного ноутбука здесь достаточно двух ядер. Имеют те же габариты и вес, что и у мультимедийных. Есть специальная панель управления аудио и видео данными. Ноутбуки такого класса довольно дорогие, но не дороже производительных. Больше пойдут для отдыха, чем для сложных работ с огромными вычислениями.

4. Тонкие и легкие ноутбуки (например, Sony Vaio серии SR, [6]) являются некой серединой между субноутбуком и дескноутом. Вес – от 2 до 2.5 кг. Нет ограничения на конфигурацию, как у субноутбуков. Диагональ экрана: от 14″ до 16.1″. Этот класс – наиболее распространенный.

Недавно появились нетбуки [7]. За короткое время они успели наделать немало шума во всем мире. Нетбуки – это среднее между КПК и полноценным ноутбуком. Это маленький и легкий «ноутбук» со слабой мощностью, низкой стоимостью. Имеют достаточно маленькие вес и габариты. Диагональ экрана – 11″ и ниже. Предназначены, в первую очередь, для доступа в Интернет, работы с офисными программами. На большее рассчитывать не стоит. Большинство нетбуков построено на базе процессора Intel Atom, а вместо жёсткого диска в них используется твердотельный накопитель.

Битва за место между ноутбуком и нетбуком

Современные субноутбуки не всегда подходят для поездок и командировок. Их размеры могут не всех устроить или субноутбук некоторым покажется тяжелым. Если вы обладаете 13,3″ ноутбуком, но стоите перед выбором: брать ли его с собой в командировку или нет (предположим, вам вроде нужен, но не хочется таскать килограммовую машину), при этом у вас ограничены средства на покупку субноутбука. В этом случае пойдет нетбук.

Нетбук – это «полноценный» ноутбук с операционной системы Windows XP или

Linux на борту, имеет примерно такой же размер, как и субноутбук (диагональ экрана до 10″ против 11″). Очень легкий. Основная изюминка – низкая цена. В среднем, в три раза дешевле бюджетного ноутбука! Возможности у бюджетного ноутбука и нетбука примерно одинаковы! Его можно с легкостью взять в поездку. Интернет-серфинг под рукой в любом месте, где это возможно. Его средние характеристики: одноядерный процессор Intel Celeron или Intel Atom; ОЗУ 512 Мб – 1 Гб; твердотельный накопитель на базе флэш-памяти (SSD) емкостью 12 Гб или жесткий диск (HDD) емкостью 80 Гб; Wi-Fi, Bluetooth, USB, аудиовыход для наушников, микрофонный вход, веб-камера; вес около 1 кг. Минусом нетбука является невозможность запускать приложения, требующие мало-мальски повышенного уровня производительности. На мой взгляд, если вам действительно нужно устройство, позволяющее с комфортом находиться в сети, набирать не очень большие тексты (из-за миниатюрности страдает эргономика клавиатуры), получать почту и прочее, то нетбук – это ваш выбор. Он идеален в качестве второго компьютера, который можно брать с собой каждый день.

Совсем недавно анонсировали и выставили на продажу очень интересный, красивый и хорошо продуманный нетбук Sony Vaio серии P [8]. Главная фишка – размерность клавиатуры составляет 80% от стандартного размера стационарной клавиатуры и великолепный 8″ экран с LED подсветкой с разрешением 1600×768 пикселей. Он является самым легким и компактным в мире – вес составляет всего 640 г. и можно поместить в карман пиджака. В форумах (например, презентация Sony VAIO P и первые впечатления [9], обзор ноутбука Sony VAIO P [10]) активно обсуждает его и вызывает большой интерес. По мнению форумчан он является хорошо сбалансированным.

В ближайшем будущем нетбуки будут оснащены процессором с двумя ядрами. Благодаря этому значительно увеличится производительность. Они смогут вытеснить бюджетные ноутбуки, а цены на ноутбуки остальных классов, возможно, снизятся.

Кроме того, на мой взгляд, будущее поколение – это Интернет-приложения. Например, Adobe Photoshop Express [11]. Для таких программ хорошо подойдут Интернет-десктопы. Например, в Японии есть модель от Sharp AQUOS [12] на платформе некой ОС, заточенно под использование Интернет-приложений. Есть все, что и у обычного десктопа, но не использует «локальные» приложения. Все личные и мультимедиа данные хранятся на HDD. Для такого десктопа необходимым условием является достаточно высокая скорость Интернет-соединения.

На каком устройстве лучше читать книжки?

На ноутбуках возможно читать книжки, сохраненные в электронном виде. Но для длительного чтения лучше подойдут электронные книги (E-book device). Основная особенность состоит в том, что вместо обычного экрана используется электронная бумага. Электронная бумага [13] (англ. e-paper, electronic paper; также электронные чернила, англ. e-ink) – это технология отображения информации, разработанная для имитации обычных чернил на бумаге. Она отображает изображение в отраженном свете, как обычная бумага. Может показывать текст и графику без потребления электричества долгое время и потребляет его только при обновлении изображения. При этом точки изображения стабильны, т.е. не меняют цвет даже при отсутствии постоянного напряжения. Её преимущества: нет подсветки – человеческий глаз не устает, т.к. электронная бумага отражает свет, как обычный печатный лист (об этом подтверждается результат исследования воздействия экрана на зрение [14]); угол обзора значительно больше, чем у ЖК; более легкая, надежная, очень тонкая (сгибается почти так же, как обычная бумага). Электронные книги имеют функцию нумерации страниц, оглавления, перелистывания страниц. Было выпущено не мало электронных книг, но

рассмотрим две доминирующие на рынке: Amazon Kindle и Sony Reader PRS-700.

Amazon Kindle

Это устройство первого поколения выпускает американский интернет-магазин Amazon Kindle [15]. Оно используется без синхронизации с компьютером. Встроен EVDO/CDMA модем, который обеспечивает бесплатную связь через американский мобильный оператор Sprint [16]. После включения электронной книги можно выбрать одну из 90 000 книг самого разного жанра и через несколько секунд читать. Первые главы доступны бесплатно, а для прочтения всей книги можно скачать целиком за отдельную небольшую плату. Можно подписываться на получение электронных версий газет, журналов и блогов. Подписка платная – несколько долларов в месяц за каждый блог. Может искать информацию в «Википедии» [17] и в Google [18], а также открывать ссылки из блогов в упрощённом веб-браузере. Kindle автономна. Sprint доступна в США, а без него онлайновые сервисы Amazon недоступны.

Внешний вид электронной читалки Kindle неказист. Острые углы, нестандартные кнопки и мозаика из букв на задней панели – понравится не каждому. Дисплей шестидюймовый монохромный, 4 градации яркости (что очень мало), разрешение 600×800 пикселей, нет функции сглаживания и подсветки. Информация на дисплее воспринимается как на обычной бумаге, можно читать без труда даже под прямыми солнечными лучами. В темноте становится не читаемой и тогда придется использовать внешний фонарик. Т.к. дисплей на основе электронных чернил, то у него малое энергопотребление. Аккумуляторы Kindle продержатся до 30 часов. Если отключить беспроводные технологии, то продержится дольше. Полная зарядка занимает два часа. Электронные чернила на этом устройстве работают очень медленно. На обновление всего экрана требуется больше секунды, поэтому о прокрутке текста и речи быть не может. Текст листается постранично с помощью двух больших левых кнопок – нижняя ведёт на следующую страницу, а верхняя - возвращает на предыдущую. Для выбора пункта меню используется колесико прокрутки, которое располагается в правой части устройства. Левее колесика есть очень узкий и высокий жидкокристаллический дисплей. Он отображает бегунок, заменяет курсор при выборе пунктов меню, иногда используется в качестве индикатора и отображает, например, процесс загрузки файла. В нижней части располагается встроенная клавиатура, которая предназначена для ввода названия книги в поисковой строке или написания заметок.

В Kindle встроено 256 Мб памяти, что равносильно ~200 книг. Можно расширить память с помощью SD-карточек. Устройство позволяет закачивать аудиокниги, MP3-файлы и прослушивать. Для этого в Kindle есть встроенный динамик на задней стороне [19] и 3.5 мм разъём для подключения наушников в нижней части [20].

За пределами США не имеет смысла использовать Kindle в силу неразрывной связи с Amazon.com через Sprint. Даже взламывание данного устройства не имеет смысла, т.к. без доступа к Amazon.com данное устройство теряет свое главное достоинство. Купленные в Amazon книги хранятся в защищённом виде, в проприетарном формате. Это специально для защиты от копирования. Электронные книги нельзя копировать, продавать, а их содержимое может быть изменено в любой момент. Нет полноценной поддержки распространенного формата PDF. Файлы разных форматов можно залить в устройство Kindle двумя способами: отправить их в Amazon на уникальный e-mail адрес, получаемый при покупке устройства, для платной конвертации или скопировать данные, подключив к компьютеру. Но, в любом случае, данные конвертируются в специальный формат, который не сохраняет форматирование текста, который есть в PDF. Разметка сбивается, таблицы портятся.

Sony Reader PRS-700

Это первая электронная книга третьего поколения [21], обладающая сенсорным дисплеем с подсветкой. В итоге получаем усовершенствованную электронную книгу Sony Reader PRS-505, которая относится ко второму поколению [22]. Из-за сенсорного экрана полностью переработано программное обеспечение по сравнению с предыдущей 505-ой моделью. Под сенсорным экраном подразумевается не сам E-ink экран, а надстройка сверху существующего экрана от 505-ой модели, в виде пластиковой и стойкой к повреждениям пластины с сенсорными функциями. Просто разработчики E-Ink не сделали готового решения. В итоге, сенсорный экран, как дополнительный светофильтр, снижает контрастность всего того, что на E-ink экране. Но в Sony поработали очень много над тем, чтобы минимизировать потерю контрастности, насколько это возможно. Если поставить рядом 505-ую и 700-ую модели и сравнить [23], то разница видна, но все равно контрастность у 700-ой модели на достаточно хорошем уровне для удобного чтения книги. Без сравнения потеря контрастности не ощутима. Хочу подчеркнуть, что ни один конкурент не удосужился сделать электронную книгу с сенсорным экраном. Характеристики 6″ E-Ink экрана: разрешение 600×800 пикселей, 8 уровней серого.

Дизайн – еще один повод для того, чем может гордиться Sony. Устройство сделано очень аккуратно, без щелей и острых неоправданных углов. Корпус гладкий, на ощупь — холодный. Наличие обложки в этой модели оправдано. Обложка из кожи или заменителя. На лицевой стороне красуется тисненная надпись «Sony» [24]. В нижней части, на торце устройства [25], сосредоточенны редко используемые разъемы, выключатели устройства и подсветки с возможностью выбора одной из двух градаций подсветки, регулировка громкости звука. В верхней части - разъемы для двух типов карт – Memory Stick DUO и SD. На скошенной правой части устройства находится стилус [26] – необязательное для управления устройством приспособление, т.к. достаточно легко управлять пальцем, причем даже не ногтем, а подушечкой пальца. На тыльной стороне есть отверстие Reset. Т.к. экран сенсорный, то физических кнопок минимум. Они находятся под экраном [27]. Наличие тактильных ощущений благодаря сенсорному экрану упрощает взаимодействие, но требует продуманности конструкции. Нет необходимости изучать, какую кнопку надо нажать для выбора меню, или как пролистать страницу. Достаточно определить, кто вы – левша или правша в настройках. Это разница в мышлении и удобстве. Вы сможете определить направление движения пальцев по экрану по своему вкусу. Можно управлять жестом, например, для листания путем движения вперед пальцем слева направо. Меню вызывается легко, прикосновением к сенсорной области на экране. При повороте экрана все меню в устройстве поворачиваются на 90°, в том числе движения пальцев по экрану, для листания. Сенсорное управление более естественное, к нему привыкнуть гораздо проще, понять логику работы устройства можно гораздо быстрее. Это удобно, особенно для новичков. Подсветка экрана осуществляется над дисплеем E-Ink, т.к. он не прозрачен, с помощью нескольких светодиодов, которые расположены с двух сторон. Освещение экрана неравномерное и выполняется несколькими пучками-прожекторами. В темноте к чтению информации на дисплее с такой подсветкой можно привыкнуть. Особенно при чтении горизонтально. В освещенном помещении можно выключить подсветку. Наличие подсветки есть только у Sony, только у 700-ой модели. Физические кнопки, расположенные под экраном, позволяют осуществлять возврат или отказ от действия; листание страницы; возврат в главное меню устройства; поиск; масштабирование, в частности управление размера шрифта (S, M, L, XL, XX); выполнение настройки устройства. Данная электронная книга имеет функцию книжной полки; сортировки книг по названию, по автору и по дате появления книги; создание, управление и удаление заметок; оглавление книг; манипулирование книгами. Все книги хранятся не в случайном

порядке, а на одной полке в одном шкафу, а для остального выбора порядка предназначена функция списка коллекции книг. В книжной полке можно видеть даже обложки книг и на каком носителе расположена та или иная книга. В правой части окна книжной полки находится буквенный указатель, размещенный вертикально. Поддерживаемые форматы книг: BBeB, ePub, TXT, RTF, PDF, DOC.

Сенсорное управление настраивается под ваше требование. Настройка движения пальцем для листания задается в настройках устройства. Доступны два варианта: слева-направо и справа-налево. Это удобно для правши и левши. Управление листанием очень простое и удобное: достаточно прикоснуться пальцем по экрану и выполнить движение влево или вправо. Если потребуется выделить текст для поиска или создания заметки — достаточно прикоснуться к букве и провести пальцем до конца слова/ предложения и затем выполнить поиск или работу с закладками.

Также устройство позволяет прослушивать аудио данные только через стереонаушники и просматривать фотографии. Аккумулятор в режиме плеера расходуется достаточно быстро, примерно 3 часа. Устройство не требует постоянного подключения к беспроводной сети. В режиме чтения книги полная зарядка аккумулятора хватает на перелистывание 7500 страниц.

Заключение

Amazon Kindle имеет ряд недостатков, такие как платная услуга чтения книги, нет возможности нормального копирования своих текстовых данных, слабый дисплей, дешевый дизайн, доступен только для американцев (для американцев это не является недостатком). Но есть и преимущества: можно добраться до желаемого печатного продукта за секунды, минуя заказ бумажных книг, подписи на газеты. Встроенная клавиатура — спорное решение: занимает много места и не всем это обязательно. Некоторым удобнее использовать сенсорный экран.

У Sony Reader PRS-700 нет конкурентов. Бледность экрана – завышенное мнение пользователей. Даже в общественном транспорте, где освещение не достаточно хорошее, можно провести нормальное чтение. Подсветку достаточно включить там, где света меньше или вообще нет его. Функциональные возможности и простота использования очень хорошо продуманы. Дизайн и качество на высоте. Нет таких ограничений с переносами текстовых данных и их чтением, как у Amazon Kindle. Наличие подсветки и сенсорного продуманного управления только в плюс.

Я провел сравнительную оценку двух доминирующих на рынке электронных книг Amazon Kindle и Sony Reader PRS-700 методом фокус-группы. Результаты оценки приведены соответственно в табл. 1, в табл. 2.

	Владелец	Автор обзора 1	Автор обзора 2	Комментатор 1	Комментатор 2
Экран	3	4	3	3	3
Дизайн	4	4	4	3	3
	Владелец	Автор обзора 1	Автор обзора 2	Комментатор 1	Комментатор 2
Управление	4	3	3	4	5
Функциональность	5	5	4	5	5
Качество	4	4	3	4	4
Общая оценка	20	20	17	19	20
Средняя оценка	19,2				

Таблица 1. Оценка устройства Amazon Kindle

	Владелец	Автор обзора 1	Автор обзора 2	Комментатор 1	Комментатор 2
Экран	4	4	4	3	3
Дизайн	5	5	5	5	5
Управление	5	5	5	4	5
Функциональность	5	5	4	4	4
Качество	5	5	5	5	5
Общая оценка	24	24	23	21	22
Средняя оценка	22,8				

Таблица 2. Оценка устройства Sony Reader PRS-700

Оценка экрана электронной книги Sony Reader PRS-700 комментаторами несколько занижены в силу невозможности передачи всего преимущества из-за возникновения при фотографировании бликов на сенсорной подложке. Мнение опрошенных, в общем, совпадает с тем, что печатается в литературе. Поэтому можно с уверенностью сделать вывод о том, что Sony Reader PRS-700 – лучшая электронная книга на данный момент. И не смотря на то, что у нас официально не продается, все равно есть не мало покупателей, которые хотят и покупают данное устройство.

Нетбуки предназначены для выполнения работ в программах с невысокими требованиями к ресурсам и позволяют брать с собой каждый день из-за своего легкого веса и размера.

Литература

1. Sony Vaio серии TT / Sony – Режим доступа: http://vaio.sony.ru/view/ShowProduct.action?product=VGN-TT11RM%2FR&site=voe_ru_RU_cons&category=VN+TT+Series&assetid=1218032875588, свободный. – Загл. с экрана. – Яз. рус., англ.
2. Ноутбуки-трансформеры от HP и lenovo / Cnews – Режим доступа: http://zoom.cnews.ru/publication/item/982, свободный. – Загл. с экрана. – Яз. рус., англ.
3. Бюджетные ноутбуки Asus / Asus – Режим доступа: http://www.asusnb.ru/cgi-bin/catalog.pl#s_4, свободный. – Загл. с экрана. – Яз. рус., англ.
4. Производительные ноутбуки от Alienware / Alienware – Режим доступа: http://www.alienware.com/products/notebook-computers.aspx, свободный. – Загл. с экрана. – Яз. рус., англ.
5. Sony Vaio серии AW / Sony – Режим доступа: http://vaio.sony.ru/view/ShowProductCategory.action?site=voe_ru_RU_cons&category=VN+AW+Series&assetid=1218032875632, свободный. – Загл. с экрана. – Яз. рус., англ.
6. Sony Vaio серии SR / Sony – Режим доступа: http://vaio.sony.ru/view/ShowProductCategory.action?site=voe_ru_RU_cons&category=VN+SR+Series&assetid=1218032875588, свободный. – Загл. с экрана. – Яз. рус., англ.
7. Новости о нетбуках / нетбуки – Режим доступа: http://asus-eee-pc.ru, свободный. – Загл. с экрана. – Яз. рус., англ.
8. Sony Vaio серии P / Sony – Режим доступа: http://vaio.sony.ru/view/ShowProductCategory.action?site=voe_ru_RU_cons&category=VP+P+Series&assetid=1218032875552, свободный. – Загл. с экрана. – Яз. рус., англ.
9. Презентация Sony VAIO P и первые впечатления / forum.mobile-review.com – Режим доступа: http://forum.mobile-review.com/showthread.php?t=64464, свободный. – Загл. с экрана. – Яз. рус., англ.
10. Обзор ноутбука Sony VAIO P / forum.mobile-review.com – Режим доступа: http://forum.mobile-review.com/showthread.php?t=64665, свободный. – Загл. с экрана. – Яз. рус., англ.

11. Adobe Photoshop Express / photoshop – Режим доступа: https://www.photoshop.com/express/landing.html, свободный. – Загл. с экрана. – Яз. рус., англ.
12. Интернет-десктоп от Sharp AQUOS / Engadget – Режим доступа: http://www.engadget.com/2007/11/07/sharp-kicks-out-trio-of-new-internet-aquos-desktops/, свободный. – Загл. с экрана. – Яз. рус., англ.
13. Электронная бумага / Википедия – Режим доступа: http://ru.wikipedia.org/wiki/Электронная_бумага, свободный. – Загл. с экрана. – Яз. рус., англ.
14. Раздел "05.12.2005" / Tet-service – Режим доступа: http://tet-service.ru/arc/, свободный. – Загл. с экрана. – Яз. рус., англ.
15. Интернет-магазин Amazon Kindle / Amazon – Режим доступа: http://www.amazon.com/Kindle-Amazons-Wireless-Reading-Device/dp/B000FI73MA, свободный. – Загл. с экрана. – Яз. рус., англ.
16. Оператор Sprint / Sprint – Режим доступа: http://www.sprint.com, свободный. – Загл. с экрана. – Яз. рус., англ.
17. Википедия / Википедия – Режим доступа: http://www.wikipedia.org, свободный. – Загл. с экрана. – Яз. рус., англ.
18. Поисковая система Google / Google – Режим доступа: http://www.google.com, свободный. – Загл. с экрана. – Яз. рус., англ.
19. Фото задней стороны электронной книги Amazon Kindle / Reeed – Режим доступа: http://reeed.ru/foto/kindle/ru/02/kindle_rev_202.jpg, свободный. – Загл. с экрана. – Яз. рус., англ.
20. Фото нижней стороны электронной книги Amazon Kindle / Reeed – Режим доступа: http://reeed.ru/foto/kindle/ru/02/kindle_rev_203.jpg, свободный. – Загл. с экрана. – Яз. рус., англ.
21. Sony Reader PRS-700 / SonyStyle – Режим доступа: http://www.sonystyle.com/webapp/wcs/stores/servlet/ProductDisplay?catalogId=10551&storeId=10151&langId=-1&productId=8198552921665562069, свободный. – Загл. с экрана. – Яз. рус., англ.
22. Sony Reader PRS-505 / SonyStyle – Режим доступа: http://www.sonystyle.com/webapp/wcs/stores/servlet/ProductDisplay?catalogId=10551&storeId=10151&langId=-1&productId=8198552921665245739, свободный. – Загл. с экрана. – Яз. рус., англ.
23. Фото сравнения экрана электронных книг Sony Reader PRS-505 и Sony Reader PRS-700 / Reeed – Режим доступа: http://reeed.ru/foto/readers/sony/700/ru/4/dc4c5zfs.jpg, свободный. – Загл. с экрана. – Яз. рус., англ.
24. Фото обложки электронной книги Sony Reader PRS-700 / Reeed – Режим доступа: http://reeed.ru/foto/readers/sony/700/ru/4/dc4c5zfw.jpg, свободный. – Загл. с экрана. – Яз. рус., англ.
25. Фото нижней части, на торце электронной книги Sony Reader PRS-700 / Reeed – Режим доступа: http://reeed.ru/foto/readers/sony/700/ru/4/dc4c5zfu.jpg, свободный. – Загл. с экрана. – Яз. рус., англ.
26. Фото стилуса электронной книги Sony Reader PRS-700 / Reeed – Режим доступа: http://reeed.ru/foto/readers/sony/700/ru/4/dc4c5zft.jpg, свободный. – Загл. с экрана. – Яз. рус., англ.
27. Фото основных кнопок электронной книги Sony Reader PRS-700 / Reeed – Режим доступа: http://reeed.ru/foto/readers/sony/700/ru/4/dc4c5zfz.jpg, свободный. – Загл. с экрана. – Яз. рус., англ.

УДК 519.683.8

МЕТОДЫ АВТОМАТНОГО ПРОГРАММИРОВАНИЯ В РАЗРАБОТКЕ WEB-ПРИЛОЖЕНИЙ

А.В. Бульёнов

Научный руководитель – д.т.н., профессор А.А. Шалыто

Основной недостаток классических методов разработки web-приложений – отсутствие гибкости на достаточно больших приложениях. На основе этого был сделан вывод о том, что наиболее удобным методом разработки web-приложений является автоматный подход. В этой статье описаны существующие методы разработки ПО с использованием автоматного подхода и сделаны выводы об их удобстве и целесообразности.

Ключевые слова: автоматный подход, web-приложения, моделирование, методы разработки программного обеспечения

Введение

Существует большое количество подходов к разработке программного обеспечения. Большинство из этих подходов универсально и применяется практически везде, в том числе и в разработке web-приложений.

Однако существующие подходы зачастую не учитывают особенностей web-приложений.

- web-приложения сложны иерархически (имеют немало страниц и их взаимосвязь зачастую неочевидна), и существующие методики не позволяют эффективно управлять большими проектами;
- web-приложения зачастую имеют сложное визуальное представление, которое зависит от множества факторов: отображаемых данных, выбора пользователя и т.д.;
- слишком велика зависимость отображаемых данных от истории выполненных ранее действий;
- не существует четкого и систематизированного графического представления на этапе проектирования

Таким образом, необходимо выработать такой подход, который позволил бы быстро разрабатывать web-приложения со сложной структурой, имел удобное графическое представление его элементов и позволил бы использовать преимущества других существующих подходов.

Всем этим требованиям отвечает автоматный подход. Он обеспечивает:

- удобное визуальное представление на различных этапах разработки;
- эффективную работу со сложными иерархическими структурами;
- сохранение истории и контекста выполнения [1].

Разработку любого приложения (в том числе и web-приложения) можно условно разделить следующие этапы [2]:

- постановка задачи;
- анализ исходных данных;
- выбор архитектуры и шаблонов программирования и т.д.;
- реализация на выбранном языке программирования;
- тестирование и усовершенствование.

Ниже мы укажем применение автоматного подхода на этапах проектирования и программирования и опишем различные варианты состояний в терминах web-программирования. Мы сравним существующие методы моделирования web-

приложений в рамках автоматного подхода и опишем дальнейшие перспективы их развития.

1. Состояние как страница

Ключевое понятие автоматного подхода [3] – состояние – можно перенести на разработку web-приложений [4]. Каждую страницу мы представим в виде состояния, а переходы между страницами – в виде переходов автомата. Входным воздействием будет являться адрес *URL* до нужной страницы.

На рис. 1 приведен *граф переходов* [3] несложного сайта: на главной странице («Новости») находятся ссылки на новости и ссылки на разделы «Статьи» и «Об авторе». По нажатию на ссылку «Статьи» будет открыта страница, ведущая на сами статьи и на остальные основные разделы («Новости» и «Об авторе»). В разделе «Об авторе» находится информация об авторе сайта и ссылки на другие разделы.

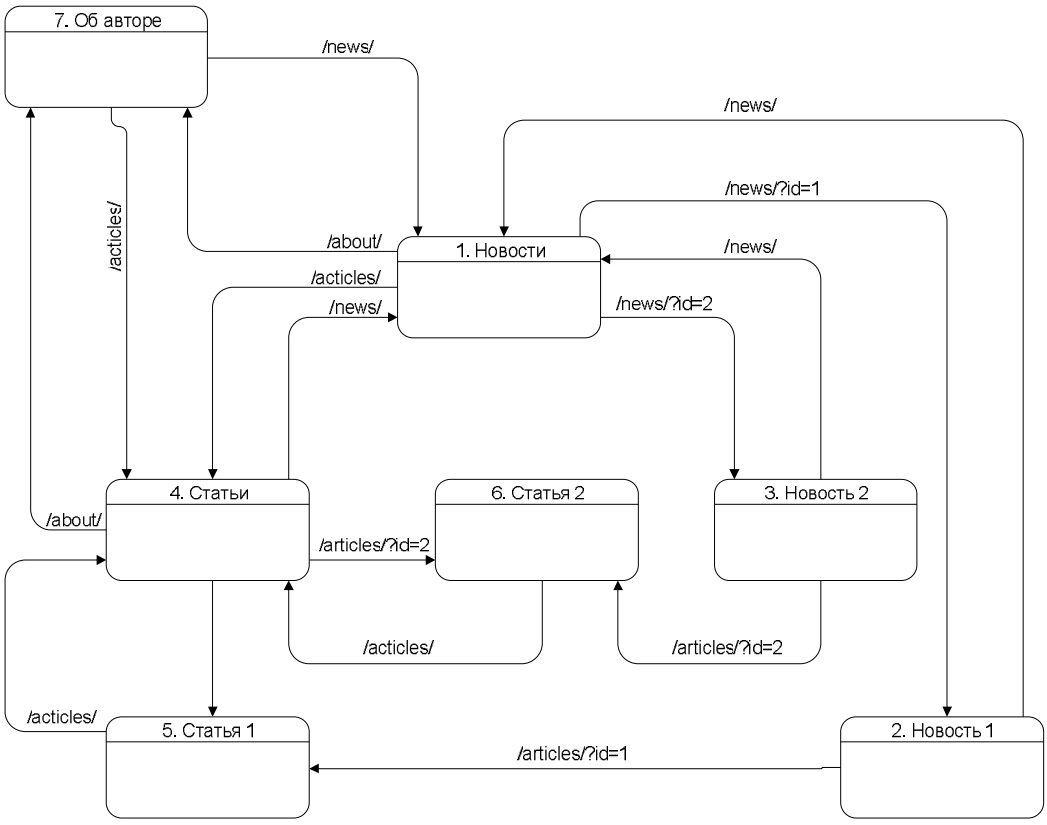


Рис. 1. Диаграмма переходов для метода моделирования «Состояние как страница»

Представление, приведенное на рис. 1 неудобно для разработки: в случае достаточно сложного web-приложения число состояний будет слишком велико, и работа с сайтом, промоделированным в виде автомата, совершенно неочевидна. Кроме того, представленная модель не отражает передачу параметров *POST* и *COOKIE*, генерацию страницы и работу с базами данных.

2. Состояние как кластер

Чтобы избежать большого количества состояний в [5] было предложено использовать метод объединения в кластеры. Кластер – состояние, характеризующее не одну страницу, а группу страниц, объединенных по общности структуры, данных или по каким-либо другим признакам. В [5] в качестве кластера были представлены только

группы страниц, однако деление на группы не решает проблем разработки: не существует четких определений, как организовывать работу web-приложения на практике и как выполнять разделение на страницы.

В данном случае более логично перейти к программам, которые выполняют генерацию страницы. Каждая программа, являющаяся в свою очередь состоянием, получает *GET*, *POST* и *COOKIE* параметры на входе, а на выходе возвращает *HTML*-код. Этот вариант решения задачи приведен на рис. 2.

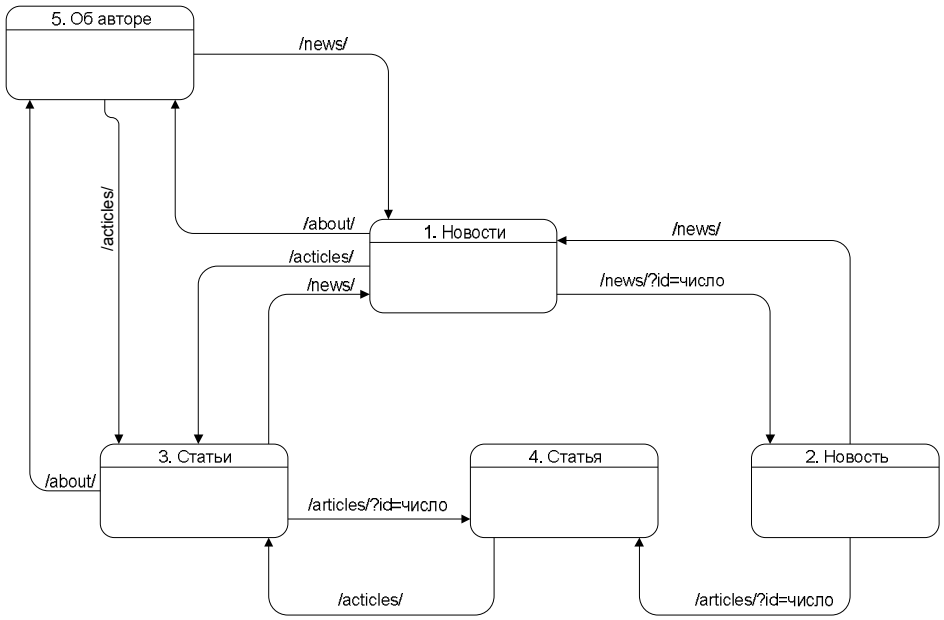


Рис. 2. Диаграмма переходов для метода «Состояние как кластер»

В этом случае такие страницы, как «Новость 1» и «Новость 2», объединены в одну, а в качестве параметра они получают идентификатор новости для дальнейшей работы.

Подход с использованием кластеров решает проблему большого количества состояний, однако вопрос о визуальном представлении данных (точнее, о том, что и в каком случае будет видеть пользователь) не может быть решен этим методом. В [5] подход также не содержит рекомендаций по реализации приложения и является чисто умозрительным.

3. Состояние как элемент PHC

Одним из вариантов избежать указанных выше недостатков является метод, предложенный в [6]. Этот подход заключается в выделении групп ссылок, которые обеспечивают взаимодействие с пользователем. Каждая их групп ссылок (в работе [6] они названы *пассивными элементами управления* или *Passive HTML Controls – PHC)* моделируется отдельным конечным автоматом.

Каждый *PHC-автомат* представляет собой пятерку элементов *(E,O, S, R, F)*:

E – конечный набор ссылок;

O – конечное множество функций выхода *O(P, DB)*, определяющих результат конкретного элемента в конкретном состоянии;

S – конечный набор состояний;

$R \in S$ – начальное состояние;

F – функция переходов, которая описывается следующим выражением:

$F : (E \times S) \to (O \times S)$

Каждое состояние соответствует странице или программе, которая выполняет ее генерацию. Параметры для конкретного состояния хранятся в *сессии* – в связанной с пользователем базе данных. Доступ к этой базе данных осуществляется по идентификатору сессии, передаваемому в состояние. В конкретном состоянии обрабатываются необходимые параметры из сессии. Использование механизма *PHC* позволяет сделать автономными элементы управления и, по мнению авторов подхода, обеспечивает независимость отдельных пассивных элементов управления от внешнего представления.

В рассматриваемом примере можно выделить несколько *PHC*-автоматов:

- Автомат, отвечающий за главное меню («Новости», «Статьи», «Об авторе»).
- Автомат, отвечающий за отображение новостей.
- Автомат, отвечающий за обработку и отображение статей.

Диаграмма переходов для первого автомата из этого списка приведена на рис. 3.

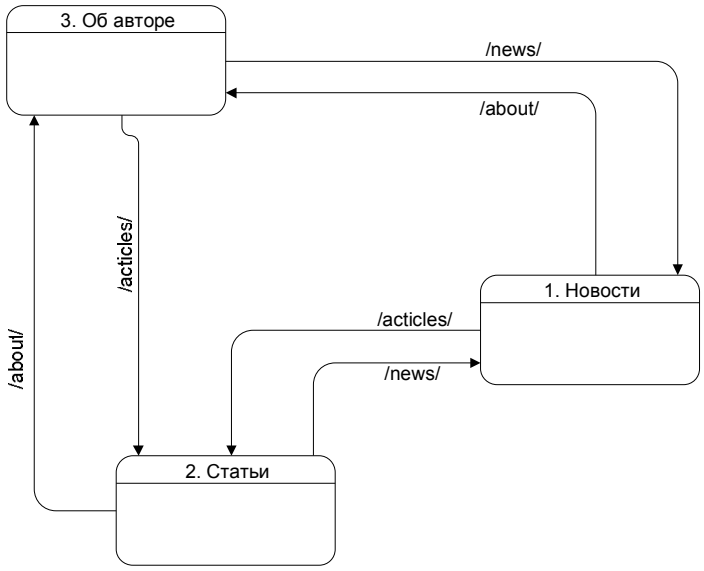


Рис. 3. Диаграмма переходов для PHC-автомата главного меню сайта

Для удобства разработки авторами подхода [6] были предложены и реализованы два языка программирования: *язык разметки* и *язык обработки данных*. Связь между отдельными PHC осуществляется через специальный интерфейс PHCI.

Недостатком данного подхода является слишком сильная связь с ссылками: авторы не рассматривают ни *HTML-формы*, ни *JavaScript.* Кроме того, не существует четкого представления о том, как объекты предметной области будут храниться в базе данных.

4. Состояние как действие блока страницы

В [7] был предложен более эффективный метод моделирования web-приложения. Каждый блок страницы (вне зависимости от того, является он PHC или нет) моделируется автоматом с набором состояний. При выполнении какого-либо действия выполняется смена состояния конкретного блока. Такой блок может соответствовать шапке, подвалу, меню сайта, области отображения *контента* и т.д.

Таким образом, разработка web-приложения сводится к созданию привычного для большинства разработчиков вида страницы, поделенного на блоки, которые могут взаимодействовать друг с другом.

Заключение

В данной статье были рассмотрены основные подходы в разработке web-приложений. Были указаны недостатки существующих подходов к разработке и был выдвинут тезис о том, что использование автоматного подхода сможет сделать разработку web-приложений более эффективной.

В этой статье были также рассмотрены следующие подходы к моделированию и разработке web-приложений с использованием автоматного подхода:

- представление страниц в виде состояния;
- представление наборов страниц в виде состояния;
- представление элементов управления в виде автоматов;
- представление логических блоков страницы в виде автоматов.

В работе были описаны достоинства и недостатки каждого из вышеперечисленных методов.

Каждый из этих подходов является логическим продолжением предыдущего, однако, по мнению авторов этой статьи, даже последний его вариант не является идеальным.

Таким образом, автоматный подход для разработки web-приложений применим, однако пока не существует техник, которые смогут составить конкуренцию существующим неавтоматным методикам.

Литература

1. Сытник С.А. Создание автоматных веб-приложений. – 2005.
2. Брауде Эрик Дж. Технология разработки программного обеспечения. СПб: Питер. – 2005. – 121 с.
3. Поликарпова Н., Шалыто А. Автоматное программирование. СПб: Питер. – 2009. – 20 с.
4. Konstantin Laufer. Interactive Web Applications Based on Finite State Machines / Loyola University Chicago. Чикаго. – 1998. – С. 1–5.
5. Anneliese A. Andrews, JeffOffutt, Roger T. Alexander. TestingWeb applications bymodeling with FSMs. – 2005. – С. 326–330.
6. Karl M. Goeschka and Juergen Falb. Using Finite State Machines as Design and Engineering Model for Database Backed Web Applications // Proceedings of the 33rd Hawaii International Conference on System Sciences. – 2000.
7. Tao He, Huaikou Miao. Modeling and Composition of Web Application Components using Extended FSM. // Fourth International Conference on Natural Computation. – 2008.
8. Горшкова Е.А., Новиков Б.А., Гуров В.С. и др. Моделирование контроллера web-приложений с использованием UML //Программирование. – 2005. – №1. – С. 44–51.
9. Коротков М.А., Лукьянова А.П., Шалыто А.А. Система управления взаимодействием скриптов в Web-программировании: Проектная документация. СПб. – 2004 – С. 1–7.

УДК 004.453

РАЗРАБОТКА ПАРАМЕТРИЗУЕМЫХ ИНТЕРФЕЙСОВ ВИДЖЕТОВ ДЛЯ ИНТЕРАКТИВНОЙ МНОГОПОЛЬЗОВАТЕЛЬСКОЙ ВЕБ-СИСТЕМЫ

И.В. Кузнецова, Д.Ф. Сулейманов, Д.Г. Николаев
Научный руководитель – к.т.н., доцент Д.Г. Штенников

В статье рассмотрен подход к проектированию интерфейсов мини-приложений, основанный на непрерывном исследовании предпочтений пользователей. Описан пример применения этого метода при проектировании интерфейсов интерактивной многопользовательской веб-системы. Предложенный подход может быть адаптирован к процессу разработки широкого круга программных продуктов различной направленности.

Ключевые слова: интерфейс, проектирование, виджет, юзабилити

Введение

Традиционно большинство разработок программного обеспечения ведется в отрыве от конкретных конечных пользователей: сначала разрабатывается бета-версия, а затем начинается работа, связанная с поиском покупателей, маркетинговым позиционированием и PR. Стив Бланк, успешный предприниматель и автор книги «The Four Steps for the Epiphany», предложил усовершенствовать процесс разработки продукта с помощью *модели исследования потребителей* (Customer Development Model). Ее суть заключается в необходимости как можно раньше и как можно чаще проверять свои идеи и предположения на конкретных людях. Это позволяет сфокусироваться не на разработке отдельных функциональных элементов, а на понимании потребителей, их проблем и потребностей.

Необходимость детального исследования предпочтений пользователей обоснована тем, что создание нового продукта или сервиса начинается с в*и*дения: как он будет использоваться и почему множество людей будет его покупать. Но б*о*льшая часть из того, что думают разработчики о рынке и потенциальных потребителях – это всего лишь догадки. Для того, чтобы преобразовать в*и*дение в реальную картину, необходимо протестировать эти догадки или гипотезы и выяснить, какие из них верны. Таким образом, основная цель проведения исследования предпочтений пользователей заключается в следующем: преобразовать исходные гипотезы о нуждах потребителей в факты. А поскольку факты находятся вне стен офиса, основная задача на данном этапе – найти потенциальных пользователей и пообщаться с ними лично. Только после этого можно сделать вывод о том, имеет ли изначальное предположение что-либо общее с реальностью [6].

Целью исследования являлась реализация веб-интерфейса, учитывающего как современные тенденции юзабилити, так и пожелания потенциальных пользователей системы на примере виджетов.

Сбор требований и проектирование интерфейсов виджетов

Виджеты – это класс веб-приложений, работающих на стороне клиента, предназначенных для отображения и обновления локальных или удаленных данных [9].

Виджетом может быть отдельная утилита или модуль в программе, приложение для показа погоды или демонстрации потокового видео. Четкого и ясного определения дать нельзя, хотя в определенной степени виджет можно охарактеризовать как простейшую программу, выполняющую ту или иную функцию, действие. Помимо выполнения исключительно полезных функций, вроде отображения информации или ново-

стей на рабочем столе, виджеты исполняют и функцию декоративную. Многие из них сделаны в определенном стиле и могут служить декоративным элементом при оформлении рабочего стола. При этом виджеты, как неотъемлемая часть современных веб-проектов, востребованы более чем 80% пользователей. Популярность мини-приложений подтверждается существованием на Западном рынке ряда коммерчески успешных проектов: Netvibes, iGoogle и других.

Разрабатываемые интерфейсы предназначены для использования в рамках виджетоориентированной веб-платформы spooort.ru. Пути монетизации этой платформы – размещение таргетированной рекламы и предоставление платных сервисов – предполагают необходимость значительной базы пользователей. Для того, чтобы предлагаемый интерфейс максимально удовлетворял требованиям потенциальных пользователей, было проведено исследование их предпочтений методом интервью.

Последовательность действий для проведения сбора требований представлена на рис. 1.

Рис. 1. Исследование предпочтений пользователей

Исходя из метода, предложенного Стивом Бланком, было проведено две серии интервью с потенциальными пользователями виджетов.

Целью первой серии интервью было выяснить, является ли идея использования виджетов в онлайн социальной сети перспективной. И если это так, то какие возможности наиболее востребованы среди потенциальных пользователей. В качестве респондентов были выбраны активные представители спортивного сообщества, поскольку платформа spooort.ru ориентирована именно на любителей спорта. Интервью проводились в соответствии с специально разработанным сценарием. Основные вопросы, вошедшие в интервью, приведены в списке ниже:

– Как Вы обычно используете Интернет для организации своей спортивной жизни? Читаете новости, общаетесь? Какую информацию ищете? (Советы экспертов, расписания, магазины?)
– Любимые ресурсы?
  Чем они Вам нравятся?
  Что Вы используете регулярно/иногда/ не используете совсем?
– Расскажите о ярких спортивных мероприятиях, в которых Вы участвуете/о которых слышали.
– Вы занимаетесть ..... (вид спорта). Обычно Ваши тренировки проходят .....(где, как часто). К чему Вы стремитесь в спорте и чего Вам не хватает для достижения этих целей? (времени, помощи профессионалов, силы воли).
– Как Вы, как профессионал/продвинутый любитель/яркий представитель фанатов, стали бы в первую очередь использовать этот сервис?
– С кем бы Вы посоветовали мне еще побеседовать? Среди Ваших знакомых есть такие люди?

На основе полученных данных были расставлены приоритеты в разработке виджетов и реализации конкретных возможностей. По результатам интервью с 30 представителями целевой аудитории был составлен и проранжирован по степени востребованности среди опрошенных пользователей список виджетов. По горизонтали виджеты отсортированы в соответствии с пожеланиями пользователей (розовым цветом выделены самые востребованные (упомянутые более, чем половиной респондентов), зеленым – менее популярные (5–15 опрошенных), голубым – идеи отдельных пользователей).

По вертикали виджеты отсортированы на основе статистики популярности отдельных видов спорта в процентах, согласно данным Ассоциации содействия международному движению «Спорт для всех» (TAFISA). Соответственно, чем больше суммарное значение в процентах, и чем правее виджет располагается в на графике – тем выше приоритет его разработки.

На рис. 2 схематически изображены результаты исследования предпочтений пользователей с учетом статистики популярности видов спорта.

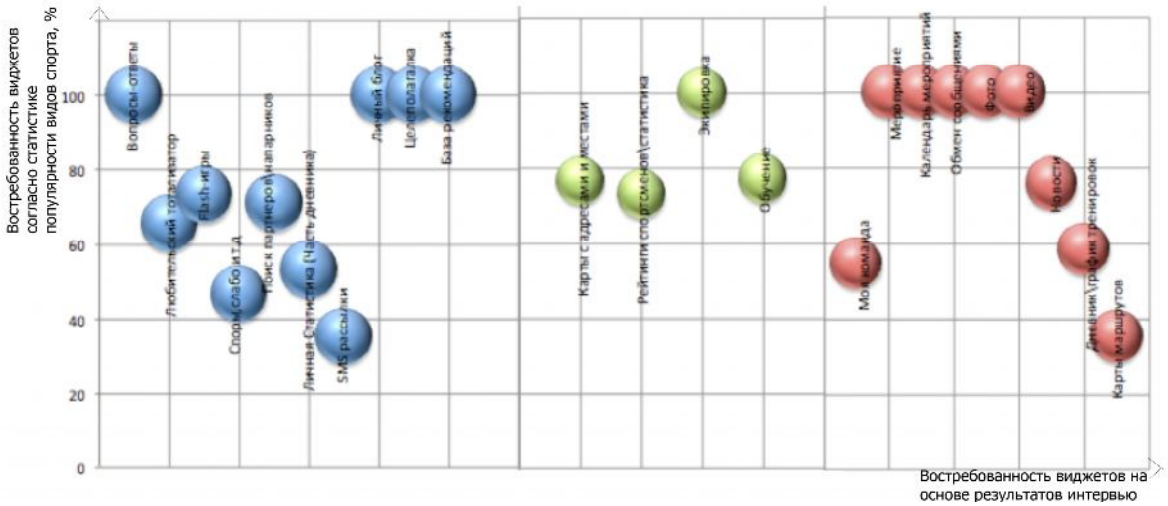


Рис. 2. График потенциальной востребованности виджетов

На основе проведенного анализа, для проектирования были выбраны следующие виджеты: Фото, Мероприятие, Поиск партнера, Календарь мероприятий, Экипировка, Новости, Карты, Микроблог.

На этапе проверки гипотезы о предлагаемом продукте разработанные прототипы были предложены для оценки группе потенциальных пользователей из 10 человек. Помимо общей оценки адекватности интерфейсов потребностям пользователей, выяснялись также наиболее комфортные варианты реализации отдельных элементов. Результаты исследования приведены ниже.

1. **Полноэкранное отображение виджета.** Варианты реализации:

   а) Виджет в раскрытом виде занимает правую половину экрана, закрывая всю область виджетов. Левая половина экрана, в которой располагается система сообщений («Пульс»), остается доступной для просмотра и взаимодействия.

   б) Виджет занимает всю левую половину экрана, закрывая систему сообщений. Остальные виджеты остаются справа.

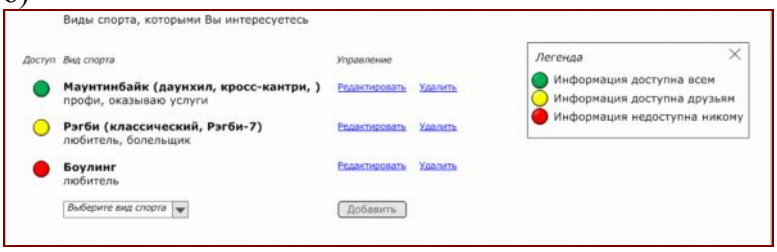
   в) Виджет открывается в отдельном окне поверх основного интерфейса. При этом основной интерфейс затеняется. В этом случае сохраняется возможность взаимодействия как с системой сообщений, так и с другими виджетами. При клике на затененную область, основной интерфейс становится активным.

   Результат: 6 респондентов из 10 выбрало вариант в)

   Обоснование выбора: Этот вариант – единственный из предложенных, который позволяет сохранять контакт с другими элементами интерфейса (Пульсом и остальными виджетами). В перспективе планируется реализовать возможность drag’n’drop элементов виджетов (например, фотографий и видеороликов). Раскрытие виджета в виде pop-up окна интуитивно понятно и привычно, однако может вызывать ассоциации с самопроизвольно открывающимися рекламными сообщениями. Этот риск может быть минимизирован с помощью правильно подобранного динамического эффекта открывания виджета.

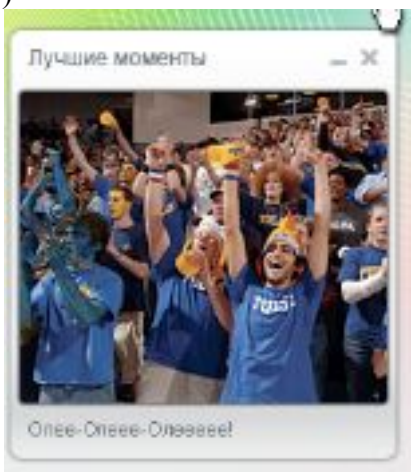
2. **Иконки переключения режимов просмотра.** Варианты реализации:
   а) 2 иконки (иконка активного режима отсутствует); б) 3 иконки (иконка текущего режима не активна)
   Результат: 7 респондентов из 10 признало вариант а) более удобным.
   Обоснование выбора: в интерфейсах большинства программных продуктов регулирование размеров окна реализовано двумя иконками.
3. **Настройки прав доступа.** Варианты реализации:

   а)
   б)



   Результат: 10 респондентов из 10 признало вариант б) более удобным.
   Обоснование выбора: Вариант реализации настроек прав доступа в виде «лампочек» более наглядный и эстетичный. При этом ассоциации со светофором позволяют однозначно трактовать значения каждого из 3-х состояний.
4. **Цвет оформления виджета.** Варианты реализации

   а) б)



   Результат: мнения разделились
   Обоснование выбора: Был выбран темный вариант, исходя из того, что светлый может сливаться с цветом фона внутри виджета. В этом случае контент пришлось бы отделять контрастной рамкой.

По итогам проведенного исследования был создан интерфейс, отвечающий как современным стандартам реализации виджетов, так и потребностям специфичной группы потенциальных пользователей.

Заключение

В статье рассмотрен процесс проектирования и реализации веб-виджетов с применением модели исследования предпочтений пользователей на разных этапах. В ходе

анализа существующих наработок, а также на основе результатов исследования предпочтений пользователей, был создан универсальный и, в то же время, максимально простой и интуитивно понятный интерфейс, подходящий для веб-виджетов любой сложности и назначения.

Литература

1. Зинченко В.П. Основы эргономики. – М.: МГУ, 1979. – 179 с.
2. Морвиль П., Розенфельд Л. Информационная архитектура в Интернете. – М.: Символ-Плюс. – 2005.
3. Нильсен Я. Веб-дизайн. Книга Якоба Нильсена. – М.: Символ-Плюс, 2006.
4. Раскин Д. Интерфейс: новые направления в проектировании компьютерных систем. – М.: Символ-Плюс. – 2005.
5. Савельев А. Технология, которая перевернёт веб //Компьютерра. – 2005. – № 6. – С. 10–13.
6. Blank S. The Four Steps for the Epiphany.: Cafepress.com, 2006. – 282 с.
7. Raskin J. Intuitive Equals Familiar //Communications of the ACM. 37:9. – 1994. – С. 17.
8. Новости Treli [Электронный ресурс] /Статистика популярности видов спорта в мире. – Режим доступа: http://treli.ru/newstext.mhtml?Part=9&PubID=10912, свободный. – Загл. с экрана. – Яз. рус.
9. Emarketer [Электронный ресурс] /Web widgets and applications. – Режим доступа: http://www.emarketer.com/Report.aspx?code=2000368, свободный. – Загл. с экрана. – Яз. рус.
10. World Wide Web Consortium [Электронный ресурс] /Widget talks. – Режим доступа: http://www.w3.org/2008/Talks/WWW2008-widgets.pdf, свободный. – Загл. с экрана. – Яз. англ.

УДК 004.451.42

ИСПОЛЬЗОВАНИЕ КОНЕЧНЫХ АВТОМАТОВ ПРИ ПОСТРОЕНИИ ЯДРА МИКРООПЕРАЦИОННОЙ СИСТЕМЫ РЕАЛЬНОГО ВРЕМЕНИ

Л.Е. Стрюк, В.О. Клебан
Научный руководитель – д.т.н., профессор А.А. Шалыто

В статье ставится задача статического и динамического синтеза процедуры диспетчеризации для операционной системы реального времени. Работа основывается на парадигме автоматного программирования.

Ключевые слова: автоматное программирование, ОСРВ, микрооперационная система

Введение

В последнее время большую распространенность получили так называемые встраиваемые системы. Среди них существует отдельный класс систем: системы реального времени (ОСРВ). Это такие системы, которые реагируют в предсказуемое время на непредсказуемое появление внешних событий, иными словами они действуют в темпе задаваемой средой, в которой они работают [1].

Поддерживать такое свойство довольно сложно, а если пытаться реализовать ОСРВ для каждой задачи заново, то многократно возрастает цена и падает надежность таких систем (реализовать программу без ошибок крайне сложно). Пусть для реализации задачи дана микроЭВМ с ограниченными ресурсами и, тем не менее, от управляющей системы требуется обладать свойствами ОСРВ. Ввиду серьезных ограничений на вычислительную мощность микроЭВМ, широко использующихся во встраиваемых системах, применение полноценной ОСРВ становиться невозможным. В этом случае прибегают к помощи микрооперационных систем, но, как будет показано далее, данная причина не является единственной.

Микрооперационная система реального времени

Микрооперационная система реального времени отличается (uОСРВ) отличается от обычной ОСРВ, в первую очередь тем, что она предназначена для решения заранее известного круга задач [2]. Данное свойство uОСРВ является чрезвычайно важным, по причине того, что оно позволяет осуществить синтез оптимальной процедуры диспетчеризации для данного конкретного набора задач.

Постановка задачи

Начнем с определений.

Процесс – последовательная смена состояний объекта во времени [3]. В рамках описываемой системы, и в соответствии с парадигмой автоматного программировании [4], процесс в uОСРВ представляет собой конечный автомат (систему автоматов), которому периодически передается управление.

Диспетчер – процесс, функцией которого является обеспечение необходимой временной диаграммы работы остальных процессов в системе. В рамках uОСРВ диспетчер является «корнем» дерева иерархии автоматов.

Авторами ставится следующая задача. По заданному набору процессов и временной диаграмме, необходимо статически или динамически синтезировать процедуру диспетчеризации (автомат диспетчера). Расширив формулировку, можно сказать, что

ставится задача создать инструментальное программное средство (ИПС) которое служило бы для автоматической генерации элементов ОСРВ.

Для решения предлагается построить специальный язык формального описания временной диаграммы работы uОСРВ. Также предполагается, что описание процессов [5] будет осуществляться на специальном языке автоматного программирования.

Диспетчеризация

Процедура диспетчеризации такой же процесс, как и остальные для целевой ЭВМ, то есть автомат. Диспетчер занимается передачей управления от одного автомата к другому в зависимости от различных факторов: наступлению определенного момента времени, получения события или сигнала и т.д. При получении управления автомат делает ровно один переход, в котором либо меняет свое состояние, либо нет (переход по петле). Считается, что во время активности одного автомата не может быть активен ни один другой автомат, за исключением системных (управление устройствами ввода вывода и другие) и специального случая, который описывается ключевым словом `wait`.

Формальный язык описания ОС

Язык, предлагаемый авторами, является расширением языка С. Это сделано по причине того, что С является наиболее наглядным, оптимальным и распространенным языком для работы с микроконтроллерами, которые представляют собой вероятную целевую ЭВМ.

В функции операционной системы входят диспетчеризация процессов, создание событий (периодических и системных), предоставление интерфейса для работы с некоторыми компонентами целевой ЭВМ.

Операционная система имеет поддержку событий. Описание события состоит из двух частей: декларации и конфигурации. Все события описываются просто перечислением имен. Конфигурация события – это набор условий при котором данное событие возникает. Возникновение события можно сделать регулярным (например, раз в десять миллисекунд) или разовым. Регулярные события описываются только во временной диаграмме ОС, так как они связаны непосредственно с системным таймером. Непосредственные операции с событиями доступны всем процессам ОС. Первичными операциями с событиями являются следующие: включение, отключение, перехват, генерация. Для включения и отключения регулярного события системой предоставляется специальные функции.

Временная диаграмма ОС также описывает вызов автоматов-процессов. При описании временной диаграммы ОС используются специальные конструкции. Например конструкцией *every(objectName, time)* описываются вызовы. В данном случае *objectName* – может быть как именем автомата, так и именем события *time* – период вызова. События и автоматы с одинаковыми именами не допускаются.

Операционная система также имеет системозависимую часть в которой реализуется использование ресурсов ЭВМ. В данной части необходимо реализовать такие операции, как работа с устройствами ввода вывода, таймерами и т.д. В данной части также необходимо указать функцию, которая вызывается по прерыванию системного таймера. В ее тело помещается часть автомата диспетчеризации. Каждый раз при вызове прерывания по таймеру диспетчер пересчитывает, сколько осталось времени до вызова различных автоматов и событий и в зависимости от результата пересчета передает управление тому или иному автомату.

Для описания автоматов предлагается использовать расширяющий С язык текстового автоматного программирования. Рамки данной статьи не позволяют описать его

полностью, поэтому здесь будут изложены основные моменты. Каждый автомат представляет из себя блок кода:

```
automata A1 {
 …
}
```

Внутри, в аналогичных блоках описываются его состояния, переходы, выходные воздействия и прочие атрибуты автомата. Помимо стандартных атрибутов в качестве «синтаксического сахара» вводится атрибут инициализации: отдельный блок кода `init{..}`, который вызывается диспетчером на старте. С целью упрощения грамматики в языке есть специальный блок `code{..}`, внутри которого может располагаться корректный код на языке *C*. Смысл этого упрощения в том, что парсеру кода будет достаточно бегло проверить на корректность код внутри этого блока (например, с точки зрения правильной последовательности открывающихся и закрывающихся скобок) и просто добавить его содержимое в результат без каких-либо изменений. Автоматы требующие отдельной инициализации перечисляются при описании системы.

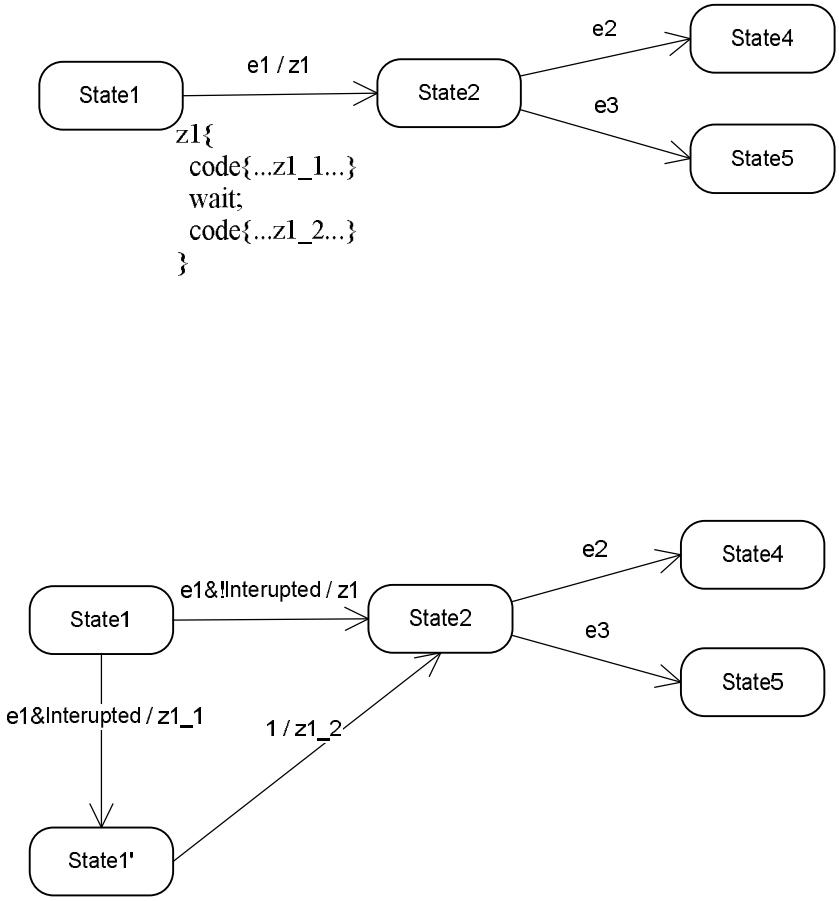


Рис. 1. Иллюстрация работы ключевого слова wait

Некоторые действия автоматов могут занимать значительное процессорное время и при этом не требовать «атомарного» выполнения. Для этих целей в язык добавлено ключевое слово `wait`. Оно помещается между блоками `code` для того чтобы указать на то, что работа автомата может быть прервана и управление может быть отдано другому автомату. Работа данной инструкции заключается в следующем: исходный автомат модифицируется так, что исходное состояние, содержащее инструкцию ожидания, разбивается на два (рис. 1). Это позволяет диспетчеру прервать исполнение данного

процесса и проверить есть ли в системе автоматы, выполнение которых нужно произвести срочно (на схеме отображено проверкой флага *interupted*). Если такие автоматы существуют, то управление передается им.

Заключение

Даная разработка в качестве целевой микроЭВМ использует микроконтроллеры семейства ARM7, но ввиду того, что никакие специализированные функции ЭВМ кроме таймера, который сейчас есть почти везде, для нее не критичны, с небольшими изменениями она сможет работать на любой архитектуре, поддерживающей язык С и необходимую периферию.

Важным свойством предлагаемого подхода является то, что построенная система обладает свойством наблюдаемости. Иными словами возможна верификация прикладных программ в совокупности с процедурой их диспетчеризации.

Литература

1. Шалыто А.А. Алгоритмизация и программирование для систем логического управления и «реактивных» систем //Автоматика и телемеханика. – 2001. – № 1. – С. 3−39.
2. Астапкович А.М. Микрооперационные системы реального времени. СПб: Политехника. – 2002.
3. Романовский И.В. Дискретный анализ. СПб: Невский Диалект.
4. Шалыто А.А. Switch-технология. Алгоритмизация и программирование задач логического управления. СПб: Наука, 1998. http://is.ifmo.ru/books/switch/1
5. Гуров В.С., Мазин М.А., Шалыто А.А. Текстовый язык автоматного программирования //Научно-технический вестник СПбГУ ИТМО. – №42.

.

УДК 004.4’242

ПРИМЕНЕНИЕ МЕТОДА ПРЕДСТАВЛЕНИЯ ФУНКЦИИ ПЕРЕХОДОВ С ПОМОЩЬЮ АБСТРАКТНЫХ КОНЕЧНЫХ АВТОМАТОВ В ГЕНЕТИЧЕСКОМ ПРОГРАММИРОВАНИИ

Ф.Н. Царев
Научный руководитель – д.т.н., профессор А.А. Шалыто

В статье описывается метод представления функции переходов с помощью абстрактных конечных автоматов. Этот метод применяется для построения управляющих конечных автоматов с помощью генетического программирования. Применение этого метода иллюстрируется на примере задачи «Умный муравей-3».
Ключевые слова: конечный автомат, генетическое программирование, функция переходов

Введение

В последнее время все шире применяется автоматное программирование, в рамках которого поведение программ описывается с помощью конечных детерминированных автоматов [1]. Для многих задач автоматы удается строить эвристически, однако существуют задачи, для которых такое построение затруднительно. К задачам этого класса относятся, например, задача «Умный муравей» [2–4], задача «Умный муравей-3» [5] и задача об управлении моделью беспилотного летательного аппарата [6]. Для построения автоматов в таких задачах можно применять генетические алгоритмы [7–9].

В ряде задач (например, в последних двух из указанных) требуется строить управляющие автоматы с достаточно сложными логическими условиями на переходах. Для представления таких автоматов существует несколько методов, например, метод сокращенных таблиц переходов [10], метод представления автоматов деревьями решений [11]. В настоящей работе предлагается новый метод представления управляющих конечных автоматов – представление функции переходов с помощью абстрактных конечных автоматов. Применение этого метода иллюстрируется на примере задачи «Умный муравей-3».

Постановка задачи

Приведем описание классической постановки задачи «Умный муравей» [2–4]. Используется двумерный тор размером 32 на 32 клетки (рис. 1). На некоторых клетках поля расположены яблоки – черные клетки на рис. 1. Яблоки расположены вдоль некоторой ломаной линии, но не на всех ее клетках. Клетки ломаной, на которых яблок нет – серые. Белые клетки – не принадлежат ломаной и не содержат яблок. Всего на поле 89 яблок.

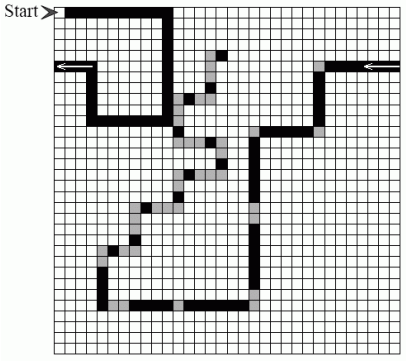


Рис. 1. Поле с яблоками

В клетке с пометкой «Start» находится муравей. Он занимает клетку поля и смотрит в одном из четырех направлений (север, запад, юг, восток). В начале игры муравей смотрит на восток. Он умеет определять находится ли яблоко непосредственно перед ним. За ход муравей совершает одно из четырех действий:

- идет вперед на одну клетку, съедая яблоко, если оно находится перед ним;
- поворачивается вправо;
- поворачивается влево;
- стоит на месте.

Съеденные муравьем яблоки не восполняются. Муравей жив на всем протяжении игры – еда не является необходимым ресурсом для его существования. Никаких других персонажей, кроме муравья, на поле нет. Ломаная *строго задана*. Муравей может ходить по любым клеткам поля. Игра длится не более 200 ходов, на каждом из которых муравей совершает одно из четырех описанных выше действий. В конце игры подсчитывается число яблок, съеденных муравьем. Это значение – результат игры.

Цель игры – создать муравья, который не более чем за 200 ходов съест как можно больше яблок. Муравьи, съевшие одинаковое количество яблок, заканчивают игру с одинаковым результатом вне зависимости от числа ходов, затраченных каждым из них на процесс еды. Однако эта задача может иметь различные модификации, например, такую, в которой при одинаковом количестве съеденных яблок, лучшим считается муравей, съевший яблоки за меньшее число ходов. Ниже будет показано, что поведение муравья может быть задано конечным автоматом. При этом может быть поставлена задача о построении автомата с минимальным числом состояний для муравья, съедающего все яблоки, или автомата для муравья, съедающего максимальное число яблок при заданном числе состояний.

Конечный автомат, изображенный на рис. 2, имеет всего пять состояний.

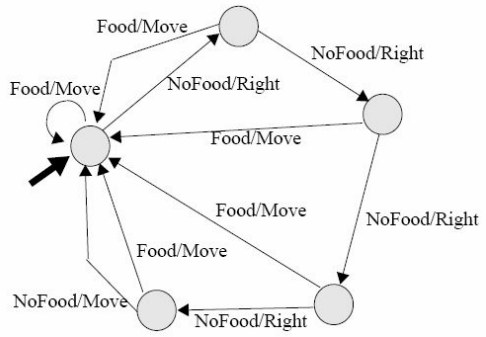


Рис. 2. Конечный автомат, задающий поведение муравья

Этот автомат описывает поведение муравья, который не решает задачу – за 200 ходов съедает только 81 яблоко, а за 314 ходов – все 89 яблок. Муравей действует по принципу «Вижу яблоко – иду вперед. Не вижу – поворачиваю. Сделал круг, но яблок нет – иду вперед».

Постановка задачи «Умный муравей-3», предложенной в работе [5], содержит несколько существенных отличий.

Во-первых, расширена область обзора муравья – вместо одной клетки он видит восемь. Таким образом, множество значений входных переменных содержит $2^8 = 256$ элементов. На рис. 3 изображена область обзора муравья (клетка, в которой находится муравей, обозначена серым цветом).

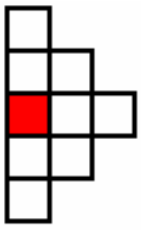


Рис. 3. Область видимости муравья

Во-вторых, расположение еды на поле не фиксировано, а генерируется случайным образом. При этом вероятность того, что яблоко окажется в некоторой клетке, одинакова для всех клеток поля и равна μ.

В этом случае число яблок, съеденных муравьем за 200 ходов, есть случайная величина ξ (определяемая муравьем) на дискретном множестве элементарных исходов Ω – множестве расположений еды – битовых матриц 32×32. Каждому исходу ω_i, содержащему k единиц поставим в соответствие вероятность $p(\omega_i) = \mu^k(1-\mu)^{n-k}$, где $n = 32\times32$.

Для вычисления этой величины в общем случае необходимо перебрать все возможные битовые матрицы размером 32×32. Поэтому для оценки эффективности автомата, задающего поведение муравья, вместо точного вычисления этого математического ожидания, оно будет вычислять приближенно – с помощью моделирования поведения муравья на 10000 случайно сгенерированных полях.

Решение задачи без применения конечных автоматов

Поведение муравья в задаче «Умный муравей-3» можно описывать следующим «жадным» алгоритмом – на каждом шаге муравей анализирует область видимости и находит клетку, содержащую еду и до которой можно добраться за минимальное число действий. Если такая клетка найдена, то муравей движется к ней по кратчайшему пути. Если же она не была найдена, то муравей делает шаг вперед в текущем направлении.

Отметим, что этот алгоритм можно реализовать и с помощью конечного автомата, однако он будет содержать достаточно большое число состояний.

Вычислительный эксперимент показывает, что такое поведение муравья достаточно эффективно – при μ=0.05 среднее число единиц еды, съеденных на 10000 случайно сгенерированных полях, равно 25.861.

Предлагаемый метод представления автоматов

В работе [11] предлагается представлять конечные автоматы с помощью деревьев решений. При применении этого подхода каждому состоянию автомата соответствует некоторое дерево решений, в листьях которого хранится информация о том, в какое состояние должен перейти автомат и какое выходное воздействие он должен выработать.

В настоящей работе предлагается вместо деревьев решений применять *абстрактные* конечные автоматы. Пусть *структурный* конечный автомат, который необходимо представить, имеет n входных логических переменных. Если их значения в некоторый момент расположить в некотором фиксированном порядке, то получится слово из нулей и единиц длины n.

Если подать это слово на вход некоторому абстрактному конечному автомату, состояния которого помечены выходными воздействиями и номерами состояний структурного конечного автомата, то рассматриваемый абстрактный автомат перейдет в некоторое состояние. Это состояние будет аналогом листа дерева решений – из него бу-

дет считана информация о том, в какое состояние должен перейти структурный автомат и какое выходное воздействие он должен выработать.

Преимуществом абстрактных автоматов является то, что для представления одной и той же функции переходов, им требуется меньшее число состояний, чем деревьям решений. Поясним это на примере. Пусть из некоторого состояния 0 структурного автомата есть три перехода (рис. 4).

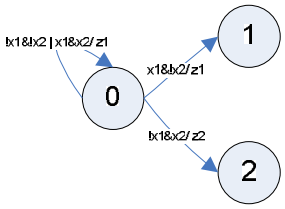


Рис. 4. Переходы из состояния 0 структурного автомата

Пометки на переходах на рис. 4 имеют следующий формат: `условие/ выходное воздействие`. Отметим, что указанная система условий на переходах из состояния 0 является полной и непротиворечивой.

Если использовать представление автоматов с помощью деревьев решений, то в дерево для рассматриваемого состояния будет содержать пять вершин (рис. 5).

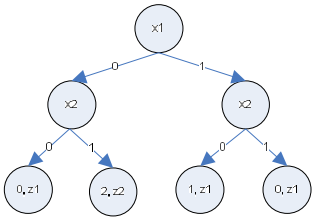


Рис. 5. Дерево решений, задающее переходы из состояния 0

Эту же систему переходов можно задать абстрактным конечным автоматом, который будет содержать всего три состояния. Его граф переходов изображен на рис. 6 (ему на вход вначале подается значение переменной x1, после чего – значение переменной x2).

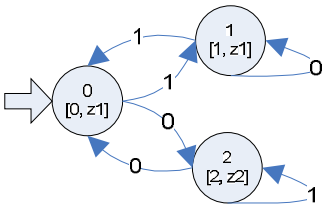


Рис. 6. Абстрактный конечный автомат, задающий структурного автомата переходы из состояния 0

На рис. 6 начальное состояние указано большой стрелкой, а пометки состояний имеют следующий формат: номер состояния [номер состояния, в которое должен перейти структурный автомат, выходное воздействие, которое он должен выработать].

Описание генетического алгоритма

Для построения управляющих автоматов применяется генетический алгоритм, аналогичный алгоритму, который использовался в работе [4]. Управляющий структур-

ный автомат в алгоритме представляется в виде совокупности описаний состояний и номера начального состояния. Описание каждого из состояний состоит из описания абстрактного конечного автомата. Описание абстрактного конечного автомата состоит из номера начального состояния, набора пометок состояний (номер состояния, в которое должен перейти структурный автомат, и набор выходных воздействий, которые он должен выработать) и описания функции переходов этого автомата в виде таблицы переходов.

Все структурные автоматы, рассматриваемые в процессе работы генетического алгоритма, содержат одинаковое число состояний, заданное до начала работы алгоритма. Начальное поколение формируется путем генерации автоматов случайным образом – для каждого из них случайно выбирается начальное состояние и случайным образом генерируются абстрактные автоматы, соответствующие состояниям. Их генерация производится методом, аналогичным описанному в работе [4].

Для скрещивания описаний структурных автоматов используется однородный кроссовер [7]. Для скрещивания описаний абстрактных автоматов, описывающих переходы из состояний структурного автомата, используется метод, аналогичный описанному в [4]. При мутации структурного автомата равновероятно выбирается один из двух вариантов – либо изменяется начальное состояние, либо производится мутация одного из абстрактных автоматов, описывающих переходы из состояний. При этой мутации равновероятно выбирается один из вариантов – изменение начального состояния, изменение пометки одного из состояний, изменение состояния, в которое ведет один из переходов.

Результаты вычислительного эксперимента

На рис. 7 приведен график зависимости максимального значения функции приспособленности для автоматов из пяти состояний (при этом абстрактные автоматы, задающие переходы также содержат по пять состояний).

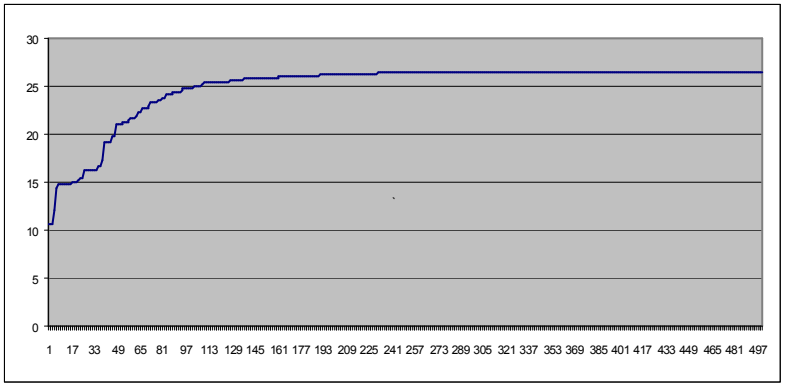


Рис. 7. График зависимости максимального значения функции приспособленности от номера поколения

Функция приспособленности в этом вычислительном эксперименте вычисляется как среднее число единиц еды, съеденное муравьем на 200 полях, сгенерированных случайным образом. К пятисотому поколению был построен автомат, значение функции приспособленности которого равно 26.54. Моделирование работы этого автомата на 10000 случайно сгенерированных полях (при μ=0.05) показывает, что среднее число единиц еды, съеденных муравьем, равно 26.418. Таким образом, построенный автомат задает более эффективное поведение муравья, чем описанный выше «жадный» алгоритм.

Выводы

В настоящей работе предложен метод представления функции переходов структурного конечного автомата с помощью абстрактного конечного автомата. Применение этого метода в генетическом программировании проиллюстрировано на задаче «Умный муравей-3». Преимущество этого метода заключается в том, что он позволяет более компактно по сравнению с деревьями решений представлять функцию переходов. Кроме этого он позволяет осуществлять построение управляющих автоматов с произвольным числом переходов из каждого состояния только на основе генетических операций для автоматов с двумя переходами из каждого состояния.

Литература

1. Шалыто А.А. Технология автоматного программирования / Труды первой Всероссийской научной конференции "Методы и средства обработки информации" М.: МГУ. 2003. http://is.ifmo.ru/works/tech_aut_prog/
2. Angeline P., Pollack J. Evolutionary Module Acquisition / Proceedings of the Second Annual Conference on Evolutionary Programming. Cambridge: MIT Press. 1993, pp.154–163. http://www.demo.cs.brandeis.edu/papers/ep93.pdf
3. Jefferson D., Collins R., Cooper C., Dyer M., Flowers M., Korf R., Taylor C., Wang A. The Genesys System: Evolution as a Theme in Artificial Life /Proceedings of Second Conference on Artificial Life. MA: Addison-Wesley. 1992, pp.549–578. www.cs.ucla.edu/~dyer/Papers/AlifeTracker/Alife91Jefferson.html
4. Царев Ф.Н., Шалыто А.А. Применение генетического программирования для генерации автомата в задаче об «Умном муравье» / Сборник трудов IV-ой Международной научно-практической конференции «Интегрированные модели и мягкие вычисления в искусственном интеллекте». Том 2. М.: Физматлит. 2007, с. 590–597. http://is.ifmo.ru/genalg/_ant_ga.pdf
5. Бедный Ю.Д., Шалыто А.А. Применение генетических алгоритмов для построения автоматов в задаче «Умный муравей». http://is.ifmo.ru/works/ant
6. Параценко Д.А., Царев Ф.Н., Шалыто А.А. Технология моделирования одного класса мультиагентных систем на основе автоматного программирования на примере игры «Соревнование летающих тарелок». Проектная документация. СПбГУ ИТМО. 2006. http://is.ifmo.ru/unimod-projects/plates/
7. Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы. М.: Физматлит, 2006.
8. Рассел С., Норвиг П. Искусственный интеллект: современный подход. М.: Вильямс, 2006.
9. Koza J. R. Genetic programming: on the programming of computers by means of natural selection. MIT Press, 1992.
10. Поликарпова Н.И., Точилин В.Н., Шалыто А.А. Применение генетического программирования для генерации автоматов с большим числом входных переменных //Научно-технический вестник СПбГУ ИТМО. Выпуск 53. Автоматное программирование, с. 24–42.
11. Данилов В.Р. Метод представления автоматов деревьями решений для использования в генетическом программировании //Научно-технический вестник СПбГУ ИТМО. Выпуск 53. Автоматное программирование, с. 103–108.

УДК 004.4'242

МЕТОД ПОСТРОЕНИЯ ДЕТЕРМИНИРОВАННЫХ АВТОМАТОВ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ВЕРОЯТНОСТНЫХ АВТОМАТОВ

С.О. Попов

Научный руководитель – д.т.н., профессор А.А. Шалыто

Работа проводится с целью исследовать возможность, особенности, достоинства и недостатки использования вероятностных автоматов для построения детерминированных автоматов с помощью генетического программирования.

Эта статья предлагает один из методов решения проблемы ускорения поиска лучших решений, при использовании генетического программирования и автоматов в качестве особей.

Ключевые слова: генетический алгоритм, генетическое программирование, вероятностный автомат, детерминированный автомат, скрещивание, кроссовер, мутация

Введение

Генетический алгоритм находит локальные решения. Обычно большинство локальных решений не соответствует решению задачи. Поэтому нужно предотвращать преждевременную сходимость к локальному решению. При использовании детерминированных автоматов для предотвращения сходимости и ускорения работы можно использовать островную модель, большую мутацию и другие методы [1]. Эти методы основаны на манипуляциях с особями. В этой статье рассматривается ещё один метод, который пытается решить проблему изнутри особей. Его можно совмещать и с другими методами, при этом особой редакции программы не потребуется.

Детерминированный автомат и вероятностный автомат

Схематично детерминированная особь представляет собой детерминированный автомат. Этот автомат точно знает для каждого состояния и набора предикатов действия, которые ему надо совершить, и свое следующее состояние.

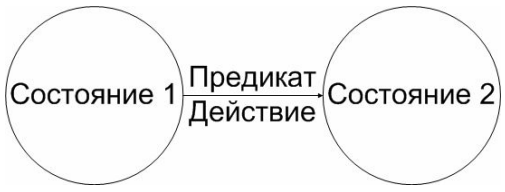


Рис. 1. Детерминированный автомат

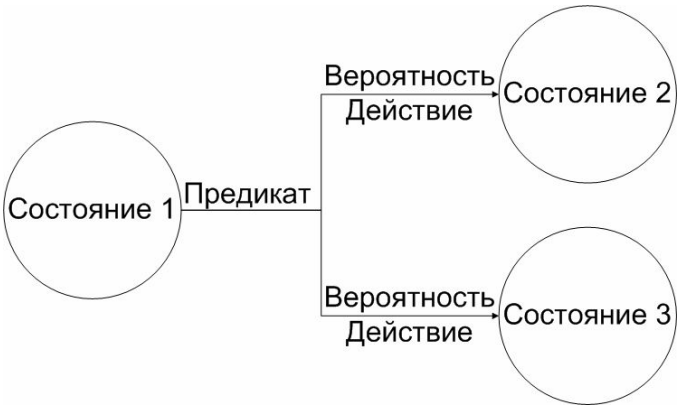


Рис. 2. Вероятностный автомат

В отличие от детерминированного автомата, вероятностный автомат заранее не знает, что он будет делать в данном состоянии с данным набором предикатов. Для каждого состояния и набора предикатов у автомата есть набор троек. Каждая тройка состоит из вероятности её выбора, набора действий и номера следующего состояния.

Переход от вероятностных автоматов к детерминированным автоматам происходит через удаление лишних троек. При удалении тройки автомат лишается выбора, когда тройка осталась одна, то только её и будет выбирать автомат. Таким образом, можно считать, что вероятностный автомат становится детерминированным, когда у него нет лишних троек для выбора.

Область решений

Если посмотреть на область решений, то детерминированная особь займет там лишь одну точку, а вероятностная особь после работы займёт целое множество точек.

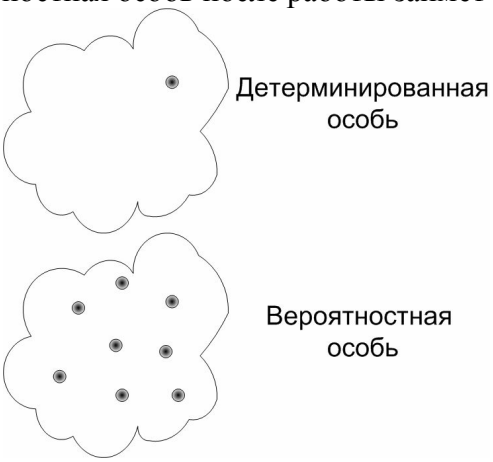


Рис. 3. Область решений

Это свойство вероятностной особи можно сравнить с алгоритмом имитации отжига [2]. В отличие от алгоритма имитации отжига, не следует стараться сделать особей детерминированными со временем.

Детерминизация особи

Предлагаемый метод в основном выращивает вероятностные особи, но в результате нужно получить правильную детерминированную особь.

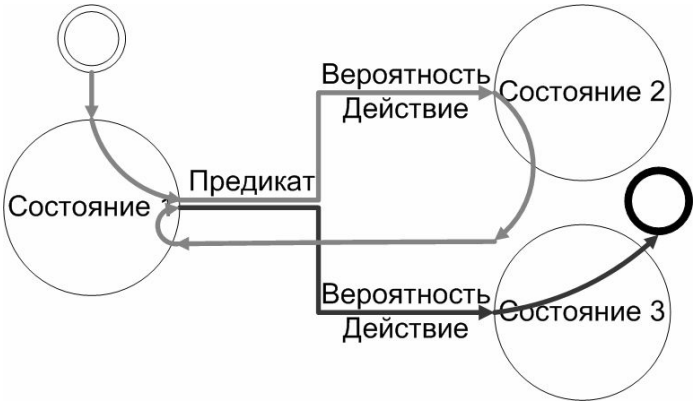


Рис. 4. Проблема выбора тройки

Если подробней рассмотреть происходящие в вероятностном автомате действия, то можно понять, что нужно несколько ограничить свободу выбора троек. Предполо-

жим, что повторилась ситуация, когда автомат повторно попал в какое-то состояние с тем же набором предикатов и выбрал другую тройку, что привело к лучшему решению, чем раньше.

Несмотря на получение лучшего решения, это решение не всегда будет показывать столь же хорошие результаты. И этот вероятностный автомат не поддается детерминизации, что приводит генетический алгоритм в локальное решение, которое не имеет смысла исследовать. Чтобы избежать подобных ситуаций, нужно запоминать выбранную тройку и в следующий раз выбирать снова ее же.

Таким образом, после тестирования особи, при хорошем результате, можно просто попросить автомат выкинуть тройки, которые небыли выбраны. Так особь сразу станет полностью детерминированной.

Генетический алгоритм

Использование вероятностных автоматов не приводит к фундаментальным изменениям. Естественно нужно модифицировать операторы мутаций, скрещивания и отбора. Но фитнесс функция и объект управления остаются не тронутыми. Вероятностный автомат полностью заменяет детерминированный автомат, без изменения кода использующего детерминированный автомат.

Оператор мутации произвольно выбирает несколько состояний, в каждом состоянии несколько наборов предикатов. В выбранных состояниях просто меняются все тройки на новые произвольные тройки.

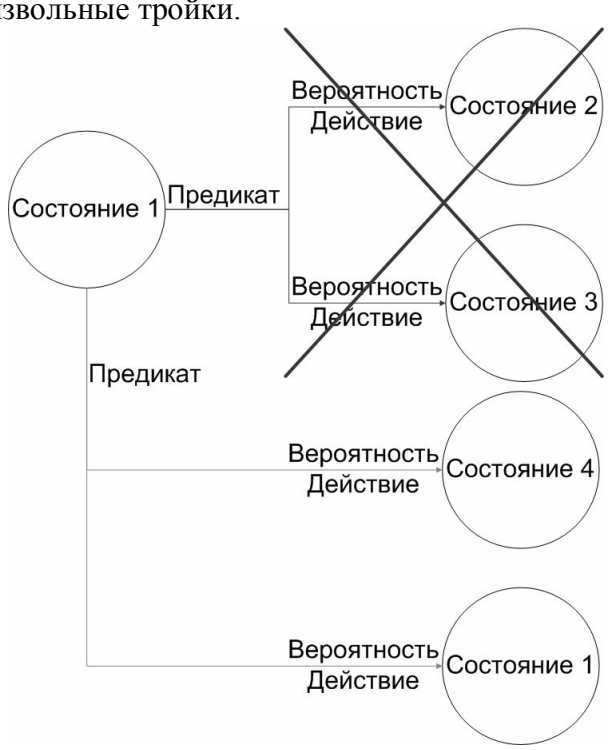


Рис. 5. Замена троек

Оператор скрещивания для каждого состояния и набора предикатов у двух вероятностных автоматов удаляет привязки троек к автоматам и создает произвольно новые привязки. При этом нужно скорректировать вероятности. У каждого автомата должна остаться хотя бы одна тройка.

Рис. 5. Перестановка троек

Испытания

Испытания проводились на задаче об умном муравье с использованием фреймворка для генетического программирования [3]. Использовалось поле 32×32 клетки с 89 яблоками, и у муравья было 200 шагов. Задача считалась решенной, кода хотя бы одна особь съедала все яблоки.

В процессе тестирования была использована одна и та же фитнесс функция. Если использовать в фитнесс функции данные о количестве лишних троек можно, либо задавить тройки, так что почти все особи станут детерминированными, либо генетический алгоритм будет искать лучший локальный минимум путем увеличения лишних троек.

Размер популяции для вероятностных автоматов был равен 1000 особей. Размер популяции для детерминированных автоматов был равен 5000 особей.

Среднее время тестирования одной итерации для детерминированной популяции 6 секунд, при использовании сети из 3 компьютеров удалось сократить время тестирования до 4 секунд. Среднее время тестирования для вероятностной популяции 2,5 секунды, но при этом вероятностная популяция была меньше в 5 раз.

Использование сети для вероятностной популяции оказалось неприменимым. По сети возвращается только результат тестирования, а для преобразования из вероятностной особи в детерминированную особь требуется знать выбранные тройки на переходах, эта информация пропадает на удаленной машине. Помимо потери информации о тройках испытание показало увеличение времени тестирования при использовании сети. Видимо передача особи по сети занимает больше времени, чем тестирование ее локально. В итоге для вероятностных особей сеть не использовалась. Но при увеличении времени тестирования ничего не противоречит применению сети для ускорения работы.

Результаты показали, что вероятностной популяции потребовалось больше поколений для нахождения решения, однако число особей в поколении было в 5 раз меньше. По времени работы вероятностная популяция показала себя не значительно хуже по времени, чем детерминированная с использованием сети из 3 компьютеров.

Поведение максимальных значений фитнесс функций у детерминированной популяции и у вероятностной популяции было схожим. Однако вероятностная популяция показывала большее средние значения фитнесс функции.

На рис. 6 показан график значения фитнесс функции в зависимости от номера популяции при использовании детерминированных автоматов. Время до нахождения решения составило около 720 секунд при использовании сети.

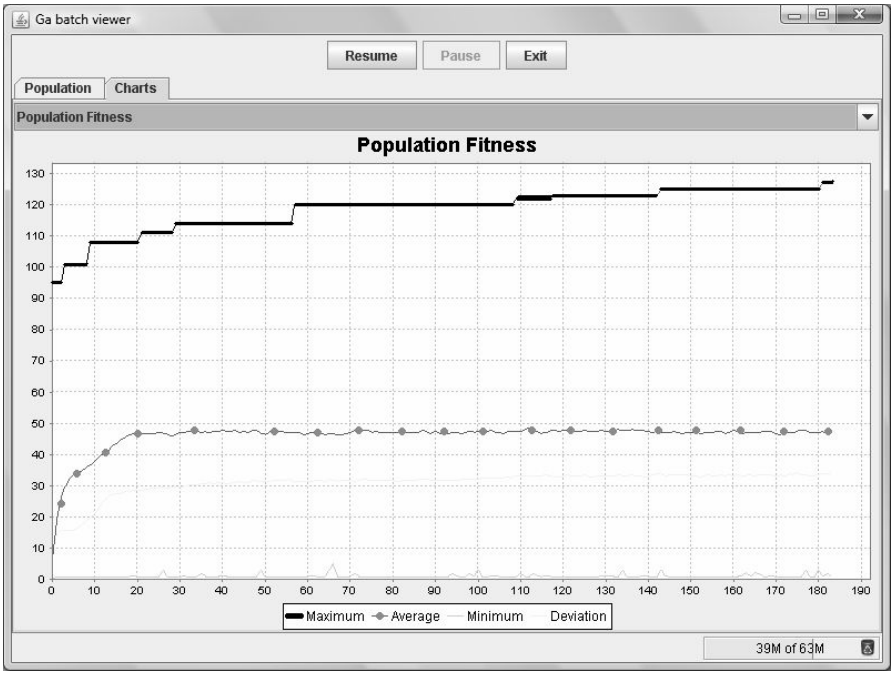


Рис. 6. Детерминированная популяция

На рис. 7 показан график значения фитнесс функции в зависимости от номера популяции при использовании вероятностных автоматов. Время до нахождения решения составило около 800 секунд без использования сети.

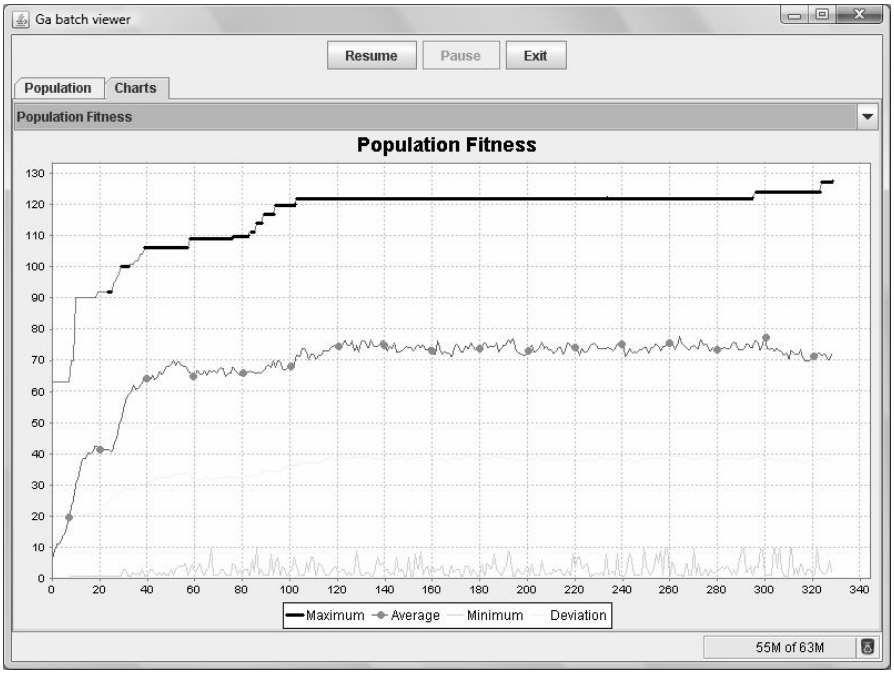


Рис. 7. Вероятностная популяция

Заключение

Разработан метод построения детерминированных конечных автоматов на основе генетического программирования с особями являющимися вероятностными автоматами.

Путем применения вероятностных автоматов удалось уменьшить число особей в популяции и ускорить обработку одного поколения особей. Вследствие чего можно было отказаться от использования сети.

При использовании вероятностных автоматов можно использовать фитнесс функцию от детерминированных автоматов. При этом ввод в фитнесс функцию учета вероятностей не целесообразен.

Литература

1. Применение островного генетического алгоритма для построения автоматов Мура и систем взаимодействующих автоматов Мили на примере задачи об «Умном муравье» [Электронный ресурс] / А.А. Давыдов, Д.О. Соколов, Ф.Н. Царев, А.А. Шалыто, Материал опубликован в сборнике докладов XI международной конференции по мягким вычислениям и измерениям (SCM'2008). СПб: СПбГЭТУ. 2008, с. 266–270 (Соколов). – Режим доступа: http://is.ifmo.ru/genalg/_scm2008_sokolov.pdf, свободный.
2. Генетические алгоритмы и другие сюжеты [Электронный ресурс] / Сергей Николенко, Machine Learning – CS Club, весна 2008. – Режим доступа: http://logic.pdmi.ras.ru/~sergey/teaching/mlcsclub/05-genetic.pdf, свободный.
3. Development of Software System for State Machine Generation Using Genetic Algorithms [Электронный ресурс] / Evgeny Andreevich Mandrikov, Vladimir Anatolievich Kulev, Proceedings of the Second Spring Young Researchers Colloquium on Software Engineering. SPb.: SPbSU. 2008. V. 1, pp. 59–60. – Режим доступа: http://is.ifmo.ru/genalg/_mandrikov-kulev_syrcose.pdf, свободный.
4. Генерация вероятностных автоматов методами Reinforcement Learning [Электронный ресурс] / Иринёв А.В. – Режим доступа: http://is.ifmo.ru/present/_irinev.ppt, свободный.
5. Применение генетического программирования для реализации систам со сложным поведением [Электронный ресурс] / Н.И. Поликарпова, В.Н. Точилин – Режим доступа: http://vestnik.ifmo.ru/ntv/39/ntv_39.3.3.pdf, свободный.
6. Генетическое программирование [Электронный ресурс] / Сергей Николенко, машинное обучение – ИТМО, осень 2006 – Режим доступа: http://logic.pdmi.ras.ru/~sergey/teaching/ml/05-genprog.pdf, свободный.

УДК 004.85

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ ДЛЯ ГЕНЕРАЦИИ ЧИСЛОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ, ОПИСЫВАЮЩИХ ДВИЖЕНИЕ, НА ПРИМЕРЕ ШАГА ВПЕРЕД ЧЕЛОВЕКОПОДОБНОГО РОБОТА

Ю.К. Чеботарева

Научный руководитель – д.т.н., профессор А.А. Шалыто

В статье предлагается подход, основанный на использовании генетических алгоритмов для автоматической генерации числовых последовательностей, описывающих движение, на примере шага вперед для человекоподобного робота. Предложенный подход позволяет абстрагироваться от физической модели робота, и с небольшими изменениями может быть применен для роботов различной конфигурации. Кроме того, в ходе генерации движения описанным методом нет необходимости в использовании дорогостоящих реальных роботов.

Ключевые слова: генетические алгоритмы, роботы, передвижение робота, поступательное движение, футбол роботов

Введение

Создание человекоподобных роботов одно из наиболее актуальных и перспективных направлений науки. Роботы такого типа могут выполнять различные задачи в мире, приспособленном для человека Международный проект *RoboCup* создан с целью привлечения внимания ученых и разработчиков к проблемам искусственного интеллекта, робототехники и смежных областей [1]. Для того чтобы стимулировать исследования в этих областях, ученым предлагается решать стандартную задачу, в которой можно применить широкий спектр технологий. В качестве такой задачи был выбран футбол. *RoboCup* ставит своей целью создание к 2050 году команды полностью автономных человекоподобных роботов, способной обыграть команду людей-чемпионов мира по футболу. Движение *RoboCup* спонсирует онлайн-соревнование по программированию роботов-футболистов *RobotStadium Contest* [2]. Участникам соревнования предлагается с помощью симулятора *Webots* написать управляющие программы для роботов *Nao* французской компании *Aldebaran Robotics*. Этот робот является официальным роботом лиги *Standard Platform* международных соревнований по футболу роботов [3, 4]. Готовые программы можно загружать на сайт, где периодически устраиваются соревнования между ними.

Очевидно, что создание конкурентоспособной управляющей программы затруднительно без набора базовых действий: шаг вперед, шаг назад, поворот влево-вправо, удар по мячу, встать из положения лежа на спине и из положения лежа на животе. В то же время задание этих действий весьма затруднительно. Каждое действие состоит из некоторого числа фаз (в примерах движений, поставляемых вместе с симулятором, от 10 до 100 и более), каждая из которых определяет значения углов сервомоторов робота. Подобрать требуемые значения вручную представляется абсолютно невыполнимой задачей. Методы, основанные на физике и биомеханике движений, требуют специфических знаний и сложны для реализации [5].

В данной работе автор предлагает использовать генетические алгоритмы для генерации движений роботов, При этом в качестве первой рассматривается задача выполнения роботом шага вперед [6–8].

1. Постановка задачи

Задача состоит в получении числовой последовательности, описывающей движение робота, такой, что ее использовании робот сохранит равновесие, переместится вперед и минимально отклонится в сторону. Модель *Nao*, используемая в *Webots*, оснащена 22 сервомоторами. Их расположение показано на рис. 1 (сервомоторы *RWristYaw*, *LWristYaw*, *RHand* и *LHand* в симуляторе не используются).

Для упрощения задачи будем считать, что только сервомоторы, управляющие ногами робота, участвуют в выполнении шага. К этой группе относятся следующие 12 сервомоторов: *RHipYawPitch*, *RHipPitch*, *RHipRoll*, *RKneePitch*, *RAnklePitch, RAnkleRoll*, *LHipYawPitch*, *LHipPitch*, *LHipRoll*, *LKneePitch*, *LAnklePitch*, *LAnkleRoll*.

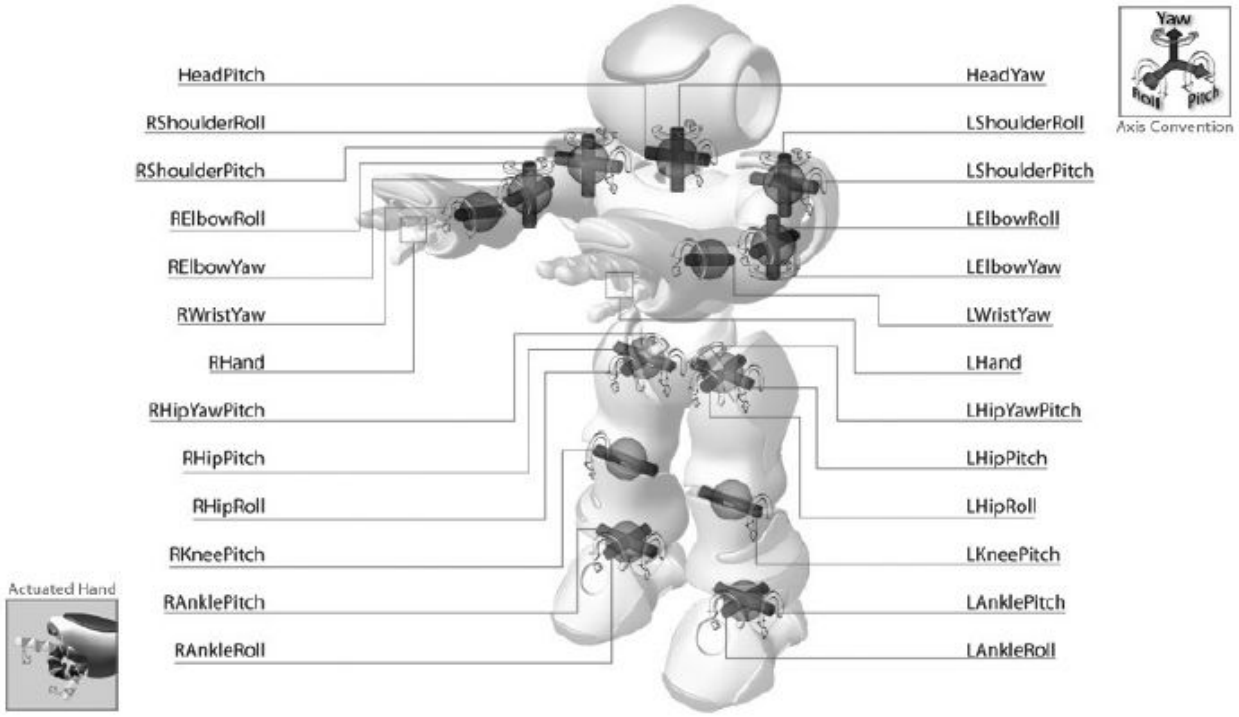


Рис. 1. Расположение сервомоторов робота

2. Описание алгоритма генетического программирования

Для работы генетического алгоритма необходимо задать алгоритм кодирования особей (движений робота) в хромосомы (числовые наборы), задать генетические операторы над хромосомами выбранного вида и задать алгоритм вычисления функции-приспособленности.

Задание особи

Сопоставим каждому из 12 выбранных сервомоторов числовой номер из промежутка $[0,..,12]$. Тогда значение угла каждого сервомотора представимо в виде функции от времени $\alpha_i = F_i(t)$, где $i \in [1,..,12]$, время t задано относительно времени начала движения. На рис. 2 показана зависимость угла α от времени для сервомотора *LHip-Pitch* (график построен по одному из примеров задания шага вперед, входящему в состав *Webots*).

Полное время шага обозначим τ (измеряется в мс), число фаз шага – m. Тогда разница по времени между соседними фазами будет составлять $\frac{\tau}{m}$ мс (в данной работе считаем все фазы равными по продолжительности).

Далее, предположим, что начальное и конечное положение робота заданы. Определим значения для углов сервомоторов во всех промежуточных фазах: $\frac{\tau}{m}, \frac{2\tau}{m}, .., \frac{(m-1)\tau}{m}$. Заметим, что значения функций $F_i(t)$ для $\left(\frac{j\tau}{m}, .., \frac{(j+1)\tau}{m}\right)$, $j \in [0, .., m-1]$ не используются для передачи роботу, и по сути могут быть любыми.

Рис. 2. Зависимость значения угла сервомотора LHipPitch от времени (мс)

Разобьем весь временной отрезок $[0, .., \tau]$ на n частей. На каждой из этих частей аппроксимируем функции F_i сплайнами третьей степени.

Для задания сплайна P_i на каждом отрезке $[t_1, .., t_2]$ достаточно задать значения $P_i(t_2)$ и $P_i'(t_2)$, кроме последнего отрезка, где достаточно только значения производной $P_i'(\tau)$ (значение $P_i(\tau)$ определено конечным положением робота), и первого отрезка, где дополнительно требуется задание $P_i(0)$.

Итак, имеем 12 сервомоторов, продолжительность шага τ мс, m фаз движения, n отрезков, на которых аппроксимируем функции F_i и $2n$ параметров для задания сплайнов. Будем считать τ, m и n параметрами генетического алгоритма наравне с числом особей в поколении N и числом поколений G. Тогда особь определяется $2n$ числами – значениями P_i и P_i' на границах отрезков (как описано выше).

Создание начального поколения

Начальное поколение заполняется N случайно сгенерированными особями, при создании которых учитываются ограничения на значения сервомоторов [9].

Скрещивание

Оператор скрещивания получает на вход две особи и выдает не более двух особей. Процесс скрещивания происходит следующим образом. Первый потомок имеет

все хромосомы первого родителя, за исключением одной, случайно выбранной, которая заменяется соответствующей хромосомой второго родителя.

У второго потомка все наоборот, одна их хромосом второго родителя заменяется соответствующей хромосомой первого родителя.

Оператор скрещивания возвращает только тех потомков, которые не совпадают ни с одним из родителей.

Следует заметить, что кроме описанного способа скрещивания, существует много других способов скрещивания. Это открывает широкий простор для экспериментов.

Мутация

При мутации у выбранной особи значение одной из хромосом заменяется новым случайным значением.

Вычисление функции приспособленности

Функция приспособленности линейно зависит от трех компонент: времени, прошедшего с начала движения до падения робота, смещения робота в сторону и перемещения вперед за один шаг.

Для того чтобы оценить два последних параметра, используется мяч, в начальный момент времени лежащий перед роботом так, что его изображение находится в середине изображения, получаемого с камеры робота. Смещение робота в сторону считается пропорциональным отклонению положения мяча от центра на изображении (чем оно меньше, тем меньше повернулся робот при выполнении шага, тем больше его приспособленность). Перемещение робота вперед пропорционально разности значений *ball.ratio2 – ball.ratio1,* где *ball.ratio1* – процент пикселей мяча в изображении с камеры до начала движения, *ball.ratio2* – процент пикселей мяча в изображении с камеры после выполнения движения. Если робот, сделав шаг, приблизился к мячу, то разность этих значений будет положительной (мяч на изображении с камеры будет выглядеть крупнее), а следовательно, и приспособленность должна вырасти.

Отбор особей для следующего поколения

После того, как для всех особей очередного поколения вычислена их приспособленность, необходимо заполнить новое поколение.

Для этого сначала выбирается k наиболее приспособленных особей из предыдущего поколения, которые переносятся в следующее поколение автоматически в неизменном виде (элитизм).

Далее, пока поколение не будет заполнено полностью, добавляем в него новые особи, полученные в результате скрещивания или мутации. Вероятность использования мутации равна p (параметр алгоритма), $0 \le p \le 1$, скрещивания, соответственно, $1 - p$. Для каждой новой особи выбор между мутацией и скрещиванием осуществляется индивидуально (при скрещивании за один раз могут быть добавлены две особи).

Критерий останова

Работа алгоритма прекращается после завершения работы с последним, G-ым, поколением.

3. Результаты

Промежуточные результаты показали, что предложенный метод является весьма перспективным. Для числа поколений $G = 10$ и числа особей в поколении $N = 100$ среди лучших особей встречались способные поднять и опустить ногу. При этом слегка сместившись, но сохранив равновесие, не теряя мяча из виду.

Правильный выбор параметров генетического алгоритма позволит ускорить рост средней приспособленности и сократить время вычислений.

Заключение

В качестве дальнейших направлений исследований автор считает наиболее перспективными изучение поведения генетического алгоритма в зависимости от значений параметров, выбор наиболее эффективной функции приспособленности, а также вопрос применимости описанного метода для генерации более сложных движений.

Литература

1. Официальный сайт проекта RoboCup [Электронный ресурс] / Федерация RoboCup, 2009. – Режим доступа: http://www.robocup.org, свободный. – Яз. англ.
2. Сайт онлайн-соревнования по программированию роботов-футболистов RobotStadium Contest [Электронный ресурс]. – Режим доступа: http://www.robotstadium.org/, свободный. – Яз. англ.
3. Michel, O. / Cyberbotics Ltd - WebotsTM: Professional Mobile Robot Simulation, pp. 39-42, International Journal of Advanced Robotic Systems, Volume 1 Number 1 (2004).
4. RoboCup Standard Platform League (Nao) Rule Book / RoboCup Technical Committee, 2009. – 25 с.
5. Changjiu Zhou, Lingyun Hu, Carlos A A Acosta, Pik Kong Yue Humanoid Soccer Gait Generation and Optimization Using Probability Distribution Models, 2006.
6. Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы. М.: Физматлит. – 2006.
7. Mitchell M. An Introduction to Genetic Algorithms. MIT Press. Cambridge. MA, 1996.
8. Wolff K., Nordin P. An Evolutionary Based Approach for Control Programming of Humanoids / Proceedings of the 3rd International Conference on Humanoid Robots (Humanoids'03). Karlsruhe: VDI/VDE-GMA. 2003.
9. Сайт Aldebaran Robotics [Электронный ресурс]. – Режим доступа: http://aldebaran-robotics.com/, свободный. – Яз. англ., франц.

УДК 004.832.28

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКОГО ПРОГРАММИРОВАНИЯ В ЗАДАЧЕ ПОИСКА УСЕРДНЫХ БОБРОВ

П.В. Федотов, Д.О. Соколов, Ф.Н. Царев
Научный руководитель – д.т.н., профессор А.А. Шалыто

В работе приведено описание задачи об усердных бобрах. Рассмотрена модификация островного генетического алгоритма с несколькими генетическими операторами, осуществляющий построение кандидатов на усердных бобров. Проведено сравнение результатов работы алгоритма с другими методами решения данной задачи.

Ключевые слова: усердный бобер, генетический алгоритм, машина Тьюринга, автомат

Введение

Поиск *усердных бобров* (*busy beaver game*) — известная задача в теории вычислимости [1]. Под *усердным бобром* (*busy beaver*) в теории вычислимости понимают машину Тьюринга [2] с заданным числом состояний конечного автомата, которая будучи запущенной на пустой ленте, записывает на нее максимально возможное число ненулевых символов и останавливается.

В настоящей работе рассмотрена одна из вариаций задачи о поиске усердных бобров и сделана попытка найти новых кандидатов на усердных бобров с использованием генетических алгоритмов [3, 4].

Постановка задачи

С момента публикации в 1962 году статьи [5], в которой автор предлагает строить усердных бобров (busy beaver game) и сравнивать между собой по указанному критерию, было сделано большое число попыток поиска усердных бобров, а также рассмотрено множество вариаций этой задачи [6].

Рассмотрим одну из вариаций задачи о поиске усердных бобров и дадим ее описание. Для этого рассмотрим машину Тьюринга, содержащую автомат с n состояниями, работающую над двоичным алфавитом $\{0, 1\}$. Существует несколько типов машин Тьюринга. В этой задаче рассматривается машина, работающая на бесконечной в обе стороны ленте. На каждом шаге машина имеет два параметра:

- состояние автомата;
- символ ленты, находящийся под головкой.

На основании этих параметров одновременно определяются:

- состояние, в которое переходит автомат;
- действие, которое совершает машина Тьюринга.

Действие может быть одним из следующих:

- записать символ в ячейку под головкой;
- передвинуть головку (влево или вправо).

Машина останавливается, когда достигает такой конфигурации, из которой нет перехода.

Пусть задана машина Тьюринга. Запустим ее на пустой ленте – на ленте, в каждой ячейке которой записан ноль.

Задача об усердных бобрах, как указано выше, состоит в поиске машины Тьюринга, содержащую автомат с n состояниями, которая будучи запущенной на пустой ленте, останавливается и записывает на ленту наибольшее число единичных символов.

Для больших значений n функцию усердного бобра сложно вычислить по нескольким причинам:

- пространство поиска очень велико – существует $(4n+1)^{2n}$ машин Тьюринга с n состояниями [7];
- отсутствие общего алгоритма для проверки того, останавливается ли машина Тьюринга [8];
- большое число шагов, которое может быть сделано машиной Тьюринга перед остановкой.

Рассматриваемой задачей является создание такого алгоритма генетического программирования, который позволил бы найти новых кандидатов на усердных бобров с управляющим автоматом из ***шести*** состояний.

Общая схема генетического алгоритма

Для генерации управляющих автоматов машин Тьюринга предлагается использовать *островной генетический алгоритм* [3].

Островной алгоритм традиционно состоит из следующих этапов:

- создание начального поколения;
- мутация и скрещивание;
- обмен особями между островами;
- отбор особей для формирования следующего поколения.

Через определенное число поколений все острова случайным образом разбиваются на пары, и на каждой паре островов особи перемешиваются – на каждом острове остается половина особей с одного острова и половина с другого.

Представление особи

Особь представляется в виде объекта в языке программирования *Java*. Этот объект имеет следующий интерфейс:

```
public interface Individual {
    public byte getInitialState();
    public void setInitialState(byte state);
    public ITransition[] getTransitions();
    public int getStepsNumber();
    public int getOnesNumber();
    public int getTransitionUsages(ITransition transition);
}
```

Генерация начального поколения

Все острова заполняются случайно сгенерированными машинами Тьюринга. Все машины имеют заранее заданное число состояний.

Оператор мутации (простой)

Простой оператор мутации, как и любой оператор мутации, получает на вход одну особь и возвращает также одну особь. При этом происходят следующие действия:

- изменение конечного состояния случайного перехода;
- с вероятностью 0.5 изменение стартового состояния на случайное;
- с вероятностью 0.5 на случайном переходе либо изменение направления перемещения ленточной головки, либо замена символа на переходе на случайный.

Оператор мутации (усиленный)

Усиленный оператор мутации отличается от простого тем, что изменение конечного состояния выполняется не у случайного перехода, а у того перехода который использовался наибольшее число раз при подсчете функции приспособленности.

Оператор скрещивания (однородный)

Однородный оператор скрещивания получает на вход две особи, и выдает также две особи потомков.

Данный оператор скрещивания особей аналогичен описанному в работе [9]. В качестве входной переменной выступает значение, прочитанное с ленты машины Тьюринга.

Оператор скрещивания (одноточечный)

Одноточечный оператор скрещивания получает на вход две особи, и выдает также две особи потомков.

Обозначим родительские особи – *P1* и *P2*, а потомков – *S1* и *S2*. Далее обозначим *P1.a* – переход в автомате особи *P1*, *P1.a.st* – номер начального состояния перехода *P1.a*.

Выполняются следующие действия:

- случайным образом выбирается состояние случайной из родительских особей, не умоляя общности, будем считать, что используется особь *P1*;
- подсчитываются кратчайшие расстояния от выбранного состояния в графе переходов особи *P1* до остальных состояний при помощи алгоритма *обхода в ширину* (*bfs*) [10]. За d_{max} обозначим максимальное из получившихся расстояний, $d[i]$ – расстояние до вершины с номером *i*;
- *S1* содержит *P1.a*, если и только если $d[P1.a.st] \le \frac{d_{\max}}{2}$; *S1* содержит *P2.a*, если и только если $d[P2.a.st] \ge \frac{d_{\max}}{2}$. Особь *S2* содержит, только переходы особей *P1* и *P2*, которые не содержатся в *S1*.

Работа данного оператора проиллюстрирована на 0.

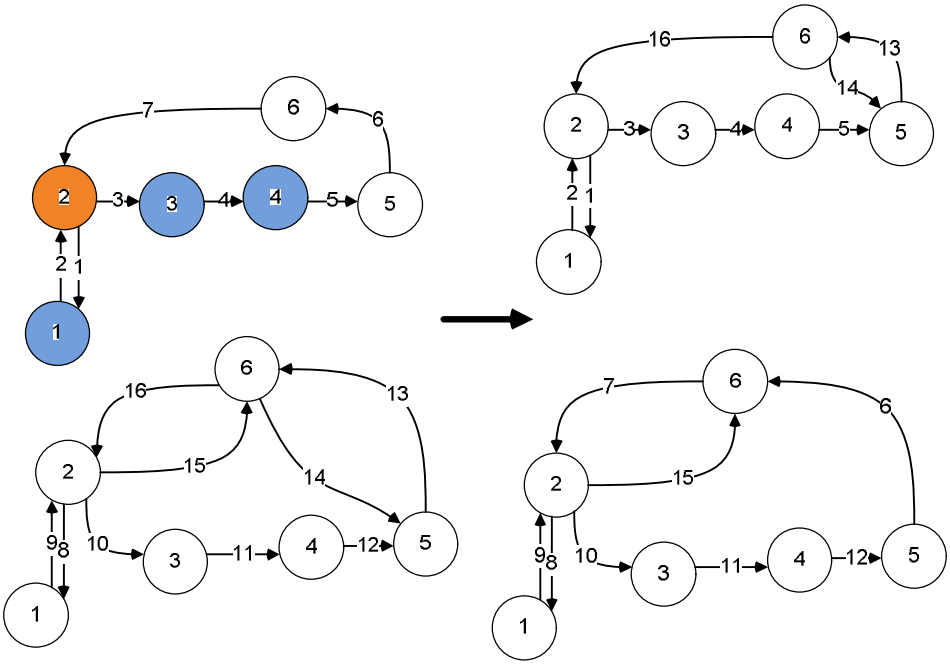


Рис. 1. Одноточечное скрещивание

На 0 оранжевым цветом отмечена стартовая вершина для алгоритма обхода в ширину, а синим – вершины, для которых выполнено $d[P1.a.st] \le \frac{d_{\max}}{2}$.

Вычисление функции приспособленности

В качестве функции приспособленности используется число единиц оставленных на ленте при эмуляции работы машины Тьюринга. Если машина не останавливается по преодолении заданного числа шагов, то эмуляция прекращается, и в качестве функции приспособленности такой машины используется выражение $F = \min(\frac{F_{\max}}{2}, c)$, где F_{max} – максимальное значение функции приспособленности среди всех особей предыдущего поколения, а c – число единиц оставленных рассматриваемой машиной Тьюринга на ленте во время работы.

Формирование следующего поколения

В качестве основной стратегии формирования следующего поколения используется *элитизм* [11]. При обработке текущего поколения отбрасываются все особи, кроме нескольких наиболее приспособленных. При рассмотрении текущего поколения отбрасываются все особи, кроме некоторой доли наиболее приспособленных — элиты. Эти особи переходят в следующее поколение. После этого оно дополняется до требуемого размера следующим образом: пока оно не заполнено, выбираются две особи из текущего поколения, и они с некоторой вероятностью скрещиваются или мутируют. Обе особи, полученные в результате мутации или скрещивания, добавляются в новое поколение. При формировании следующего поколения для проведения мутации используется либо простой, либо усиленный оператор мутации. Аналогично, для проведения скрещивания используется либо однородный, либо одноточечный оператор скрещивания. При этом смена используемых операторов происходит через фиксированное число поколений. Описанная эволюция происходит независимо на каждом из островов.

Также к поколению может применяться «малая» и «большая» мутации. При «малой» мутации поколения ко всем особям кроме элиты применяется оператор мутации. При «большой» мутации каждая особь либо мутирует, либо заменяется на случайно сгенерированную. Число поколений до «малой» и «большой» мутации постоянно во время работы алгоритма.

Результаты

При реализации описанного выше подхода была написана программа на языке *Java*. Программа использует датчик случайных чисел, поэтому при нескольких запусках могут получаться различные результаты.

Лучшая по всем запускам особь оставляет на ленте 70 единиц. Однако в среднем по всем запускам программы лучшая особь оставляет 20 единиц на ленте. Построить машины Тьюринга с подобными характеристиками вручную не представляется возможным [12]. Однако применением перебора автоматов машин Тьюринга были получены лучшие результаты – 239 единиц на ленте [6].

Во время работы алгоритма генетического программирования имеется возможность мониторинга результатов его работы. В каждом сгенерированном поколении можно изучить любую особь. На рис. 2 представлена диаграмма переходов управляющего автомата машины Тьюринга, сгенерированная программой.

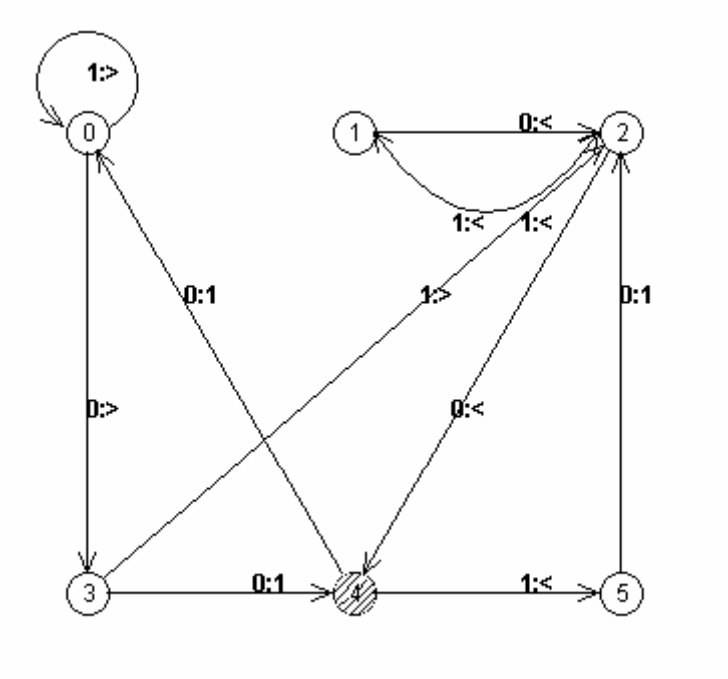


Рис. 2. Диаграмма переходов управляющего автомата машины Тьюринга

Приведенный на рис. 2 автомат машины Тьюринга получен в 500-м поколении. Соответствующая ему машина Тьюринга оставляет на ленте 20 единиц после завершения работы, совершая при этом 129 шагов.

На переходах автомата машины Тьюринга используются пометки в формате `S:A`, где `S` – символ, по которому происходит переход; `A` – действие, выполняемое при переходе.

Действие бывает двух типов: запись нового символа на ленту, в этом случае `A` является нулем или единицей, либо перемещение ленточной головки в одном из направлений: символ «<» при перемещении головки налево и символ «>» при перемещении направо.

Стартовое состояние автомата машины Тьюринга заштриховано.

Описанную программу можно загрузить с сайта http://my-svn.assembla.com/svn/beaver/.

Заключение

В работе приведено описание задачи о поиске усердных бобров. Предложен островной алгоритм генетического программирования, осуществляющий построение кандидатов на усердных бобров. Написана программа, демонстрирующая работу описанного алгоритма.

Литература

1. Ехали тьюрмиты и тримувьи на… машине Тьюринга //Компьютерные инструменты в образовании. 2005. Вып. 3.
2. Хопкрофт Д., Мотвани Р., Ульман Д. Введение в теорию автоматов, языков и вычислений. М.: Вильямс, 2002.
3. Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы. М.: Физматлит, 2006.
4. Рассел С., Норвиг П. Искусственный интеллект: современный подход. М.: Вильямс, 2006.

5. Rado T. On Non-Computable Functions //The Bell System Technical Journal. 1962. Vol. 41. N3, pp. 877–884.
6. Ross K., Kellett O., Heuveln B., Bringsjord S. A New-Millenium Attack on the Busy Beaver Problem. 2006. http://www.cs.rpi.edu/~kelleo/busybeaver
7. Shallit J. Handout on The Busy Beaver Problem. University of Waterloo. 1988. http://grail.cba.csuohio.edu/~somos/beaver.ps
8. Turing A. On Computable Numbers, with an Application to the Entscheidungsproblem //Proceedings of the London Mathematical Society. 1937. Ser. 2. Vol. 42, pp 230–265.
9. Царев Ф.Н., Шалыто А.А. О построении автоматов с минимальным числом состояний для задачи об «умном муравье» /Сборник докладов X международной конференции по мягким вычислениям и измерениям. СПбГЭТУ "ЛЭТИ". Т.2, 2007, с. 88–91. http://is.ifmo.ru/download/ant_ga_min_number_of_state.pdf
10. Кормен Т., Лайзерсон Ч., Ривест Р. Алгоритмы. Построение и анализ. М.: МЦМНО, 2000. 960 с.
11. De Jong K. An analysis of the behavior of a class of genetic adaptive systems. PhD thesis. Univ. Michigan. Ann Arbor, 1975.
12. Посов И.А. Занятой бобер //Компьютерные инструменты в образовании. 2007. Вып. 2.

УДК 004.357

РЕАЛИЗАЦИЯ ДРАЙВЕРА ДЛЯ АНАЛОГОВОГО USB-РАДИО, ИСПОЛЬЗУЮЩЕГО VIDEOFORLINUX-ИНТЕРФЕЙС В ЯДРЕ LINUX

А.Г. Климов
(Московский физико-технический институт (государственный университет))
Научный руководитель – Ф.Ф. Суетов
(Центральный научно-исследовательский институт «Комета»)

В докладе рассказывается реализация драйвера для операционной системы Linux, описана работа этого драйвера внутри ядра ОС.
Ключевые слова: драйвер, VideoForLinux, usb, модуль, Linux

Введение

Для ядра Linux существует проблема: недостаток драйверов устройств, особенно это касается некоторых редких USB-устройств.

Ядро Linux (загрузить исходные тексты можно с сайта kernel.org) представляет некоторые USB-устройства в пространство пользователя в виде hid-интерфейса. Однако, если устройство является радио- или тв-тюнером, то для работы с ним, придется пользоваться специальными программами, причем различающимися для каждого отдельного устройства. Намного эффективнее пользоваться одной-двумя программами для своего типа устройств, которые взаимодействуют с VideoForLinux (V4L) слоем, предоставленным ядром.

Основная часть

Устройство, для которого написан драйвер, представлено через hiddev-интерфейс, поэтому некоторая трудность состояла в том, чтобы удалить процесс регистрации устройства в hid-слое.

Задача состоит в следующем: создать модуль, который с одной стороны управляет устройством через USB-подсистему, а с другой стороны регистрируется в слое Video For Linux, обрабатывая ioctl-вызовы, попадающие в V4L2 и предназначенные для данного устройства. Работа этого слоя описана в [1]. Посмотреть текущую версию можно на сайте linuxtv.org. Схематически на рис. 1 показано иерархическое место модуля в структуре ОС.

Для взаимодействия с USB-подсистемой можно воспользоваться идеей URB (USB Request Block). Кроме этого, существуют три функции, благодаря которым можно отказаться от использования URB. Это: usb_bulk_msg, usb_control_msg и usb_interrupt_msg. Для простого обмена данными с устройством вполне подходит usb_bulk_msg. Эта функция формирует URB, посылает его и ждет завершения операции или таймаута. Функции для работы с USB-подсистемой описаны в [2].

Для представления в V4L2 слое модуль регистрируется в нем как радио-устройство, используя video_register_device с параметром VFL_TYPE_RADIO. В модуле происходит назначение ioctl-вызовов, которые выполняются при необходимости. В итоге создается файл /dev/radio0, который используют пользовательские программы, например – kradio, gnomeradio или mplayer.

Стоит сказать пару слов о том, что происходит с модулем, когда ОС совершает операцию Suspend-to-Disk. В модуле имеются две функции, служащие этой цели – usb_amradio_suspend и usb_amradio_resume. Они являются частью структуры,

описывающей usb-драйвер. Очевидно, что первая – останавливает устройство, вызывая amradio_stop, вторая – делает прямо противоположное.

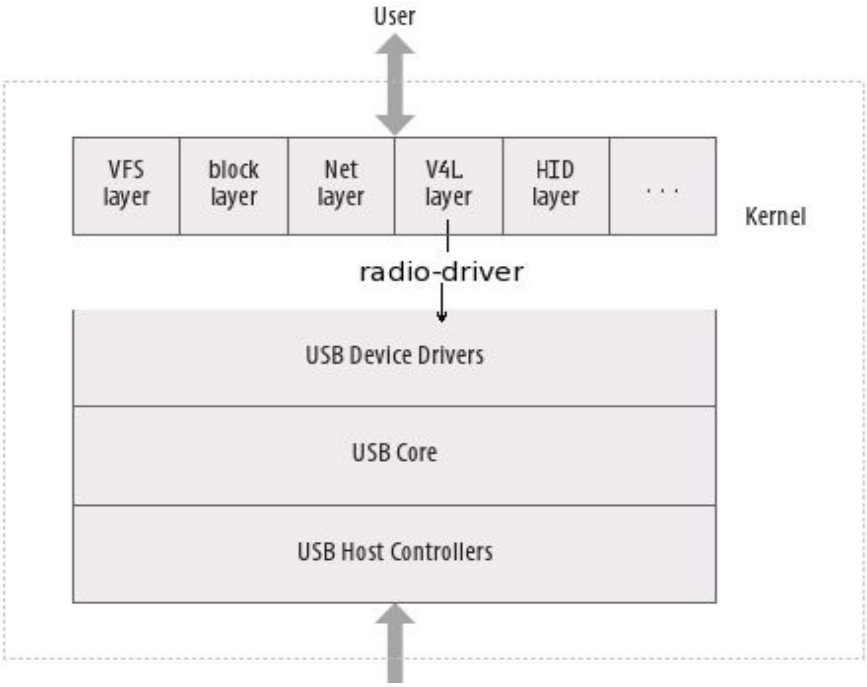


Рис. 1. Иерархическое место модуля в структуре ОС

Заключение

В настоящее время модуль находится в V4L/DVB-репозитории на сервере linuxtv.org. Кроме этого, первая работающая версия драйвера уже включена в ядро Linux 2.6.28. Финальные исходные тексты модуля обсуждались с разработчиками V4L2-подсистемы и драйверов, использующих этот интерфейс. Также исходный текст был просмотрен одним из программистов Intel (ранее он работал в Red Hat) – Аланом Коксом. Ведется дальнейшая разработка драйвера для поддержки им большей функциональности устройства и стабильности работы самого драйвера.

Литература

1. Video for Linux Two API Specification. [Электронный ресурс] – 2008. – LinuxTV – Television with Linux http://linuxtv.org, режим доступа свободный.
2. Corbert J., Rubini A., Kroah-Hartman G. Linux Device Drivers. – 3-е изд. – O`Reilly – 2005. – 542 с.

УДК 519.255

ПРИМЕНЕНИЕ ПРЕОБРАЗОВАНИЯ АДАМАРА ДЛЯ ПРОСТРАНСТВЕННОЙ ФИЛЬТРАЦИИ ШУМОВ

А.А. Сухарев
(Санкт-Петербургский государственный политехнический университет)
Научный руководитель – д.ф.-м.н. Б.Г. Подласкин
(Физико-технический институт им. А.Ф. Иоффе РАН)

В докладе рассмотрена концепция пространственной фильтрации временного шума канала связи при использовании предварительного кодирования информации с помощью преобразования Адамара. Показана возможность концентрации максимальной плотности шума в различных частях приемного экрана при использовании различных способов упорядочивания базисных функции интегрального преобразования.

Ключевые слова: преобразование Адамара, кодирование информации, фильтрация шума

Введение

Обработке изображений с помощью преобразования Адамара (Hadamard) в настоящее время уделяется большое внимание. Основными целями, которые преследуются при использовании этого преобразования, являются сжатие передаваемой информации, фильтрация изображений, распознавание образов в случае достаточного взаимного различия их пространственных спектров и ряд других задач, связанных с удобством кодирования и восстановления сигналов. В работах [1, 2] была поставлена и обоснована задача пространственной локализации аддитивного шума путем перестановки функций Уолша (Walsh), составляющих матрицу преобразования при кодировании изображений с помощью матрицы Адамара. Специфика современной элементной базы, главным образом двумерных многоэлементных фотоприемников, которые используются для устройств ввода анализируемых изображений, оставляют реализацию преобразования Адамара в рамках достаточно быстрых, но, тем не менее, последовательных методов обработки двумерных массивов информации, которые представляют собой различного рода изображения.

В настоящее время накоплен большой опыт по обработке, сжатию и фильтрации изображений, в том числе с использованием интегральных бинарных преобразований типа преобразование Уолша-Адамара [3]. Такая задача может быть успешно решена при предварительном представлении исходных данных в виде двумерных массивов. Известны работы по кодированию и дальнейшей передаче временных сигналов в формате преобразования Адамара, в которых показана возможность сокращения объема передаваемой информации за счет отсечения слабых спектральных коэффициентов. Преобразование Адамара было выбрано по той причине, что набор базисных функций является фиксированным, а матрица преобразования является по сути двоичной, т.е. максимально простой для построения и обработки [4]. В отличие от большинства известных работ, акцент нашего внимания сосредоточен на обработке сигнала с целью не столько предварительного сжатия информации, сколько обеспечения максимального подавления шумов канала связи на основе метода пространственной локализации дисперсии шума. Пространственная фильтрация временного шума является принципиально новой концепцией, основанной на замене переменной при передаче сигнала по каналу связи и представлении шумов канала в виде изображения его спектра в базисе Адамара [5]. Исследование пространственной локализации аддитивного шума путем перестановки базисных функций является фундаментальной задачей при изучении комбинаторных свойств интегральных преобразований. Разработка новых информационных технологий, основанных на использовании таких матриц, актуальна для создания но-

вых форматов передачи информации. Применение пространственной фильтрации шума актуально при передаче любых сигналов, имеющих области повышенной информативности.

Постановка задачи

Задача исследования пространственной локализации шума возникает при последовательной передаче по каналу связи элементов матрицы спектральных коэффициентов $W = HF$, полученных в результате двумерного преобразования Адамара H над изображением F. В этом случае образуется вектор $L(HF)$ (L – операция построчной развертки), на который в канале связи накладывается шум ψ. При обратном преобразовании восстанавливается новое изображение F′, представляющее собой сумму исходного изображения F и аддитивного члена $F' = F + H^{-1}L^{-1}\psi$, который является изображением спектра шума ψ в базисе H, то есть:

$$F' = F + H^{-1}(L^{-1}\psi).$$

Была высказана гипотеза о том, что, изменение организации системы базисных функций путем перестановки строк в матрице Адамара (т.е. изменение порядка передачи спектральных компонент), влияет на распределение спектра шума в пространстве изображения. При этом можно добиться сосредоточения максимальных шумовых искажений изображения в различных зонах изображения. Иначе говоря, можно производить пространственную фильтрацию временного шума, концентрируя основную его часть в наименее информативных участках восстановленного изображения. Математическое обоснование выдвинутой нами гипотезы было проведено в работе [2]. В этой работе был проведен математический анализ влияния перестановки строк матриц преобразования Адамара на распределение дисперсии шума в поле восстановленного изображения. Было показано, что при переходе от классического упорядочивания функций Уолша по Пэли (Pely) к секвентному упорядочиванию (т.е. упорядочиванию расположения строк по числу перемены знака) с помощью преобразования Грэя происходит концентрация дисперсии шума в различных участках экрана.

По определению, преобразование Грея (Gray) представляет собой функцию g, сопоставляющую каждому $i \in [0,1)$ число $g(i) \in [0,1)$, k-я двоичная цифра которого равна $(i_k + i_{k-1}) \bmod 2;\ k = 1, 2...n;\ i_0 = 0$. Здесь i – номер функции Уолша в упорядочивании Пэли. В результате можно представить перестановочную матрицу G, с помощью которой координата x_k переводится на g(k)-ое место, а на ее место становится координата $x_{g^{-1}(k)}$. Поскольку $G^{-1}HG^{-1} = H$ и $GHG = H$, то в результате применения преобразования Грея на выходе декодирующего устройства будем иметь: $F' = F + HG^{-1}\psi$, то есть тождественно восстановленное изображение F и спектр шума в базисе Адамара, упорядоченному по Грею.

Для подтверждения возможности пространственной фильтрации временного шума с помощью описанной процедуры было проведено расчетное моделирование этих процессов при различной спектральной плотности шума и при различной организации строк матрицы Адамара. В качестве спектральной плотности аддитивного шума была выбрана функция Гаусса при различных параметрах σ:

$$p(t) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(\frac{-(t - t_0)^2}{2\sigma^2}\right).$$

Рассматривая помеху ψ как случайный вектор, поставим вопрос об определении вероятностных характеристик погрешности $\Delta F = F' - F = \psi H$. Поскольку ψ – стационарный в широком смысле вещественный случайный процесс, централизованный математическим ожиданием, то $E[\psi_i] = t_0 = 0$ и $E[\psi_i \psi_j] = K(i-j) = K(m)$, где $K(m)$ корреляционная функция, которая является положительно определенной и допускает спектральное представление:

$$K(m) = \int_{-\pi}^{\pi} e^{imt}\, p(t)dt,$$

где $p(t)$ – спектральная плотность шума.

На основе корреляционной функции $K(m)$ могут быть вычислены дисперсии компонент вектора $H\psi$, которые определяются диагональными элементами ковариационной матрицы

$$\sigma^2\left((H\psi)_i\right) = K(0) + \frac{2}{N}\sum_{m=1}^{N-1} K(m) \sum_{k=0}^{N-m-1} h_{i,k} h_{i,k+m}, \qquad (1)$$

где i принимает значения от 1 до N (здесь и ранее N – число элементов изображения).

Поскольку каждая дисперсия выражается через элементы соответствующие ей по номеру строки матрицы Адамара, изменение порядка расположения строк в матрице Адамара изменяет порядок следования компонент векторов дисперсии. Таким образом, после преобразования векторов дисперсии в матрицу, дисперсии будут по-другому располагаться в пространстве изображений. В связи с этим важным вопросом становится способ упорядочивания функций Уолша, образующих строки (и столбцы) матрицы H.

Классический способ упорядочивания, называемый схемой Пэли, образуется при формировании матрицы Адамара порядка 2N при помощи следующей операции:

$$H_{2N} = \begin{vmatrix} H_N & H_N \\ H_N & -H_N \end{vmatrix}.$$

При использовании этой схемы распределение дисперсии шума по полю восстановленного изображения крайне нерегулярно. В данной работе схема Пэли используется, прежде всего, для иллюстрации нерегулярного распределения дисперсий и для собственно формирования матрицы Адамара заданной размерности.

Поскольку количество элементов матрицы Адамара пропорционально четвертой степени размера сигнала, дальнейший анализ распределения дисперсий, задаваемых формулой (1) для сколько-нибудь существенных размерностей преобразования решено проводить с помощью компьютерного моделирования передачи сигналов различной размерности по каналу с шумом. Необходимо отметить, что подобные программы уже создавались ранее (для матриц Адамара малой размерности (2×2) и (4×4)).

Основная часть

Данное исследование направлено, в том числе, и на нахождение матриц преобразования, производящих необходимую пространственную фильтрацию шума. При этом такие матрицы остаются матрицами преобразования Адамара, вариации подвергается лишь упорядоченность их строк. Всего использовано пять типов упорядочивания строк: упорядочивание «по Пэли», по возрастанию секвенты строки, по убыванию секвенты строки, по убыванию нечетной и возрастанию четной секвенты строки, по возрастанию нечетной и убыванию четной секвенты строки. Данные упорядочивания обозначены соответственно: «Pely», «Increase», «Decrease», «Inc_Even», «Dec_Even».

Был проведен анализ воздействия преобразования Адамара на шум, путем подсчета теоретического распределения дисперсий шума в пространстве сигнала. По-

скольку одновременный анализ, как сигнала, так и шума, достаточно сложен, то было проведено рассмотрение влияния преобразования Адамара на зашумленный нулевой сигнал. Оцениваемым критерием в данной задаче является пространственное распределение дисперсий шума, в случае применения различных форм упорядочивания строк матрицы преобразования. Полученные для одинарного преобразования распределения дисперсий шума в пространстве изображения размерности 32×32 для различного упорядочивания матриц представлены на рис. 1.

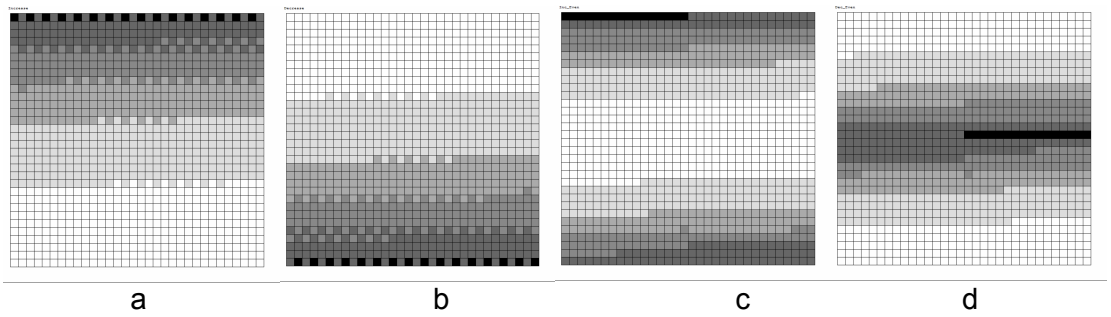


Рис. 1. Распределение дисперсии шума для различного упорядочивания матрицы Адамара a – «Increase»; b – «Decrease»; c – «Inc_Even»; d – «Dec_Even»

Последующим этапом работы стало введение концепции и использование двойного преобразования Адамара, т.е. передачи двух сигналов – преобразованного одной из вышеупомянутых матриц и преобразованного такой же, но «повернутой» матрицей. Суммарная дисперсия в каждой точке изображения была рассмотрена, как сумма дисперсий от обеих передач, т.е. в предположении, что данные передачи происходят последовательно и совершенно независимо. В ходе данного этапа были получены картины распределения дисперсий, хорошо согласующиеся с теоретическими представлениями и позволяющие утверждать, что данный способ кодирования сигнала позволяет эффективно перераспределять дисперсии внутри изображения и в частности создавать области изображения с дисперсией на 1–2 порядка меньшими, чем при передаче без осуществления преобразования. Полученные для двойного преобразования распределения дисперсий шума в пространстве изображения размерности 32×32 для различного упорядочивания матрицы Адамара представлены на рис. 2.

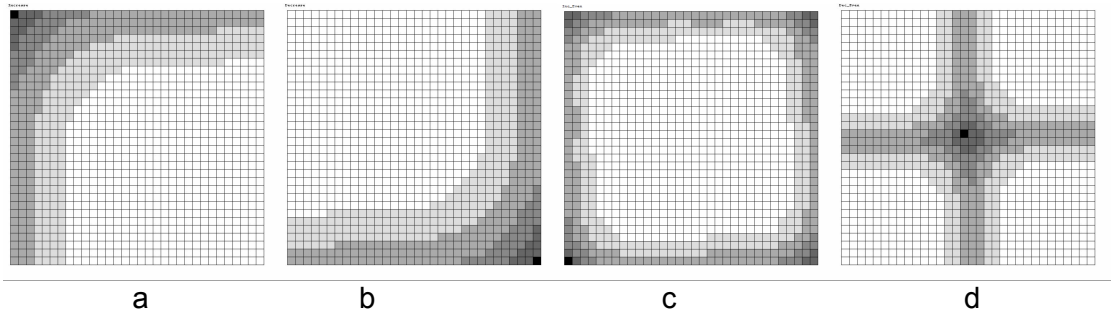


Рис. 2. Распределение дисперсии шума для различного упорядочивания матрицы Адамара при двойном ортогональном преобразовании a – «Increase»; b – «Decrease»; c – «Inc_Even»; d – «Dec_Even»

Дальнейшее повышение размеров передаваемых сигналов сопряжено с серьезными трудностями, возникающими по причине того, что размерность матрицы преобразования Адамара пропорциональна квадрату размерности сигнала и уже для сигналов размерности 128×128 элементов количество элементов матрицы преобразования составляет 2^{28}. Несмотря на отмеченную ранее возможность хранения элементов матрицы Адамара в однобитовом представлении, обработка таких больших массивов данных затруднительна, и что более важно, существенно замедляет проведение вычислений. В

связи с этим в ходе данной работы был реализован алгоритм построчного формирования матриц Адамара любой заданной размерности. (Основным отличительным свойством строки матрицы Адамара является ее секвента, т.е. число смен знака элементов данной строки, именно этот параметр и является единственным необходимым для формирования строки матрицы). Это позволило полностью избавиться от хранения в памяти и обработки внутри программы огромных матриц преобразования за счет того, что, при проведении преобразования, строки матрицы Адамара заново формируются в порядке, задаваемом последовательностью секвент, и не записываются для хранения. Несмотря на то, что при таком подходе к осуществлению преобразования матрицы Адамара формируются не единовременно, а многократно, на каждом акте преобразования, время, затрачиваемое на осуществление серии преобразований, оказывается меньше, а объем, занимаемой программой памяти, может падать на порядки (в зависимости от размеров матриц). Также необходимо отметить, что подобный способ формирования матриц Адамара не приводит к каким-либо проблемам при осуществлении двойного преобразования, в котором используется «повернутая» матрица преобразования, т.к. он позволяет формировать и такие матрицы.

На последнем этапе данной работы исследуются распределения самого шума при моделировании передачи сигнала в канале. В работе показано, что распределение дисперсий шума можно использовать, как хорошую оценку распределения самого шума в пространстве изображения. В ходе данного этапа для одинарного преобразования Адамара получены распределения шума при различных значениях соотношения мощностей шума и сигнала, и для различных форм упорядочивания строк матриц преобразования. В качестве грубой оценки распределения шума введен порог. Все значения выходного сигнала, отличающиеся от входных больше, чем на значение порога будем считать переданными «неправильно», в противном случае – «правильно». Полученные для одинарного преобразования распределения «правильно»/«неправильно» переданных элементов для соотношения мощностей шума и сигнала равного единице в размерности сигнала 64×64 для различного упорядочивания матриц Адамара представлены на рис. 3.

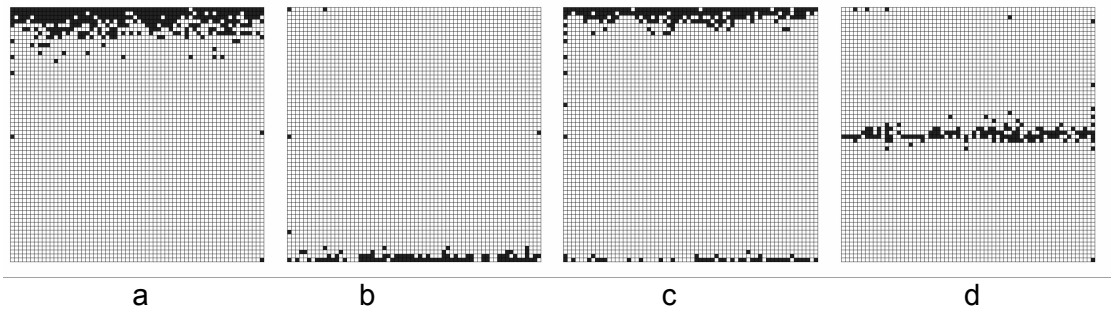


Рис. 3. Распределение ошибочно переданных элементов для различного упорядочивания матрицы Адамара при двойном ортогональном преобразовании a – «Increase»; b – «Decrease»; c – «Inc_Even»; d – «Dec_Even»

При сравнении с соответствующими распределениями дисперсий видно, что распределения дисперсий шума в пространстве изображения отвечают распределениям реального шума, при моделировании передачи сигнала, и, соответственно, могут быть использованы для оценки локализации шума в пространстве изображения.

Заключение

В результате проведенной работы была подтверждена концепция возможности пространственной фильтрации временного шума канала связи на основе использования

преобразования Адамара. К важнейшим полученным результатам можно отнести следующее:

(1) Доказана возможность применения преобразования Адамара для перераспределения дисперсий шума в передаваемом сигнале большой размерности, без потери какой либо информации в сигнале в случае отсутствия шума и написана программа, подтверждающая это путем моделирования данного эксперимента.

(2) Построены схемы использования преобразования, в частности двойное преобразование, получены соответствующие им формулы, описывающие теоретические распределения дисперсий.

(3) Получены теоретические распределения дисперсий и распределения шума в пространстве сигнала для матриц преобразования различной размерности и формы упорядочивания строк. Получены теоретические распределения дисперсий и распределения шума в пространстве сигнала для матриц преобразования различной размерности и формы упорядочивания строк.

Дальнейшие исследования будут проводиться в следующих направлениях:

(1) Исследование коррелированных способов передачи пары сигналов при использовании двойного преобразования.

(2) Исследование влияния шумов, задаваемых принципиально различными спектральными плотностями, на распределение дисперсий в пространстве изображения.

Литература

1. Подласкин Б.Г. Пространственная фильтрация временного шума при реализации преобразования Адамара на фотоприемной матрице //ЖТФ. – 2007. – Т.77. – Вып.5. – С. 139–142.
2. Каргаев П.П., Фомин С.В. Разложение Уолша-Фурье со случайными коэффициентами //Теория вероятностей и ее применение. 1990. Т.35, Вып.2, С.271–281.
3. Ahmed N., Rao K.R. Spectral analysis of linear digital systems //Electr. Lett. – 1993. – V.6, №2, P.117–121.
4. Хармут Х. Теория секвентного анализа. – М.: Мир, 1980. – 574 с.
5. Подласкин Б.Г., Гук Е.Г., Сухарев А.А. Развитие теории двумерного преобразования Адамара для пространственной локализации аддитивного шума //ЖТФ. – 2008. – Т.78. №8. – С. 9–13.

УДК 004.855.5

ЭЛЕКТРОННЫЙ ПРАКТИКУМ ДЛЯ ОСВОЕНИЯ УНИВЕРСАЛЬНЫХ ИНСТРУМЕНТАЛЬНЫХ КОМПЕТЕНЦИЙ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

А.С. Пирская
Научный руководитель – д.т.н., профессор Л.С. Лисицына

Статья посвящена разработке электронного практикума для формирования практических способностей применять информационные технологии для создания цифровых ресурсов. Проведена детализация исходной компетенции и разработаны 2 компетентностные модели – модель иерархии результатов обучения и модель причинно-следственных связей, которая позволяет формировать различные образовательные траектории. Описаны технические средства для автоматизации планирования различных траекторий образовательного процесса.

Ключевые слова: компетентностные модели, инструментальные компетенции, элементарные компетенции, содержательные компетенции, базовые образовательные модули, состояния образовательного процесса

Введение

В соответствии с компетентностным подходом к образованию процесс обучения определяется компетентностной моделью специалистов, которая включает профессиональные, общенаучные, инструментальные и социально-личностные компетенции. Универсальные инструментальные компетенции являются общими для направлений подготовки и предшествуют формированию профессиональных компетенций: объекты деятельности универсальных компетенций выступают в роли видов деятельности профессиональных компетенций. Универсальные компетенции формируют в процессе подготовки базовые навыки принятия решений в сфере техники и технологий, владение современными информационными и коммуникационными технологиями и т.п. [1].

При разработке электронного практикума необходимо учитывать, что структурирование предмета должно отражать компетентностный характер подготовки специалистов – минимизация содержания образования для освоения элементарных компетенций и должно быть произведено на основании следующих принципов [2]:

1. *Направленность изучения*. Изучение дисциплины должно обеспечивать последовательное формирование возрастающей компетентности у обучаемого. Для этого необходимо разработать перечень универсальных инструментальных компетенций, которые должен освоить обучаемый.

2. *Модульность структуры*. Для каждой универсальной инструментальной компетенции должен быть разработан образовательный модуль, состоящий из БОМ, каждый из которых будет обеспечивать приращение компетентности у обучаемого при изучении предмета, определяемое на основе требований к уровням компетентности, профилям и уровням образования.

3. *Многопрофильность подготовки*.

4. *Вариативность содержания*. Используя альтернативные модели, методы, технологии и т.п. для освоения ЭК, можно разработать вариативное содержание образовательного модуля для ЭК. Альтернативные способы изучения предмета позволят задавать различные характеристики нагрузки.

При разработке компетентностно-ориентированной структуры и содержания электронного практикума для освоения универсальных инструментальных компетенций в области информационных технологий должны быть решены следующие задачи:

1. Анализ предметной области для выявления объектов и видов деятельности обучаемых.

2. Разработка моделей для управления структурой и содержанием практикума.

3. Разработка содержания электронного практикума.

4. Автоматизация проектирования возможных траекторий образовательного процесса.

Основная часть

Целью изучения практикума является формирование у обучаемых практических способностей *применять информационные технологии для создания цифровых ресурсов*. На основе анализа и детализации видов деятельности обучаемых были сформулированы следующие универсальные инструментальные компетенции (1-ый этап детализации), выражающие *необходимость формирования у обучаемых способности*:

1. Применять растровый графический редактор Adobe Photoshop CS3 для создания цифровых ресурсов.

2. Применять векторный редактор Adobe Flash CS3 для создания цифровых ресурсов.

3. Применять язык гипертекстовой разметки HTML 4.01 для создания цифровых ресурсов.

4. Применять каскадные таблицы стилей для оформления сайтов.

5. Применять язык JAVASCRIPT 1.7 для управления событиями объектов web-страницы и обозревателя.

6. Применять HTML-редактор Adobe Dreamweaver CS3 для создания цифровых ресурсов.

7. Применять расширенный язык разметки XML 1.0 для создания цифровых ресурсов.

8. Применять подход AJAX для создания цифровых ресурсов.

На втором этапе детализации полученных компетенций разрабатывались содержательные компетенции, т.е. уточнялись виды цифровых ресурсов для каждой технологии, которые позволят обучаемым освоить данные виды деятельности. Данный этап завершился получением четырнадцати содержательных компетенций, освоение которых планировалось на начальном и базовом уровнях. Таким образом, для достижения результатов сформированности разработанных за два этапа детализации компетенций было установлено тридцать одно различное состояние образовательного процесса. Для идентификации результатов сформированности компетенций в этих тридцать состояниях была проведена дальнейшая детализация компетенций (третий этап) и сформулировано девяносто четыре умения, которые должны сформировать практические навыки у обучаемых по применению тех или иных информационных технологий для создания цифровых ресурсов.

Полученная надстройка в виде иерархии результатов формирования компетенций у педагогов, приведенная на рис. 1, определяет модульную структуру разрабатываемого практикума. Таким образом, структура разрабатываемого практикума содержит шестнадцать образовательных модулей, состоящих из тридцати одного базового образовательного модуля (БОМ) (по количеству различных состояний образовательного процесса).

Далее для отбора компетентностно-ориентированного содержания модулей разрабатывается модель образовательного процесса, устанавливающая причинно-следственные связи между умениями его состояний. Модель причинно-следственных связей приведена на рис. 2. Такая модель или план-граф является ориентированным гиперграфом и служит компетентностной моделью для планирования целостного образовательного процесса. В этой модели вершины моделируют состояния образовательного процесса, соответствующие результатам обучения, а дуги – траектории образователь-

ного процесса, соответствующие базовые образовательные модули. Таким образом, практикум имеет модульную структуру – состоит из образовательных модулей, каждый из которых обеспечивает направленное формирование и приращение компетентности в процессе обучения.

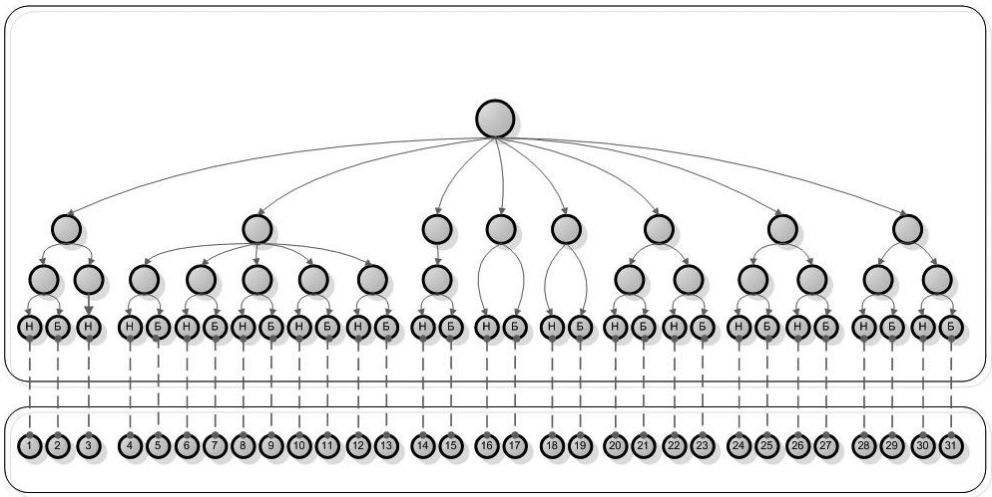


Рис. 1. Модель иерархии результатов обучения

План-граф позволяет синтезировать минимальный модульный план изучения дисциплины. Для этого необходимо решить следующие задачи:

1. Минимизировать перечень состояний компетентности, освоение которых необходимо и достаточно для ожидаемого результата обучения.

2. Определение порядка освоения состояний компетентности.

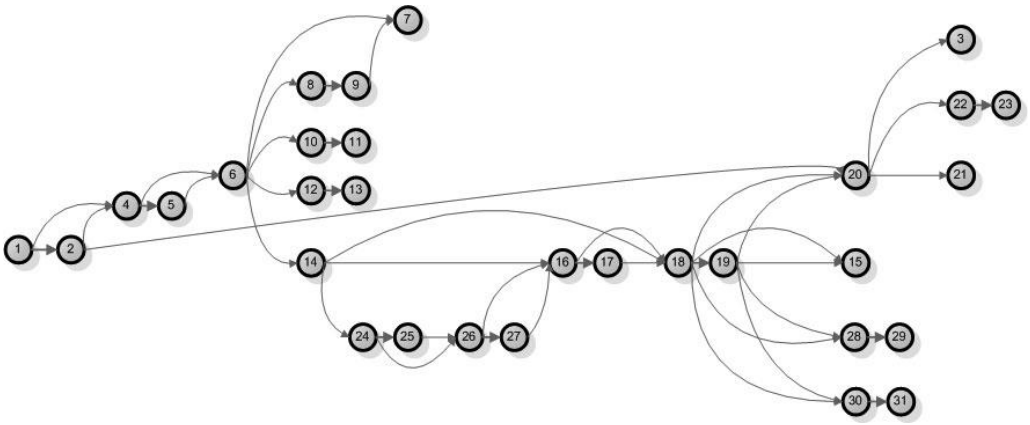


Рис. 2. Модель причинно-следственных связей

Содержание БОМ разрабатывается по принципу необходимости и достаточности [2], т.е. в состав БОМ входят учебно-методические материалы при изучении которых обучаемый получит необходимый и достаточный объем знаний и пониманий, умений и навыков для формирования соответствующих компетенций. В табл. 1 приведен перечень образовательных модулей и рекомендуемая трудоемкость каждого модуля.

№ п/п	Наименование образовательного модуля	Кол-во БОМ	Хар-ки уч. нагрузки		Всего, ч.
			нач. ур.	баз. ур.	
1	Применение растрового графического редактора Adobe Photoshop CS3 для создания и редактирования изображений	2	2	4	6

2	Применение растрового графического редактора Adobe Photoshop CS3 для фотогалереи для web	1	2	-	2
3	Применение векторного редактора Adobe Flash CS3 для создания анимированных изображений (баннеров, анимированных кнопок и т.д.)	2	2	4	6
4	Применение векторного редактора Adobe Flash CS3 для создания сайтов	2	2	6	8
5	Применение векторного редактора Adobe Flash CS3 для создания интерактивных демонстрационных материалов	2	6	8	14
6	Применение векторного редактора Adobe Flash CS3 для создания фотогалереи для web	2	4	6	10
7	Применение векторного редактора Adobe Flash CS3 для создания тестов	2	4	6	10
8	Применение языка гипертекстовой разметки HTML 4.01 для создания сайтов	2	2	4	6
9	Применение каскадных таблиц стилей для оформления web-страниц	2	2	4	6
10	Применение языка JAVASCRIPT 1.7 для управления событиями объектов web-страниц	2	2	4	6
11	Применение HTML-редактора Adobe Dreamweaver CS3 для создания сайтов	2	2	6	8
12	Применение HTML-редактора Adobe Dreamweaver CS3 для создания тестов	2	2	4	6
13	Применение расширенного языка разметки XML 1.0 для разработки структурированных документов	2	2	4	6
14	Применение расширенного языка разметки XML 1.0 для создания web-страниц	2	4	6	10
15	Применение подхода AJAX для создания фотогалереи для web	2	6	8	14
16	Применение подхода AJAX для создания сайтов	2	6	8	14
ИТОГО:		31	50	78	132

Таблица 1. Структура и характеристики учебной нагрузки образовательных модулей для освоения элементарных компетенций результата обучения «Применять информационные технологии для создания цифровых ресурсов»

Для моделирования траекторий образовательного процесса разработан программных модуль в помощь преподавателю для отбора ожидаемых результатов обучения и построения минимального модульного плана изучения дисциплины в соответствии с требуемой учебной нагрузкой. Ядром данной технологии является синтез компетентностной модели специалиста в виде рекомендуемого модульного плана, который представляет собой упорядоченный перечень состояний компетентности обучаемых, необходимый и достаточный для получения ожидаемого результата обучения. Упорядоченность перечня указывает на порядок освоения состояний компетентности и служит для планирования и расчета траектории целостного образовательного процесса на основе разработанного план-графа.

Модуль в пошаговом режиме предоставляет возможность отбора элементарных результатов обучения и синтезирует на основе отбора модульный план с упорядоченным перечнем образовательных модулей для достижения ожидаемого результата обучения. Для построения модульного плана в план-графе происходит поиск и композиция минимальных путей достижения результата обучения.

На рис. 3 и 4 приведен пример выбора информационных технологий для обучения студентов в рамках изучения дисциплины и виды цифровых ресурсов, которые могут быть созданы в рамках использования данной технологии и выбрать уровень освоения компетенции.

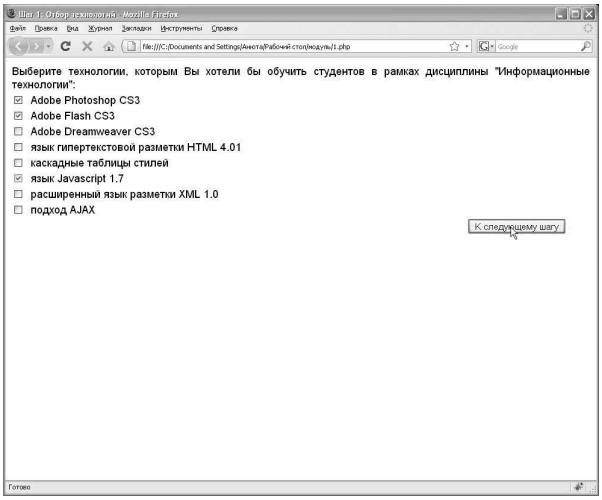


Рис. 3. Первый шаг работы модуля

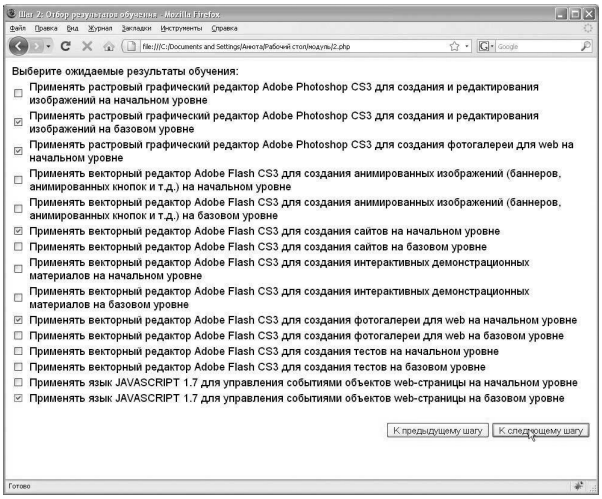


Рис. 4. Второй шаг работы модуля

Следующим шагом работы модуля является построение минимального модульного плана проведения занятий, построенного на основе модели причинно-следственных связей. Отобранные преподавателем технологии и виды цифровых ресурсов соответствуют состояниям образовательного процесса (рис. 5). Модульный план строится на основе композиции путей в план-графе.

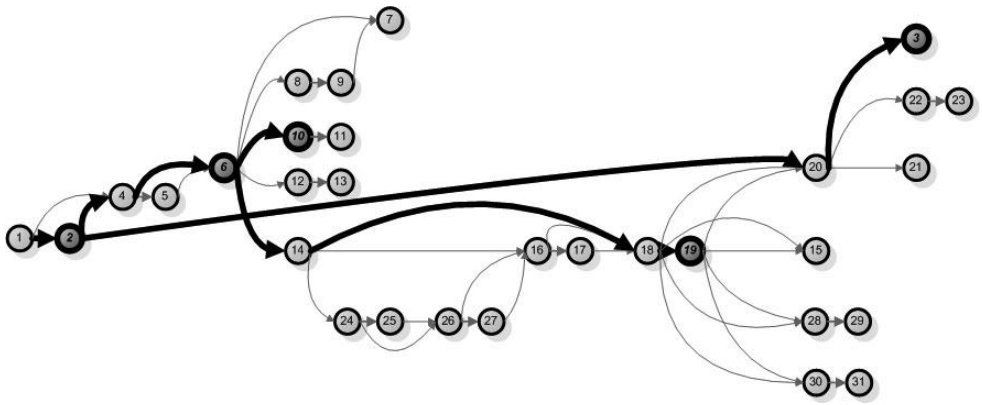
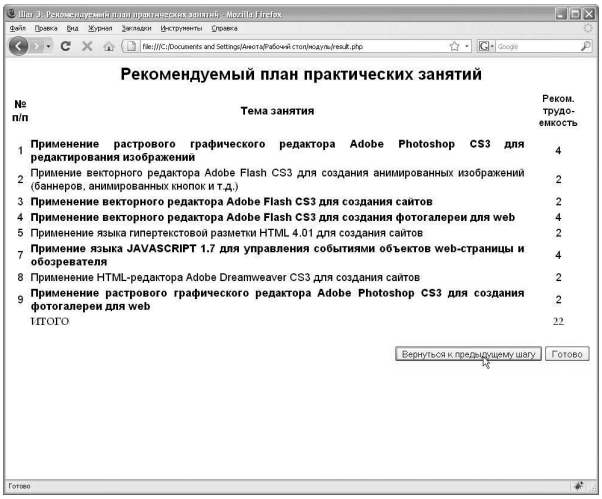


Рис. 5. Синтез образовательной траектории на основе план-графа

На рис. 6 приведен результат работы модуля.



Рекомендуемый план практических занятий

№ п/п	Тема занятия	Реком. трудо-емкость
1	**Применение растрового графического редактора Adobe Photoshop CS3 для редактирования изображений**	4
2	Применение векторного редактора Adobe Flash CS3 для создания анимированных изображений (баннеров, анимированных кнопок и т.д.)	2
3	**Применение векторного редактора Adobe Flash CS3 для создания сайтов**	2
4	**Применение векторного редактора Adobe Flash CS3 для создания фотогалереи для web**	4
5	Применение языка гипертекстовой разметки HTML 4.01 для создания сайтов	2
7	**Применение языка JAVASCRIPT 1.7 для управления событиями объектов web-страницы и обозревателя**	4
8	Применение HTML-редактора Adobe Dreamweaver CS3 для создания сайтов	2
9	**Применение растрового графического редактора Adobe Photoshop CS3 для создания фотогалереи для web**	2
	ИТОГО	22

Вернуться к предыдущему шагу | Готово

Рис. 6. Третий шаг работы модуля

Заключение

Таким образом, практикум с компетентностно-ориентированными структурой и содержанием должен быть разработан в соответствии с принципами модульности структуры, направленности и вариативности содержания. Для управления структурой практикума разработаны модели иерархии результатов обучения, позволившие выявить состояния образовательного процесса, и установить причинно-следственные связи между состояниями на основе разработанных содержательных компетенций для достижения ожидаемых элементарных результатов обучения. Результатом стала компетентностная модель образовательного процесса в виде план-графа, которая позволяет моделировать различные траектории образовательного процесса и определяет структуру практикума за счет отбора соответствующих базовых образовательных модулей, необходимых и достаточных для достижения ожидаемого результата обучения.

Литература

1. Лисицына Л.С. Средства и технологии для управления самостоятельной работой студентов. Методическое пособие. СПб: СПбГУ ИТМО. 2008. – 53 с.
2. Лисицына Л.С. Теория и практика компетентностного обучения и аттестаций на основе сетевых информационных систем. СПб: СПбГУ ИТМО. 2006. – 147 с.

УДК 004.855.5

ЭЛЕКТРОННЫЙ УМК ДЛЯ ФОРМИРОВАНИЯ ИКТ-КОМПЕТЕНТНОСТИ ПЕДАГОГОВ И ЕГО ВНЕДРЕНИЕ НА КУРСАХ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ ПЕДАГОГИЧЕСКИХ РАБОТНИКОВ СИСТЕМЫ ОБРАЗОВАНИЯ САНКТ-ПЕТЕРБУРГА

С.В. Мерзлякова
Научный руководитель – д.т.н., профессор Л.С. Лисицына

На основе проведенного анализа ИКТ были установлены объекты деятельности педагогов. Анализ видов деятельности педагогов по применению ИКТ в образовании позволил произвести декомпозицию исходного результата обучения и сформулировать три учебные задачи для решения которых было сформулировано тринадцать содержательных компетенций по формированию практических навыков применения ИКТ в образовательной деятельности педагогов. Для отбора компетентностно-ориентированного содержания был разработан дескриптор для начального, базового и углубленного уровней формирования содержательных компетенций, что позволило сформулировать тридцать четыре элементарных результата обучения. В соответствии с этими результатами обучения была проведена модернизация модели результатов образовательного процесса (план-графа) и содержания образовательных модулей Методического интернет-центра.

Ключевые слова: компетентностно-ориентированное содержание, содержательные компетенции, элементарный результат обучения, базовые образовательные модули, состояния образовательного процесса

Введение

Одним из направлений образовательной деятельности кафедры КОТ СПбГУ ИТМО является повышение квалификации педагогических работников в области ИКТ. За период с 2000г. по 2008 г. через краткосрочные курсы повышения квалификации кафедры прошло более 15 тысяч человек, в том числе 3 тыс. чел. в 2007 г., 2108 чел. в 2008 г. из числа педагогических работников Санкт-Петербурга по заказу Комитета по образованию.

Характерной особенностью предметной области обучения на курсах является ее изменчивость: ИКТ меняются каждый год, каждый год кафедра КОТ разрабатывает новое содержание образовательных программ для таких курсов. Кроме того, в рамках этой деятельности кафедра разработала сетевую информационную систему – Методический Интернет-центр (МИЦ) [2], в котором собраны и систематизированы образовательные модули с электронными учебно-методическими материалами для методической поддержки курсов повышения квалификации различных категорий работников образования в области ИКТ. Доступ к ресурсам МИЦ имеют в настоящее время образовательные учреждения (ОУ) высшего и дополнительного профессионально образования из 22 регионов РФ, в том числе более 40 тьюторских площадок нашего университета, созданных на базе ОУ системы образования Санкт-Петербурга. Все ОУ объединены в МИЦ в сетевое сообщество для ведения совместной научно-методической и образовательной деятельности по повышению квалификации педагогов в области ИКТ в своих регионах.

Основная часть

Особую важность имеет проблема ежегодной актуализации структуры и содержания образовательных модулей МИЦ, которыми пользуются преподаватели и тьюторы ОУ, в том числе при проведении курсов повышения квалификации в дистанционной форме. Поэтому появилась необходимость разработки электронного УМК с новым компетентностно-ориетированным содержанием и структурой, отражающих современ-

ное состояние ИКТ для формирования ИКТ-компетентности педагогов, а также его внедрения на курсах повышения квалификации педагогических работников системы образования Санкт-Петербурга в 2008 г. Для достижения этой цели были поставлены и решены следующие задачи:

- анализ отобранных ИКТ для применения в образовательной деятельности педагогов;
- детализация исходной компетенции педагогов «Применять информационные технологии в образовательной деятельности» и разработка полного перечня содержательных компетенций для ее формирования [2];
- разработка компетентностной модели образовательного процесса курсов;
- разработка структуры и содержания УМК для реализации компетентностной модели;
- загрузка электронного УМК в сетевую среду МИЦ.

В качестве исходной компетенции была сформулирована компетенция по формированию способности у педагога «Применять ИКТ в образовательной деятельности». На основе проведенного анализа и детализации видов деятельности педагогов были сформулированы следующие три компетенции (1-ый этап детализации), выражающих *необходимость формирования у педагогов способности*:

- «Применять информационные технологии для создания иллюстрационных и раздаточных материалов»;
- «Применять информационные технологии для создания электронных образовательных ресурсов»;
- «Использовать информационные технологии для организации сетевого общения».

На втором этапе детализации полученных компетенций разрабатывались содержательные компетенции, т.е. уточнялись те ИКТ, которые позволят педагогам освоить данные три вида деятельности. Данный этап завершился получением 13 содержательных компетенций, освоение которых планировалось на вводном, базовом и углубленном уровнях в соответствии с дескриптором уровней сформированности компетенции, используемым в МИЦ. Таким образом, для достижения результатов сформированности разработанных за два этапа детализации компетенций было установлено 34 различных состояний образовательного процесса, в том числе 5 новых состояний, которые еще не были описаны в МИЦ. Для идентификации результатов сформированности компетенций в этих 34 состояниях была проведена дальнейшая детализация компетенций (3-ий этап) и сформулировано 92 умения, которые должны сформировать практические навыки у педагогов по применению тех или иных ИКТ для создания иллюстрационных и раздаточных материалов к урокам, для создания электронных образовательных ресурсов и для организации сетевого общения.

Полученная надстойка в виде иерархии результатов формирования компетенций у педагогов (модель иерархии результатов приведена на рис. 1) определила модульную структуру разрабатываемого УМК. Таким образом, структура разрабатываемого УМК содержит 13 образовательных модулей, состоящих из 34 базовых образовательных модуля (БОМ) (по количеству различных состояний образовательного процесса).

Далее для отбора компетентностно-ориентированного содержания модулей была построена модель образовательного процесса, устанавливающая причинно-следственные связи между умениями его состояний. Такая модель или план-граф является ориентированным гиперграфом и служит компетентностной моделью для планирования целостного образовательного процесса курсов средствами автоматизации образовательных траекторий в МИЦ. В этой модели вершины модулируют состояния образовательного процесса, соответствующие результатам обучения, а дуги – траектории образовательного процесса, соответствующие БОМ.

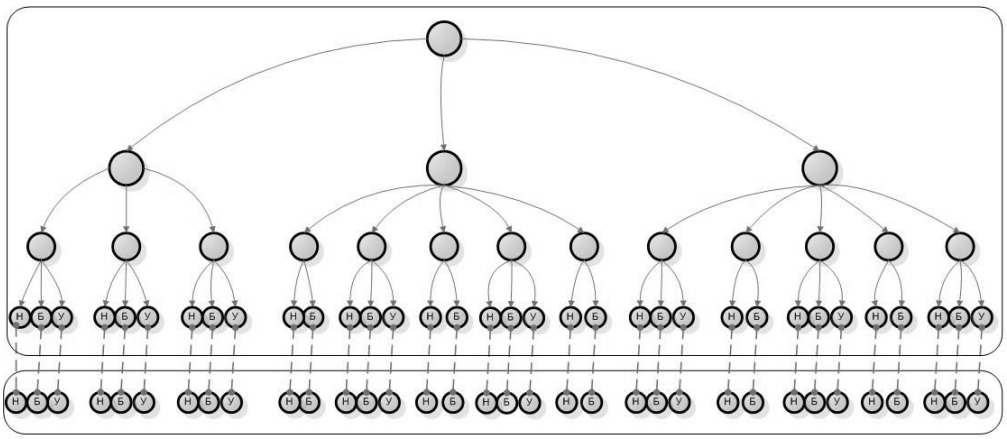


Рис. 1. Модель иерархии результатов формирования компетенций у педагогов

На рис. 2 приведен фрагмент план-графа МИЦ, который связан с выполненной работой. Здесь выделены состояния с индексами I.4-1.1 – I.7-3.2, I.8-1.1 – I.8-1.3, II.1-1.1 – II.1-3.3 и II.1-5.1 – II.1-5.2, в которых изменен состав умений, а, следовательно, модернизированы требования к содержанию БОМ, обеспечивающих достижение соответствующих состояниям результатов. Состояния с индексами I.7-5.1 – I.7-5.2 и I.8-2.1 – I.8-2.3 – новые состояния образовательного процесса, для достижения которых потребовалась разработка новых БОМ. Индексами II.1-4.1 – II.1-4.3 и II.1-8.1.1 – II.1-8.2.3 выделены состояния, для достижения которых требуется заменить или модернизировать содержание БОМ в перспективе. Другие состояния план-графа, присутствующие на рисунке не исследовались в работе в связи с тем, что они выходят за рамки поставленной задачи.

Содержание БОМ разрабатывалось по принципу необходимости и достаточности, т.е. в состав БОМ вошли учебно-методические материалы при изучении которых слушатель получит необходимый и достаточный объем знаний и пониманий, умений и навыков для формирования соответствующих компетенций. Материалы были подготовлены в форматах, использующихся для тиражирования в информационной среде МИЦ. Таким образом, для 34 БОМ было разработано 89 слайд-фильмов к лекционным занятиям, файлы подготовлены в формате *.PPT, 34 практикума, 7 практикумов для самостоятельной работы слушателей, файлы подготовлены в формате *.PDF, и наборы тестовых заданий для промежуточных аттестаций слушателей, файлы подготовлены в формате *.XML. Учебно-методические материалы разработанного электронного УМК были загружены в сетевую среду Методического интернет-центра посредством XML-транслятора. Для апробации электронного УМК на курсах повышения квалификации педагогических работников Санкт-Петербурга в 2008 г. мною в соавторстве с другими преподавателями кафедры были подготовлены два учебно-методических пособия:

1. Бобцов А.А., Мерзлякова С.В., Николаев Д.Г. Основы работы на персональном компьютере. Учебно-методическое пособие. – СПб.: СПбГУ ИТМО, 2008. 116 с. (тираж – 1200 экз.)
2. Мерзлякова С.В., Пирская А.С., Смирнова Е.В. Основы работы в сети Интернет. Учебно-методическое пособие. – СПб.: СПбГУ ИТМО, 2008. 120 с. (тираж – 300 экз.).

Данные пособия использовались при обучении полутора тысячах слушателей курсов повышения квалификации педагогических работников системы образования Санкт-Петербурга:

- 1114 человек прошли переподготовку по программе «Основы ИКТ для применения в образовательной деятельности»;
- 239 по программе «Интернет-технологии для сетевого преподавателя»;
- 170 по программе «Интернет-технологии для преподавателя предметника».

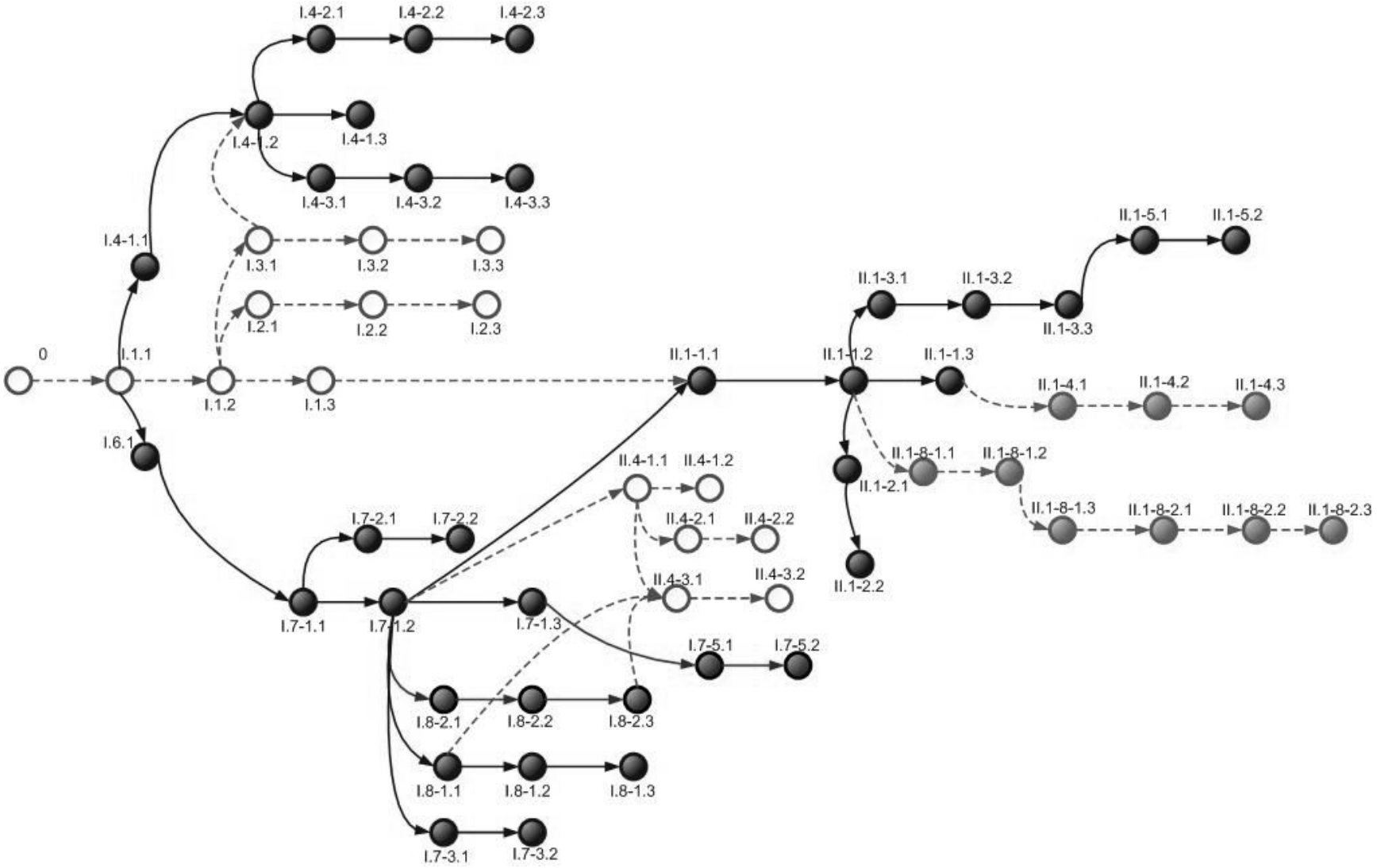


Рис. 2. Компетентностная модель образовательного процесса курсов

Заключение

В результате проведенной работы был разработан компетентностно-ориентированный электронный УМК, содержащий ресурсы в цифровых форматах для обеспечения таких видов нагрузки как лекции, практические занятия, самостоятельные занятия слушателей. Для контроля уровня освоения материала подготовлены наборы тестовых заданий. УМК имеет модульную структуру, разработанную на основе детализации исходной компетенции педагогов «Применять информационные технологии в образовательной деятельности», обеспечивает обучение и аттестацию слушателей курсов из числа педагогов системы общего образования. Разработанный УМК загружен в сетевую среду Методического интернет-центра, апробирован на курсах повышения квалификации педагогических работников системы образования Санкт-Петербурга в 2008 году.

Литература

1. Васильев В.Н., Лисицына Л.С., Лямин А.В. Методический интенет-центр. СПб: Питер, 2005. – 96 с.
2. Лисицына Л.С. Теория и практика компетентностного обучения и аттестаций на основе сетевых информационных систем. СПб: СПбГУ ИТМО, 2006. – 147 с.

УДК 004.4

ДЕКЛАРАТИВНОЕ ОБЪЯВЛЕНИЕ СЕРВИСОВ В ДИНАМИЧЕСКИХ КОМПОНЕНТНЫХ СИСТЕМАХ

П.Ю. Маврин
Научный руководитель – к.т.н., доцент Г.А. Корнеев

В статье рассмотрены подходы к реализации метода декларативного объявления сервисов в динамических компонентных системах. Предложены динамические версии алгоритмов работы с графом зависимостей компонент, часть из которых работает так же эффективно, как и в случае со статической системой.

Ключевые слова: компонентно-ориентированное программирование, компонентные системы

Введение

В последние годы большое развитие получило *компонентно-ориентированное программирование* [1] – парадигма программирования, в которой программа представляется как набор взаимодействующих *компонент*.

Каждая компонента может предоставить некоторые *сервисы* для использования другими компонентами. При этом, компоненты, использующие сервис, не знают, как он реализован. Другими словами, предоставляя сервис, компонента специфицирует то, **что** она делает, оставляя скрытым то, **как** она это делает.

В *динамических* компонентных системах компоненты могут запускаться и останавливаться независимо. То есть, в такой системе можно перезапустить некоторые компоненты, изменив их конфигурацию, при этом другие компоненты будут продолжать работу. Это удобно использовать в ответственных системах, которые нежелательно перезапускать целиком. При этом если выделить в отдельные компоненты части системы, выполняющие ответственную работу, то можно перезапустить второстепенную компоненту, не нарушая работу ответственной части системы. Наиболее известным стандартом для построения динамических компонентных систем является стандарт OSGi [2].

1. Ядро компонентной системы

Поскольку компоненты не связаны явно друг с другом (а лишь с сервисами), необходим дополнительный участник, обеспечивающий связывание компонент в единую систему. Этим участником будет *ядро компонентной системы*. Помимо связывания компонент ядро может выполнять множество дополнительных функций, как например ведение лога, отслеживание потоков компонент, определение ошибок в структуре зависимостей компонент (например, циклических зависимостей).

1.1. Декларативный и императивный способы объявления сервисов

Существует два основных способа передать ядру информацию о том, какие сервисы нужны компоненте для работы. Первый способ – императивный. Ядро предоставляет компонентам интерфейс, позволяющий им получить доступ к компоненте, предоставляющий нужный сервис, если такая компонента запущена. При этом активная роль принадлежит компонентам: они решают, в какой момент запросить нужный им сервис. Этот способ используется, например, в OSGi. Второй способ – декларативный. В этом случае ядро собирает информацию о связи компонент и сервисов еще **до запуска** компонент, чтобы иметь возможность запускать их в правильном порядке, обеспечивая их нужными сервисами. Паттерн проектирования для реализации этого способа называет-

ся Dependency Injection [3]. Декларативный способ объявления сервисов имеет ряд важных преимуществ по сравнению и с императивным способом.

(1) При использовании декларативного способа пропадает явная зависимость компонент от ядра.

(2) Компоненте не нужно заботиться о получении требуемых сервисов, все сервисы уже предоставлены ей в момент запуска.

(3) Ядро получает полную информацию о взаимосвязи компонент и сервисов. За счет этого оно может, например, обнаруживать тупиковые и циклические зависимости и сообщать о них администратору.

1.2. Типы сервисов

В данной работе мы будем предполагать, что существует два типа сервисов по отношению к компоненте, *предоставляемые* и *требуемые*. Рассмотрим каждый из типов подробнее.

Сервис предоставляется компонентой, если она содержит его реализацию и готова выполнять по нему запросы от других компонент. Будем называть предоставляемый сервис *активным*, если компонента, предоставляющая его, запущена.

Требуемый сервис – это сервис, без которого работа компоненты невозможна. Если у компоненты есть требуемые сервисы, они должны быть активны, когда работает эта компонента.

1.3. Типы компонент

Будем также считать, что каждой компоненте задан один из двух режимов запуска: *пассивный* или *инициативный*. Компоненты с инициативным режимом запуска обязательно должны быть запущены системой. Компоненты в пассивном режиме запускаются, только если это требуется для запуска инициативных компонент.

2. Статические компонентные системы с пассивными компонентами

Для облегчения понимания алгоритмов для динамических компонентных систем, сначала рассмотрим случай, когда система является статической, то есть нам заранее известен набор компонент, которые требуется запустить.

В этом разделе рассмотрены алгоритмы, используемые для обеспечения работы компонентной системы, а также нахождения ошибок в структуре зависимостей компонент.

Будем считать, что нам известен набор сервисов, предоставляемых и используемых каждой компонентой.

2.1. Граф зависимостей

Зависимости компонент и сервисов удобно представлять в виде графа. Вершины этого графа соответствуют компонентам и сервисам, а ребра — зависимостям между ними. Зависимости появляются: от компоненты к требуемым сервисам и от сервиса к предоставляющей его компоненте (см. рис. 1).

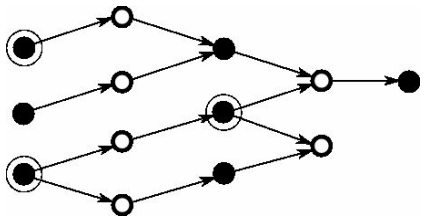


Рис. 1. Пример графа зависимостей. Заполненными кружками обозначены компоненты, пустыми – сервисы. В круги обведены компоненты с инициативным режимом запуска

2.2. Форсирование компонент и сервисов

Будем называть компоненту *форсированной*, если ее необходимо запустить, аналогично назовем сервис *форсированным*, если его необходимо активировать. Определим список форсированных компонент и сервисов. Это достаточно просто сделать, имея граф зависимостей. Достаточно найти все вершины графа зависимостей, до которых можно дойти от инициативных компонент. Это можно сделать, например, обходом в глубину [4]. На рис. 2 представлен результат работы алгоритма, форсированные вершины и сервисы обведены кружком.

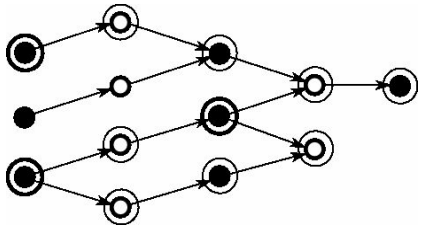


Рис. 2. Результат работы алгоритма поиска форсированных компонент и сервисов.

2.3. Обнаружение ошибок в структуре зависимостей

Если форсированный сервис не предоставляется никакой компонентой, то он не сможет быть активирован. Соответственно компоненты, зависящие от этого сервиса, не смогут запуститься. Чтобы найти список таких компонент можно воспользоваться поиском в глубину на графе, обратном графу зависимостей.

Если в графе зависимостей есть цикл, то компоненты, входящие в него никогда не смогут быть запущены. Для того чтобы найти все компоненты, лежащие на циклах, воспользуемся следующим соображением: если вершина лежит на цикле, то она также лежит на некотором фундаментальном цикле графа. Таким образом, выделив фундаментальные циклы и объединив множества вершин в них, получим искомое множество. С точки зрения администрирования компонентной системы может быть полезно вывести циклы зависимых компонент в явном виде.

3. Динамические компонентные системы

Главное отличие динамических компонентных систем с точки зрения построения алгоритмов состоит в том, что граф зависимостей меняется со временем. Рассмотрим основные события в компонентной системе, ведущие к изменению графа зависимостей.

(1) Добавление компоненты. При этом в граф добавляется несколько вершин (компонента и ее сервисы), а так же несколько ребер (по одному на каждый сервис).

(2) Удаление компоненты. При этом происходит обратный процесс: удаляется несколько вершин и ребер.

Отметим, что если считать, степени вершин в графе зависимостей (то есть, количество сервисов, ассоциированных с компонентой, и количество компонент, ассоциированных с сервисом) ограничены некоторой константой k, то за одно действие добавления или удаления компоненты в граф добавляется или удаляется не более $(k+1)$ вершины и не более k ребер.

Задача в связи с динамичностью также несколько модифицируется. Требуется запускать и останавливать компоненты так, чтобы в каждый момент времени требуемые сервисы запущенной компоненты были активны. При этом потребуем, чтобы компонента запускалась сразу, как только все требуемые сервисы стали активны, и останавливалась только тогда, когда требуемый сервис нужно деактивировать.

3.1. Структура данных

Для того чтобы быстрее обрабатывать события, будем хранить дополнительную информацию о компонентах и сервисах. А именно для каждой компоненты u будем хранить количество неактивных требуемых сервисов $p[u]$. Таким образом, компонента может работать тогда и только тогда, когда $p[u] = 0$.

В этом разделе будем считать, что все компоненты запускаются инициативно.

3.2. Добавление компоненты

Опишем алгоритм добавления компоненты на псевдоязыке программирования. Добавление компоненты описано в процедуре `Добавить(u)`, которая использует процедуру `Запустить(u)` для рекурсивного запуска компонент.

```
01    Процедура Запустить(u) {
02        Запустить компоненту u.
03        Для каждого сервиса s, предоставляемого u:
04            Для каждой компоненты w, требующей s:
05                Уменьшить p[w] на один.
06                Если p[w] = 0, то Запустить(w).
07    }
08
09    Процедура Добавить(u) {
10        Обновить граф зависимостей.
11        Посчитать значение p[u].
12        Если p[u] = 0, то Запустить(u).
13    }
```

Несложно видеть, что представленный алгоритм запускает все компоненты, для которых все требуемые сервисы активны и только их. Действительно, значение $p[u]$ может стать равным нулю только в двух случаях: сразу при добавлении компоненты (строка 11) или при активации требуемого сервиса (строка 5).

Проанализируем время работы данного алгоритма. Рекурсивная процедура `Добавить(u)` (строка 1) выполняет порядка k^2 действий, при этом запускается новая компонента. Таким образом, время работы алгоритма линейно зависит от числа компонент, которые требуется запустить.

3.3. Удаление компоненты

Алгоритм добавления компоненты пишется почти аналогично, за исключением того, что компоненты, зависящие от останавливаемой компоненты нужно остановить **до** нее.

```
01    Процедура Остановить(u) {
02        Для каждого сервиса s, предоставляемого u:
03            Для каждой компоненты w, требующей s:
04                Увеличить p[w] на один.
05                Если компонента w запущена, то Остановить(w).
06        Остановить компоненту u.
07    }
08
09    Процедура Удалить(u) {
10        Если компонента u запущена, то Остановить(u).
11        Обновить граф зависимостей.
12    }
```

Так же, как и для добавления компоненты, несложно показать, что время работы алгоритма удаления компоненты линейно зависит от числа компонент, которые нужно остановить.

3.4. Обнаружение ошибок в структуре зависимостей

Легко заметить, что если в системе нет ни тупиковых, ни циклических зависимостей, то все компоненты можно запустить. Поэтому если запущены не все компоненты, это автоматически свидетельствует о том, что в структуре зависимостей есть ошибки.

Более сложный вопрос — какая именно ошибка в структуре зависимостей мешает запуску. Тупиковые сервисы обнаружить довольно легко. Достаточно хранить число требуемых сервисов, не предоставляемых ни одной компонентой. Если же таких сервисов нет, а компоненты запущены не все, то в графе зависимостей есть цикл.

К сожалению, не известно способа обнаружить цикл в изменяющемся графе быстрее, чем за обход графа. С другой стороны, можно считать, что циклические зависимости не являются нормальной ситуацией в компонентной системе и происходят нечасто. Поэтому можно иногда проверять граф зависимостей на наличие циклов (для этого придется обойти его целиком) и, если цикл обнаружится, сообщать об этом администратору.

4. Динамические компонентные системы с пассивными компонентами

Решение задачи форсирования сервисов в динамической компонентной системе связано с определенными трудностями. Дело в том, что при добавлении или удалении активной компоненты может понадобиться обойти весь граф, чтобы пометить форсированные компоненты. Приведем соответствующие алгоритмы.

4.1. Структура данных

Для каждой компоненты u будем хранить число $f[u]$. Для пассивных компонент $f[u]$ будет равно количеству форсированных предоставляемых сервисов, а для инициативных – тому же числу плюс один. Таким образом, компонента форсирована тогда и только тогда, когда $f[u] > 0$.

4.2. Добавление компоненты

Добавление компоненты описано в процедуре `Добавить(u)`, которая использует процедуры `Запустить(u)` и `Форсировать(u)` для рекурсивного запуска и форсирования компонент.

```
01    Процедура Запустить(u) {
02        Запустить компоненту u.
03        Для каждого сервиса s, предоставляемого u:
04            Для каждой компоненты w, требующей s:
05                Уменьшить p[w] на один.
06                Если p[w] = 0 и f[w] > 0, то Запустить(w).
07    }
08
09    Процедура Форсировать(u) {
10        Для каждого сервиса s, требуемого u:
11            Для каждой компоненты w, предоставляющей s:
12                Увеличить f[w] на один.
13                Если f[w] = 1, то Форсировать(w).
14    }
15
16    Процедура Добавить(u) {
17        Обновить граф зависимостей.
18        Посчитать значения p[u] и f[u].
19        Если f[u] > 0, то Форсировать(u).
20        Если p[u] = 0 и (f[u] > 0), то Запустить(u).
21    }
```

Проведем анализ времени работы предложенного алгоритма. Процедура `Запустить(u)`, как и раньше, работает за время, линейно зависящее от числа вновь запущенных компонент. Аналогичный анализ для рекурсивной процедуры

Форсировать(*u*) показывает, что время ее работы линейно зависит от числа компонент, ставших форсированными.

Таким образом, алгоритм добавления компоненты работает за время, линейно зависящее от числа компонент, на которые повлияло это добавление.

4.3. Удаление компоненты

Удаление компоненты описано в процедуре Удалить(*u*), которая использует процедуры Остановить(*u*) и Восстановить(*u*) для рекурсивной остановки и восстановления (снятия форсированности) компонент.

```
01    Процедура Остановить(u) {
02        Для каждого сервиса s, предоставляемого u:
03            Для каждой компоненты w, требующей s:
04                Увеличить p[w] на один.
05                Если компонента w запущена, то Остановить(w).
06        Остановить компоненту u.
07    }
08
09    Процедура Восстановить(u) {
10        Для каждого сервиса s, требуемого u:
11            Для каждой компоненты w, предоставляющей s:
12                Уменьшить f[w] на один.
13                Если f[w] = 0, то Восстановить(w).
14    }
15
16    Процедура Добавить(u) {
17        Если компонента u запущена, то Остановить(u).
18        Если f[u] > 0 то Восстановить(u).
19        Обновить граф зависимостей.
20    }
```

Аналогичный анализ показывает, что данный алгоритм работает за время, линейно зависящее от количества остановленных компонент плюс компонент, ставших неформированными.

4.4. Вывод

Механизм пассивных и инициативных компонент является достаточно удобным инструментом для автоматического запуска компонент «по требованию», однако его реализация в динамических компонентных системах из-за меняющейся структуры графа зависимостей, приводит к дополнительным затратам по времени работы.

Заключение

В данной работе предложен подход к реализации метода декларативного объявления сервисов в динамических компонентных системах. Были предложены динамические версии алгоритмов работы с графом зависимостей компонент, часть из которых работает так же эффективно, как и в случае со статической системой (алгоритмы запуска и остановки компонент), другая же часть требует дополнительных затрат времени (алгоритм определения циклических зависимостей, форсирования компонент).

Литература

1. Непейвода Н.Н. Стили и методы программирования. – М.: ИНТУИТ.ру. 2005. – 320 с.
2. OSGi Alliance. OSGi Service Platform. – IOS Press, 2003, 604 с. Яз. англ.
3. Martin Fowler [Электронный ресурс] – Режим доступа: http://martinfowler.com/articles/injection.html, свободный. – Загл. с экрана. – Яз. англ.
4. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: Построение и Анализ. – М.: МЦНМО. – 1999. – 960 с.

УДК 004.4.24

ПРИМЕНЕНИЕ АВТОМАТНОГО ПРОГРАММИРОВАНИЯ ДЛЯ ПОСТРОЕНИЯ СИСТЕМ УПРАВЛЕНИЯ БИЗНЕС-ПРОЦЕССАМИ

Е.А. Мандриков, В.А. Кулев
Научный руководитель – д.т.н., профессор А.А. Шалыто

В данной статье рассматривается задача консолидации языков описания бизнес-процессов в единой системе управления. Будет показано, что в основе предлагаемой системы целесообразно использовать автоматные программы.
Ключевые слова: автоматизация, бизнес-процессы, конечные автоматы

Введение

Основной задачей систем управления бизнес-процессами является автоматизация процессов, проходящих в бизнесе [1]. При построении программных продуктов, работающих с бизнес-процессами, можно выделить три основные роли: конечный пользователь системы, бизнес-аналитик и разработчик. Бизнес-аналитик изучает и описывает бизнес-процесс и формулирует требования к программному обеспечению, а разработчик реализует их в конечном продукте.

Традиционные системы управления бизнес-процессами пытаются отталкиваться от модели, построенной бизнес-аналитиком, и строить на основании нее исполняемую программу. Такой способ автоматизации бизнес-процессов постепенно вынужден отходить на второй план ввиду того, что внесение даже небольших изменений в схему процесса означает необходимость перепрограммирования и большие затраты времени и средств. В результате прикладные программы не успевают обновляться в том темпе, который диктуют изменяющиеся условия бизнеса и потребности самого предприятия [2]. Также следует отметить, что разработанные таким способом программные продукты жестко привязаны к конкретным бизнес-процессам и конечному потребителю, что не позволяет осуществлять их быстрое внедрение на других предприятиях.

На смену традиционному способу автоматизации бизнес-процессов приходят различные предметно-ориентированные языки программирования (*DSL – Domain-Specific Language*) [3], предназначенные для описания специфичных видов бизнес-процессов, таких как: управление задачами (*Issue Tracking*, *Bug Tracking*) [4], управление документооборотом (*Document Management System*) [5] и т.д. При использовании данного подхода бизнес-аналитик и разработчик общаются на одном языке с графическим представлением процесса. Бизнес-аналитик ответственен за графическое представление и не должен разбираться с техническими деталями процесса. Но без этих деталей бизнес-процесс не будет полностью определен и следственно не сможет быть выполнен, поэтому разработчик ответственен за их программную реализацию.

Большинство существующих программных продуктов позволяют использовать только один или несколько языков описания бизнес-процессов. Это затрудняет интеграцию различных бизнес-процессов, происходящих на одном предприятии, и вынуждает разработчиков проделывать дополнительную работу. В данной статье рассматривается подход к решению этой проблемы путем трансляции описаний бизнес-процессов в автоматные программы [6].

Языки описания бизнес-процессов

BPEL – язык описания бизнес-процессов, созданный для работы в среде веб-сервисов [7]. Он построен на базе WSDL, и хотя WSDL позволяет использование JavaBeans, более естественным вариантом для него являются веб-сервисы.

Разворачивание бизнес-процесса в BPEL приводит к публикации веб-сервиса, который является основным средством взаимодействия с процессом. Переменные внутри BPEL являются фрагментами XML или базовыми типами XSD. BPEL имеет конструкции для описания управляющей логики и вызова других WSDL сервисов. В конечном итоге BPEL – язык для описания бизнес-процессов управления веб-сервисами.

Другим популярным языком является jPDL, созданный в рамках проекта JBoss jBPM [8]. Одним из его основных предназначений является управление задачами. Для этого в языке предусмотрены специальные конструкции для создания задач. Изменения, происходящие в задачах (такие как начало или конец выполнения), также являются управляющими событиями бизнес-процесса. Язык jPDL поддерживает асинхронное исполнение задач и ветвление бизнес-процесса на несколько параллельных.

На примере BPEL и jBPM видно, что существование предметно-ориентированных языков описания бизнес-процессов оправдано широким спектром задач, с которыми приходится сталкиваться при автоматизации предприятий. Однако легко заметить, что у этих языков есть множество общих черт, в частности представление модели бизнес-процесса в виде графа.

Трансляция описаний бизнес-процессов в автоматную программу

Предлагаемый подход заключается в трансляции описаний бизнес-процессов в системы взаимодействующих автоматов. Автоматы могут взаимодействовать:

- по вложенности – один автомат вложен в одно или несколько состояний другого автомата;
- по вызываемости – один автомат вызывается с определенным событием из выходного воздействия, формируемого при переходе другого автомата;
- по обмену сообщениями – один автомат получает сообщения от другого;
- по состояниям – один автомат проверяет, в каком состоянии находится другой автомат.

На рис. 1 приведен пример описания простейшего процесса на языке jPDL. На данном примере покажем, как можно осуществлять трансляцию в автоматную программу.

Рис. 1. Пример описания бизнес-процесса на языке jPDL

В данном примере *task node* транслируется во вложенный автомат, управляющий внутренним состоянием задачи. Полученная автоматная программа приведена на рис. 2.

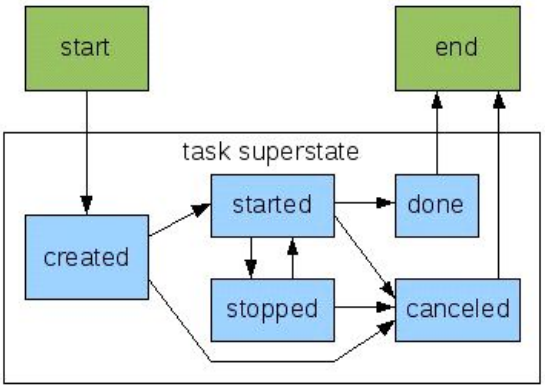


Рис. 2. Пример полученной автоматной программы

Аналогичным образом можно транслировать в автоматные программы и все другие высокоуровневые конструкции языков описания бизнес-процессов. Получаемые при этом автоматные программы могут быть исполнены в единой для всех процессов среде (*Process Virtual Machine*), либо транслированы в исполняемый код.

Заключение

Среди плюсов предлагаемого подхода можно выделить:

- возможность использования бизнес-аналитиком привычных для него средств моделирования бизнес-процессов;
- легкость интеграции различных языков описания бизнес-процессов в единой системе;
- расширяемость системы благодаря возможности добавления новых языков;
- возможность верификации бизнес-процессов (фактически верификация полученной автоматной программы [9]).

Литература

1. http://en.wikipedia.org/wiki/Business_process_management
2. Применение конечных автоматов в документообороте В.О. Клебан, Ф.А. Новиков // Научно-технический вестник СПбГУ ИТМО. Выпуск 53. Автоматное программирование. – С. 286–294.
3. http://en.wikipedia.org/wiki/Domain-specific_programming_language
4. http://en.wikipedia.org/wiki/Issue_tracking_system
5. http://en.wikipedia.org/wiki/Document_management_system
6. Сайт по автоматному программированию и мотивации к творчеству http://is.ifmo.ru/
7. Business Process Execution Language – http://en.wikipedia.org/wiki/BPEL
8. http://www.jboss.com/products/jbpm/
9. Верификация программ, построенных на основе автоматного подхода Е.А. Курбацкий, А.А. Шалыто / Сборник докладов XV Международной научно-методической конференции «Высокие интеллектуальные технологии и инновации в образовании и науке». СПбГПУ. 2008. – С. 293–296. http://is.ifmo.ru/download/2008-02-25_politech_verification_kurb.pdf

УДК: 004.932

ИСПОЛЬЗОВАНИЕ GPGPU ДЛЯ УСКОРЕНИЯ ПРОЦЕССА ПОСТРОЕНИЯ КАРТ ДИСПАРАТНОСТИ

А.Н. Волкович
(Объединенный институт проблем информатики НАН Беларуси)
Научный руководитель – д.ф.-м.н., профессор А.В. Тузиков
(Объединенный институт проблем информатики НАН Беларуси)

Работа исследует процедуры автоматического восстановления трехмерной модели объектов по стереоизображениям. Описываются алгоритмы построения карт диспаратности, обсуждаются подходы к их параллельной реализации и приводятся результаты вычислительного эксперимента по сравнению эффективности выполнения последовательной и параллельной реализаций алгоритма.
Ключевые слова: обработка изображений, стерео изображения, трехмерная модель, системы наблюдения

Введение

Построение объемной модели на основе стерео изображений традиционно была, и остается одним из наиболее актуальных направлений в развитии компьютерного зрения. Последние исследования в этой области значительно продвинули область знания в вопросах качества и адекватности построений. К сожалению, на современном этапе исследований требования к производительности значительно превышают возможности элементной базы – алгоритмы стереовосстановления обычно требуют от нескольких секунд до нескольких минут машинного времени, для построения единственной карты диспаратности. Однако существует значительное количество актуальных приложений, таких как задачи навигации и виртуальной реальности, которые требуют построения карт диспаратности с частотой близкой или эквивалентной стандартному видео. Кроме того обработка больших изображений (таких как аэрофотоснимки и т.п.) существующими методами требуют неприемлемо больших временных затрат.

Подготовка изображений

Входной информацией для алгоритма определения множества сопряжённых точек на паре изображений служат лишь сами изображения. На начальном этапе работы алгоритма выделяются множества точек на изображениях, среди которых находятся предполагаемые соответствия путём сравнения их окрестностей.

Сопряженные точки могут задаваться вручную или отыскиваться автоматически при помощи алгоритма автоматического нахождения сопряжённых точек [5].

Выравнивание изображений позволяет получить более простую эпиполярную геометрию в том смысле, что фундаментальная матрица для преобразованных изображений имеет вид:

$$F = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}$$

Для выполнения выравнивания пары изображений к каждому изображению применяется специальное проективное преобразование. Проективные преобразования выбираются так, чтобы соответствующие эпиполярные линии были параллельны оси x. В качестве выравнивающего преобразования можно использовать преобразование, которое переносит эпиполюс z в бесконечно удалённую точку. При этом преобразование

определяется не однозначно, чем можно воспользоваться для уменьшения внесённых проективных искажений. В результате получим, что сопряжённые точки на изображениях будут иметь кроме равных у координат также и близкие значения x-координат [1].

Построение плотной карты диспаратности

Методы построения плотной карты диспаратности можно разделить на две группы: локальные методы, которые работают с небольшими окрестностями точек для нахождения соответствий (например, блочный метод), и глобальные, которые работают со строками изображения (динамическое программирование) или с изображением целиком (метод максимального потока в графе). Локальные методы могут быть достаточно эффективны, однако они чувствительны к локально-неоднозначным регионам (например, регионам с однородной текстурой). Глобальные методы менее чувствительны к таким регионам, однако они более ресурсоёмки.

Простейший локальный алгоритм – блочный алгоритм. Он определяет диспаратность, сравнивая небольшой регион (блок) вокруг точки первого изображения с последовательностью таких же регионов на втором изображении в некоторой области поиска [6].

Существует также алгоритм, использующий динамическое программирование для построения плотной карты диспаратности. Этот алгоритм работает с парами соответствующих строк на изображении, рассматривая их независимо от остальных строк, в результате чего на карте диспаратности могут появиться характерные горизонтальные штрихи [7].

Третий подход к построению карты диспаратности состоит в сведении задачи к нахождению максимального потока в графе. В построенном специальным образом графе находится минимальный разрез, который и определяет искомые значения диспаратности [8].

Реконструкция трехмерной модели

В общем случае процесс реконструкции по множеству пар сопряжённых точек можно описать следующими шагами:

- вычисление фундаментальной матрицы;
- вычисление матрицы камер по фундаментальной матрице;
- вычисление точки в пространстве, изображением которой эти точки являются.

Когда для реконструкции используются только лишь изображения, возникает неоднозначность реконструкции: пространственные координаты могут быть определены лишь с точностью до проективного преобразования.

Таким образом, без какой-либо информации о параметрах камер и реконструируемого объекта можно выполнить реконструкцию с точностью до проективного преобразования. Используя дополнительную информацию можно сократить неоднозначность [1].

Использование параллельных систем с целью увеличения эффективности методов обработки

Сегодня достигнут предел увеличения вычислительной мощности одноядерных вычислительных процессоров, базирующийся на увеличении тактовой частоты и архитектурных инновациях. Для решения данных задач требуется концентрация вычислительных мощностей, а так же решение задач оптимизации вычислений. Ведущие изго-

товители микроэлектронных компонентов для сохранения тенденций роста производительности, переходят на разработку многоядерных процессоров с новой архитектурой, обеспечивающих распараллеливание обработки данных. Появление многоядерных процессоров является качественным скачком на пути создания эффективных супервычислителей, обладающих существенно более высокими показателями производительность/ стоимость, по сравнению с существующими высокопроизводительными системами вычислений на базе суперЭВМ и кластерных систем. Использование многоядерных процессоров предоставляет гибкие возможности в части варьирования конфигураций и масштабирования мощности вычислительных систем от персональных компьютеров, рабочих станций, серверов до кластерных систем.

Идея распараллеливания вычислений базируется на том, что большинство задач может быть разделено на набор меньших задач, которые могут быть решены одновременно.

Производя декомпозиционный анализ процесса построения объемных моделей на основе стерео изображений, оптимальным для параллельной реализации определен этап построения плотной карты диспаратности. Данный этап представляет собой совокупность однотипных опреаций по сравнению областей изображений и/или строк. Данный шаг возможно разделить на независимые блоки, которые будут обрабатываться в различных вычислительных узлах.

Построение карт диспаратности на «классических» параллельных системах

Используя особые точки на изображении (такие как угловые точки), можно с целью определения целесообразности использования параллельных методов были проведены тестовые сравнения процесса построения плотных карт диспаратности в параллельном и последовательном режимах на многоядерных вычислительных системах.

Для проведения эксперимента производилась обработка двух пар изображений: стереоизображения реальной местности; калибровочная стереопара (тестовая пара стереоизображений куба в сфере).

Для получения информации об отношении скорости расчетов в последовательном и параллельном режимах произведено измерение времени выполнения последовательно реализованного алгоритма, а затем и параллельно реализованной версии. С целью получения наиболее объективных данных проведено десять замеров и вычислено среднее значение скорости выполнения.

Эксперименты показали, что параллельная реализация алгоритма позволяет увеличить его производительность на двуядерных или двуконвеерных системах на 30–40% по сравнению с их последовательной реализацией. Однако двуядерная архитектура не позволяет достичь скорость обработки близкой к частоте видео. Таким образом, возникает необходимость использования более сложных параллельных вычислительных систем, главным недостатком которых являются: чрезвычайно высокая стоимость; сложность инфраструктуры; большие потери на межузловой коммуникации и громоздкость системы.

Высокопроизводительные вычислительные системы на базе GPU

На современном этапе в качестве альтернативы могут выступать системы использующие графические процессоры в качестве высокопроизводительных вычислителей. Изначально GPU не могли использоваться для вычислений. Однако рост требований представляемых перед графическими ускорителями стал толчком в увеличению производительности и совершенствованию архитектуры.

В последнее время, в ходе своего развития, программируемые графические процессоры превратились в полноценную вычислительную единицу. Обладая многоядерной архитектурой и высокопропускной памятью, современные GPU представляют высокопроизводительные ресурсы и для графической и для неграфической обработки.

Процессор типа G80 (NVidia GeForce 8800) является многоядерным и многопоточным высокопроизводительным микропроцессором. По своим функциональным характеристикам и вычислительной мощности он может рассматриваться как графический процессор и как универсальный процессор для эффективной реализации неграфических приложений, требующих интенсивных вычислений. Как графический процессор он полностью реализует функции классического графического конвейера, устраняя недостатки предшествующих моделей GPU. Как универсальный процессор на операциях с плавающей точкой он превосходит по критерию производительность-стоимость все существующие традиционные и многоядерным CPU и GPU. Базовыми инновациями G80 являются:

- унифицированная архитектура массива ядерных потоковых процессоров с плавающей точкой. пригодных для исполнения как графических конвейерных операций (геометрических преобразований,
- обработки вершин и пикселов), реализуемых единообразно на потоковых процессорах, так и неграфических вычислений;
- технология NVIDIA GigaThread Technology, широкомасштабная многопоточная архитектура, поддерживающая исполнение тысячи независимых, параллельно исполняемых тредов(потоков команд), обеспечивающая высокую эффективность обработки потоковых данных и использования вычислительного потенциала нового поколения многоядерных GPU. Для сравнения современные многоядерные CPU поддерживают работу на порядок и даже на два порядка меньше количества нитей.

При реализации на G80 неграфических вычислений наиболее значимыми компонентами являются массив унифицированных потоковых процессоров, доступные им ресурсы памяти, коммуникационные и управляющие средства.

Разделяемые ресурсы памяти внутри кластеров позволяют обеспечить синхронизацию и коммуникацию между нитями (потоками команд), работающими внутри кластера. G80 обладает мощной параллельной архитектурой. Каждый потоковый процессор, на основе механизмов управления работой нитей, способен динамически переназначаться для исполнения конвейерных графических или других вычислительных операций, обеспечивая, таким образом, пиковую загрузку ресурсов GPU и максимальную сбалансированную гибкость при обработке задач.

Тенденция роста вычислительной мощности GPU, проиллюстрированная на рисунке позволяет говорить о возможности использования систем для больших вычислений. В мировой практике уже существуют прецеденты использования вычислений на GPU, а также попытки сравнения с эффективностью фактических вычислений на CPU. Так Исследователи в Антверпенском университете (Бельгия) создан высокопроизводительный компьютер на базе четырех видеокарт NVIDIA GeForce 9800 GX2 (8 GPU). По результатам сравнения вычислительных мощностей объявлено его вычислительная эквивалентность кластеру из 300 ПК с Intel Core 2 Duo 2.4GHz.

Использование GPU для построения карт диспаратности

На сегодняшний день в мировой практике были предприняты попытки реализации алгоритмов построения карт диспаратности на GPU. Исследователями был реализован алгоритм динамического программирования с коррекцией карты за счет второго про-

хода. В свою очередь пред и пост обработки производились на центральном процессоре с тактовой частотой 3 GHz.

Данный алгоритм был выбран по причине его хорошей распараллеливаемости в отличие от глобальных алгоритмов и одновременной возможности получения удовлетворительных результатов. Результаты работы показывают возможность построения 16 уровневой карты диспаратности для рисунка 320×240 точек с частотой 42 кадра в секунду (0.023 секунды на обработку одного кадра).

Также было произведено сравнение вычислений карт диспаратности по указанному алгоритму для изображений различного разрешения и с различным количеством уровней:

Размер	Уровней	GPU	CPU
640×480	16	0.079	15.2
	32	0.131	29.1
	48	0.183	42.4
320×240	16	0.023	3.61
	32	0.042	6.78
	48	0.054	9.63

Таблица 1. Сравнительные характеристики вычислений диспаратности на CPU и GPU

Базируясь на приведенных данных возможно предположить, что использование одного GPU для построения карты диспаратности изображений SD-разрешения (720×576) позволит достичь частоты около восьми кадров в секунду, а HD-разрешения (1920×1080) порядка одного.

Заключение

Анализируя вычислительные мощности графических ускорителей заявляемые производителями, базируясь на имеющихся в мировой практике опытах использования GPU в качестве высокопроизводительных систем, а также на заявляемой возможности использования нескольких GPU-вычислителей, возможно создать систему оперативного восстановления объемных моделей на основе стереизображений. Текущая производительность GPU-систем и возможность использования нескольких ускорителей в одной системе позволяют судить о возможности достичь скорость обработки близкую или эквивалентную частоте стандартного видео для изображений SDTV и HDTV разрешений.

Кроме того использование GPU-вычислений позволит ускорить построение карт диспаратности при помощи алгоритмов, которые не предполагают быстрого выполнения, но обладают, на современном этапе критически долгое выполнение, затрудняющее их использование.

В свою очередь значительно меньшая стоимость оборудования, простота монтажа, а также компактность размещения позволит использовать данные системы в качестве программно-аппаратных комплексов стереовидения.

Литература

1. Hartley R., Zisserman A. Multiple View Geometry in Computer Vision. – Cambridge University Press, 2001. – 624 p.
2. Fougeras O., Luong Q.-T. The Geometry of Multiple Images. – The MIT Press. – 2001. – 646 p.

3. Scharstein D., Szeliski R. A taxonomy and evaluation of dense two-frame stereo correspondence algorithms // International Journal of Computer Vision. – 2002. – Vol. 47. – № 1–3. – P. 7–42.
4. Тузиков А.В., Шейнин С.А, Жук Д.В. Математическая морфология, моменты, стереобработка: избранные вопросы обработки и анализа цифровых изображений. Минск, Белорус. наука. – 2006. – 198 с.
5. Borodach A, Tuzikov A. Automatic determination of matching points on two images. Proceedings of the 9th International Conference “Pattern Recognition and Information Processing”, 22–24 May, 2007, Minsk, Belarus. – Vol. 1. – PP. 49–53.
6. Жук Д.В., Тузиков А.В. Реконструкции трехмерной модели по цифровым изображениям. // Информатика. – 2006. – № 1. – С. 16–26.
7. Hartley R. Theory and Practice of Projective Rectification // International Journal of Computer Vision. – 1999. – 35(2). – PP. 115–127.
8. Pollefeys M., Koch R., Van Gool L. A simple and efficient rectification method for general motion // Proc. International Conference on Computer Vision (Corfu, Greece). – 1999. – PP. 496–501.
9. Christopher Zach, David Gallup, Jan-Michael Frahm. Fast Gain-Adaptive KLT Tracking on the GPU . University of North Carolina Chapel Hill, NC. – 2008. – 7 p.
10. Liang Wang, Miao Liao, Minglun Gong, Ruigang Yang, David Nister. High-quality Real-time Stereo using Adaptive Cost Aggregation and Dynamic Programming. Abstracts of University of Kentucky. – 2008. – 8 p.
11. NVIDIA CUDA Homepage. http://www.nvidia.ru/object/cuda.html
12. Воробьев А., Медведев А. NVIDIA GeForce 8800 GTX (G80). http://www.ixbt.com/video2/g80-part1.shtml
13. Аляутдинов М.А., Троепольская Г.В. Использование современных многоядерных процессоров в нейрокомпьютерах для решения задач математической физики Нейрокомпьютеры: разработка, применение. – № 9. – 2007. – С/ 71–80.
14. A.N. Volkovich, D.V. Zhuk, A.V. Tuzikov. Construction of three-dimensional models from images using parallel systems. Proceedings of the 9th International Conference “Pattern Recognition and Information Processing”, 22–24 May, 2007, Minsk, Belarus. – Vol. 2. – PP. 232–235.
15. Волкович А.Н., Жук Д.В., Тузиков А.В. Методы построения трехмерных моделей местности и их реализация для параллельных систем. Доклады 5-й международной конференции "Обработка информации и управление в чрезвычайных и экстремальных ситуациях", 24–26 октября, Минск, Беларусь. – 2006. – С. 100–104.

УДК 535

МОДЕЛИРОВАНИЕ ОПТИЧЕСКИХ СВОЙСТВ МЕТАЛЛ-ДИЭЛЕКТРИЧЕСКИХ ДВУМЕРНЫХ СВЕРХРЕШЕТОК

Г.А. Кичин
(Московский физико-технический институт (государственный университет)),
T. Odom, J. Henzie, H. Gao (Northwestern University, Evanston, Illinois, USA),
T. Weiss, H. Gissen (4th Physics Institute, University of Stuttgart, Germany)
Научный руководитель – д.ф.-м.н., профессор С.Г. Тиходеев
(Институт общей физики РАН)

В работе обсуждаются оптические свойства металл-диэлектрических полупроводниковых наноструктур. Исходный образец – периодическия слоистая структура – был произведен методом мягкой литографии (soft lithography method). Численные расчеты проводились с применением метода матрицы рассеяния. Наблюдаемые на спектре аномалии были также обсчитаны теоретически.
Ключевые слова: наноструктура, фотонный кристалл, сверхрешетка, плазмон

Введение

В настоящее время особый интерес представляет область физики, связанная с созданием метаматериалов и изучением их свойств. Метаматериалы – это в основном метал-диэлектрические фотонно-кристаллические структуры, обладающие трансляционной сим-метрией и имеющие периодичность меньше длины волны. Новейшие методы литографии позволяют выращивать структуры этого типа. Задавая параметры такой структуры, можно контролировать ее оптические свойства. Добавочное структурирование фотонного кристалла в сверхрешетку со сложной элементарной ячейкой дает дополнительную возможность управлять оптическими свойствами. В случае использования металло-диэлектрических структур возникают дополнительно плазмонные резонансы, возбуждения коллективных колебаний электронов проводимости в металле. Плазмонные резонансы возможны двух типов: локализованные и делокализованные (поверхностные плазмоны). Каждый резонанс по-своему влияет на свойства структуры.

Основная часть

Существующие в настоящее время вычислительные методы описания оптических свойств метаматериалов требуют чрезвычайно больших компьютерных ресурсов. Компьютерное моделирование не дает хороших результатов в случае двумерных и сложных одномерных сверхрешеток. Поэтому важным является создание упрощенных моделей, которые позволяют дать качественное объяснение физических процессов, происходящих в исследуемых системах.

Целью работы было развитие упрощенной одномерной модели сложной сверхрешетки и двумерной модели простой 2D сверхрешетки. Исходная металл-диэлектрическая сверхрешетка представляла собой перфорированный методом soft interface lithography 1 80 нм слой металла (золота) на стеклянной подложке. В центре элементарной ячейки квадратной сверхрешетки (со сторонами 6×6 $\mu м^2$) имелась 4×4 $\mu м^2$ область с решеткой отверстий 0.1×0.1 $\mu м^2$ и периодом 0.4 μм.

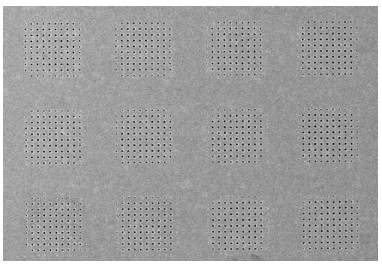


Рис. 1. Исследуемая структура

Для данной структуры были проведены измерения спектров оптического пропускания в зависимости от энергии фотона и проекции его волнового вектора на плоскость структуры.

В качестве упрощенной модели сначала была взята одномерная сверхрешетка с таким же периодом и сверхпериодом, что и оригинальная двумерная структура. Для проверки эффектов возникающих в связи со сверхпериодичностью была взята простая двумерная модель. В расчетах был использован модифицированный метод матрицы рассеяния 24. По расчетам удалось объяснить качественно многие свойства изначальной двумерной структуры.

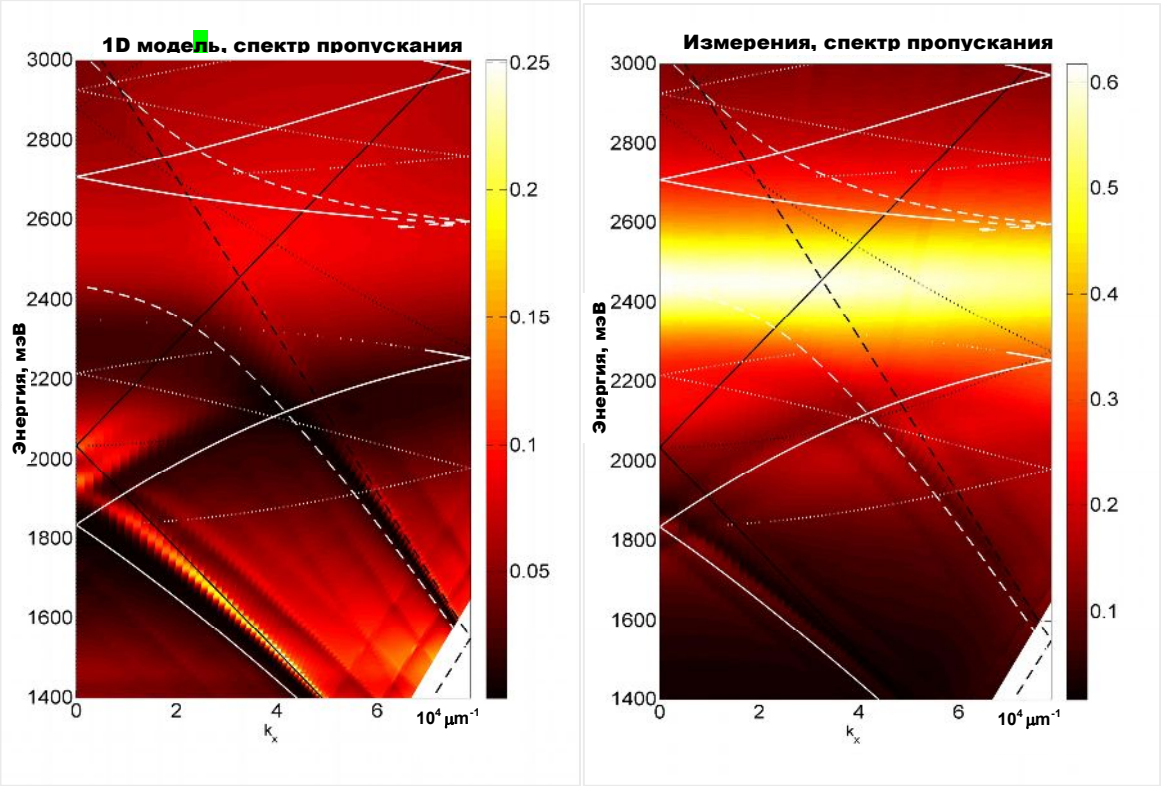


Рис. 2. Слева: Рассчитанный спектр оптического пропускания упрощенной одномерной модели. Справа: Измеренный спектр пропускания выращенной структуры. Цветом показана величина пропускания (цветовая шкала объясняется справа). Законы дисперсии фотонов (черные линии) и поверхностных плазмонов (белые линии) для стекла (сплошные линии) и воздуха (пунктиры) свернуты в 1-ю зону Брюллиэна решетки

Заключение

Многие важные аномалии в спектрах оптического пропускания, которые наблюдаются в измерениях, можно понять, используя для метал-диэлектрического фотонного кристалла приближение пустой решетки 57. Особенности, которые наблюдаются в спектрах, лежат на свернутых в первую зону Бриллюэна дисперсионных законах фото-

нов в воздухе и в подложке, а также поверхностных плазмонов на границах раздела воздух/металл и подложка/металл.

Литература

1. Henzie J., Lee M. H. and Odom T. W.,Nature Nanotechnology 2, 549 - 554 (2007).
2. Tikhodeev S. G., Yablonskii A. L., Muljarov E. A., Gippius N. A., Ishihara T.. PRB **66**, 045102 (2002).
3. Granet G., Guizal B. J. Opt. Soc. Am. A **13**, 1019 (1996).
4. Lifeng Li, J. Opt. Soc. Am. A/ Vol. 13, No. 9 (1996).
5. Sakoda K., Optical properties of photonic crystals, Springer (1998).
6. Christ A., Zentgraf T., Tikhodeev S. G., Gippius N. A., Kuhl J., Giessen H., PRB **74**, 155435 (2006).
7. Christ A., Zentgraf T., Tikhodeev S. G., Gippius N. A., Kuhl J., Giessen H., PRB **73**, 115103 (2006).

УДК 004.738.5:002.513.5

АВТОМАТИЗАЦИЯ ПРОЕКТИРОВАНИЯ ПРЕДМЕТНЫХ ОНТОЛОГИЙ С ИСПОЛЬЗОВАНИЕМ ИНТЕЛЛЕКТУАЛЬНЫХ АГЕНТОВ

Я.А. Седова
(Астраханский государственный технический университет)
Научный руководитель – к.т.н., профессор И.Ю. Квятковская
(Астраханский государственный технический университет)

Онтологии являются эффективным способом представления знаний. В настоящее время онтологии проектируются вручную, поэтому актуальна задача автоматизации этого процесса. В статье рассмотрены особенности разработки автоматизированной системы проектирования предметных онтологий с использованием интеллектуальных поисковых агентов.

Ключевые слова: онтологии, интеллектуальные агенты, LSPL-шаблоны, информационный поиск

Введение

В условиях информационного взрыва актуальной становится реализация новых методов упорядочения информации. В связи с этим большую популярность приобретают онтологии. Согласно определению, данному Т. Грубером, онтология – «явная спецификация концептуализации» [1]. На момент написания данной статьи поисковой системой Swoogle было проиндексировано свыше 10 тысяч онтологий, доступных в Веб. Сейчас трудоемкий процесс проектирования онтологий выполняется экспертом вручную на основе его знаний о предметной области. Актуальна задача автоматизации этого процесса. Необходимо также отметить, что существующие программные средства для разработки онтологий не осуществляют интеллектуальной поддержки этого процесса. В данной статье будут рассмотрены особенности создания автоматизированной системы проектирования онтологий.

Основная часть

Архитектура разрабатываемой системы представлена на рисунке.

В качестве источника данных для построения онтологии используется сеть Интернет. Автоматизированный сбор информации из нее требует реализации алгоритмов информационного поиска. В частности, используется интеллектуальный агент – поисковый робот-паук (crawler). Паук представляет собой программный модуль, который переходит по заданным пользователем гиперссылкам, сохраняет текстовые копии посещенных веб-ресурсов в базе данных, находит новые гиперссылки, после чего посещает их и т.д. Процесс обхода теоретически конечен, поскольку конечно множество веб-ресурсов. Разработанный автором поисковый робот прекращает работу и в том случае, если превышен заданный пользователем предельный объем трафика или предельное время работы.

Поскольку индексирование большого количества веб-ресурсов требует значительных материальных затрат для хранения индекса, поисковые модули разрабатываемой системы могут также обращаться к индексной базе крупной поисковой системы «Яндекс» и получать результаты поиска по заданному запросу с помощью технологии «Яндекс.XML». Затем модуль-паук должен посетить страницы, адреса которых были получены из системы «Яндекс» и сохранить в базе данных их тексты. Поиск новых гиперссылок и переход по ним в этом случае не происходит.

Поскольку анализ естественного языка является сложной задачей, которая в общем случае до сих пор не имеет точного решения, в разрабатываемой системе использовались методы, ориентированные на задачи информационного поиска. При этом учитывались следующие особенности данных, используемых при построении онтологий:

1. Данные формулируются на естественном языке, часто близком к своему разговорному варианту.
2. Необходимо быстро обрабатывать объемные текстовые коллекции, причем лишь некоторые фразы текста несут смысловую нагрузку, представляющую интерес для пользователя.
3. Глубокому смысловому анализу подлежат не предложения в целом, а их отдельные части или словосочетания.
4. Нет необходимости извлекать все содержащиеся в тексте факты, поскольку онтология будет дорабатываться экспертом.
5. Морфологические признаки многих слов, составляющих подлежащие извлечению из текста факты, являются фиксированными (например, глагол обычно употреблен в настоящем времени, поскольку эксперта, составляющего онтологию, интересуют существующие факты, а не имевшие место в прошлом или планируемые).

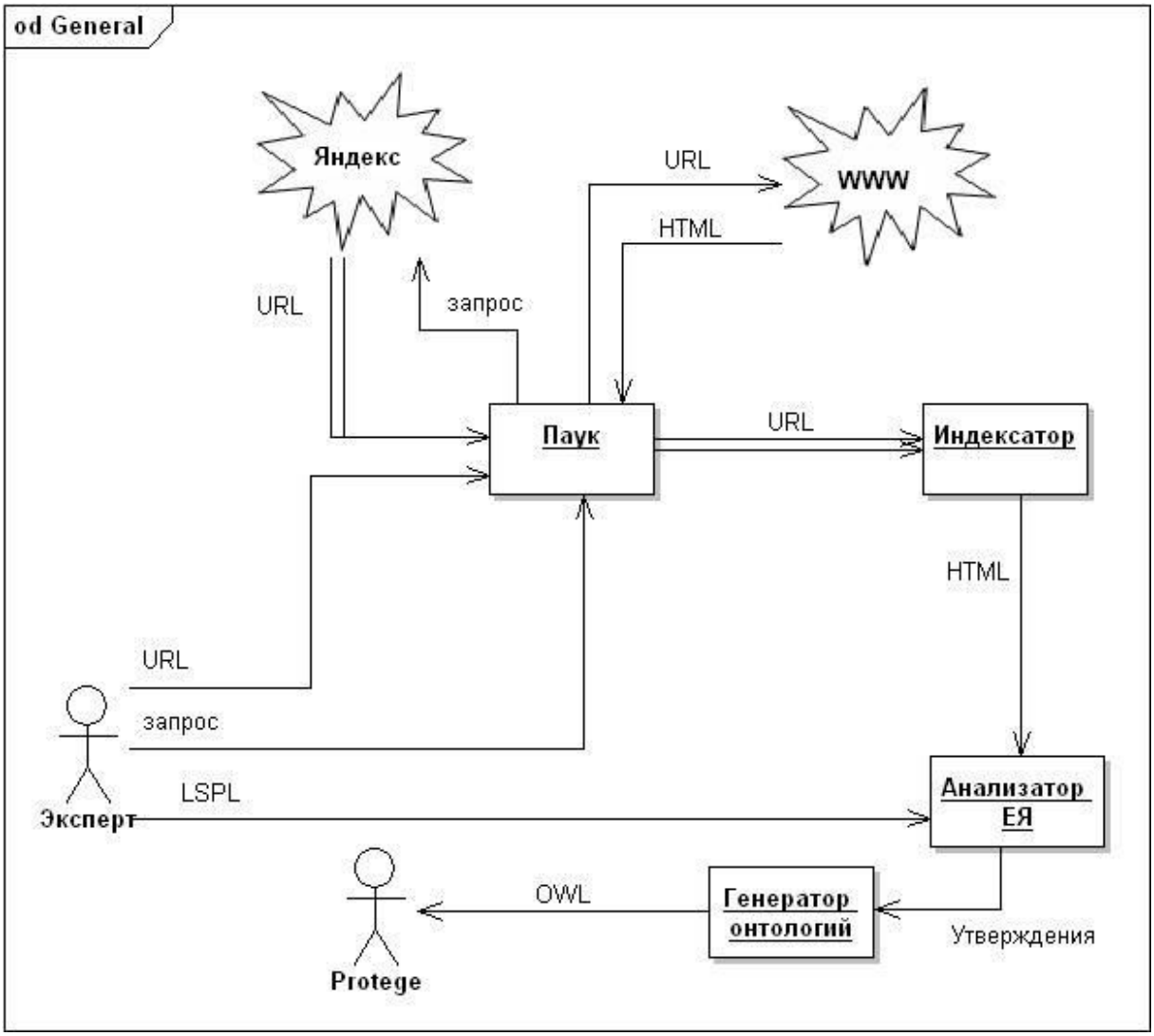


Рисунок. Архитектура системы

С учетом перечисленных особенностей анализ естественного языка целесообразно осуществить с помощью 1) алгоритма стемминга (stemming) и 2) лексико-синтаксических шаблонов.

Алгоритм стемминга Портера (Porter) [2] – эвристический алгоритм, идея которого заключается в выделении основы слова. Стемминг не может заменить полноценный морфологический разбор, однако в задачах информационного поиска данный алгоритм применяется успешно.

Для выделения из текста утверждений, необходимых для онтологии, удобно использовать лексико-синтаксические шаблоны, записанные на языке LSPL [3]. Шаблоны можно рассматривать как альтернативу синтаксическому разбору предложений в тексте. Анализ языка LSPL должен осуществлять модуль-интерпретатор.

Автором была построена формальная грамматика языка LSPL, представленная в таблице.

S->Declare	Attr->RusWord; Signs
S->Expr Exprs	Attr->Signs
Declare->Id=Exprs (Id)	Attr->RusWord
Declare->Id=Exprs	Signs->Sign, Signs
Exprs->Expr Exprs	Signs->Sign
Exprs->Expr	Sign->sname=sval
Exprs->Expr|Exprs	Sign->Element=Equality
Exprs->Id Exprs	Equality->Element=Equality
Exprs->[Exprs]	Equality->Element
Exprs->{Exprs}	Element->Id.sname
Exprs->{Exprs}<Num>	Element->Id
Expr->Expr<Attr>	Num->number,number
Expr->Id	Num->number
Expr->String	

Таблица. Грамматика языка LSPL

Для лексического разбора LSPL-шаблонов был построен конечный автомат. Для синтаксического разбора целесообразно использовать метод рекурсивного спуска.

При ручном анализе текстов тематики «виноделие» был сформирован ряд шаблонов типичных языковых конструкций. Исходя из соответствия шаблону набора слов естественного языка, может быть сделано предположение относительно семантической связи между этими словами и смысла фразы.

Например, по соответствию фразы шаблону

NP [A<который; A=NP>] V<исчисляться|вычисляться|измеряться; t=pres, p=3> “в” N<n=plur, c=pre>,

где NP – именная группа, может быть сделано предположение, что объект N является единицей измерения объекта NP («длительность послевкусия измеряется в каудалях»).

Функция модуля «Генератор онтологий» - преобразование выделенных по шаблонам из текста языковые конструкции в OWL-утверждения, из которых и будет составлен черновой вариант онтологии.

Составленная таким образом онтология экспортируется в редактор онтологий, например, Protégé, после чего эксперт может дорабатывать ее.

Заключение

Применение автоматизированной системы, архитектура которой была описана в данной статье, позволит существенно ускорить работу эксперта при проектировании онтологии и повысить эффективность доступа к знаниям конкретной предметной области. В настоящее время автором разработаны модули информационного поиска. Разрабатываются модули интерпретации языка LSPL, поиска соответствий шаблонам в тексте и генерации утверждений на OWL.

Литература

1. Gruber T. A translation Approach to Portable Ontology Specifications [Электронный ресурс]. – Режим доступа: http://tomgruber.org/writing/ontolingua-kaj-1993.pdf, свободный. – Загл. с экрана. – Яз. англ.
2. Russian stemming algorithm [Электронный ресурс]. – Режим доступа: http://snowball.tartarus.org/algorithms/russian/stemmer.html, свободный. – Загл. с экрана. – Яз. англ.
3. Большакова Е.И., Баева Н.В., Бордаченкова Е.А., Васильева Н.Э., Морозов С.С. Лексико-синтаксические шаблоны в задачах автоматической обработки текста. // Труды Международной конференции «Диалог-2007». – М.: Издательский центр РГГУ, 2007. – С. 70–75.

УДК 004.75

РАЗРАБОТКА DESKTOP ПРИЛОЖЕНИЙ С СОВМЕСТНЫМ ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ GWT И EXTJS

А.В. Кирпичников
(Оренбургский государственный университет)
Научный руководитель – д.т.н., профессор Н.А. Соловьёв
(Оренбургский государственный университет)

В данной статье рассмотрены технологии построения DESKTOP-ориентированных WEB приложений, на базе технологий Google Web Toolkit и ExtJS. Применение данных технологий обеспечивает полную реализацию пользовательского интерфейса на базе концепции DESKTOP в окне браузера, с применением языка JAVA.

Ключевые слова: ExtJS, GWT, Ext-GWT, desktop, WEB, пользовательский интерфейс, JAVA, тонкий клиент, фреймворк, IDE, коммьюнити

1. Введение

В настоящее время развитие интернет технологий достигло такого уровня, что решения, построенные на базе WEB, способны по своим возможностям конкурировать с обычными Desktop приложениями. Реализуемые в окне браузера, они полностью соответствуют концепции полноценного пользовательского интерфейса, со всей вытекающей отсюда спецификой и правилами построения. В окне обозревателя Интернета, пользователь видит перед собой полноценную и привычную среду, с таблицами, меню, всплывающими подсказками, кнопками, полями ввода и так далее, не задумываясь о том, как работать, потому как, в таком интерфейсе использованы, давно привычные пользователю решения.

Несомненным преимуществом построения интерфейса пользователя на базе WEB, является кроссплатформенность приложения. Точнее, в данном случае, о зависимости от платформы речи не идёт вообще, так как, построенные, в конечном итоге, на базе языка JavaScript, интерфейсы не имеют платформо-зависимого кода. Весть код выполняется на базе браузера, что исключает зависимость от операционной системы.

Далее, концепция WEB интерфейса, реализует концепцию «тонкого» клиента, которая позволяет, в качестве конечного клиента применять дешевые решения, базирующиеся на недорогих, вследствие своей невысокой производительности, комплектующих.

2. Технологии

Некоторое время назад, построение интерфейсов с использованием JavaScript, было связано с рядом трудностей, такими, например, как сложность отладки ошибок, сложность при программировании, связанных с особенностями типизации данных в языке, сложность поддержки больших объёмов кода и др. Но на данный момент существует некоторый набор технологий, который решает описанные проблемы. Например, это решение на базе использования при программировании трёх технологий:

1) GWT – Google Web Toolkit – свободный Java фреймворк, который позволяет WEB-разработчикам создавать Ajax приложения на основе Java;

2) Ext – Javascript фреймворк для разработки веб-приложений и пользовательских интерфейсов;

3) Ext GWT (GXT) – библиотека, объединяющая возможности вышеописанных фреймворков, сочетающая возможность программирования интерфейса на языке Java, с мощью библиотеки Ext.

В совокупности эти технологии позволяют использовать в качестве основы пользовательского приложения фреймворк GWT, что позволяет использовать в качестве языка программирования, язык Java, под который написано множество IDE с широчайшими возможностями для отладки кода. Использование же библиотеки, позволяет в языке использовать не только конструкции GWT, но и расширенные возможности Ext, при помощи которых возможности реализации пользовательских интерфейсов выходят на новый уровень. При учёте, что как Goolge, постоянно дорабатывает свой проект, так и Ext и GXT – это динамично развивающиеся проекты с живым и активным коммьюнити.

Подход к программированию, с применением решений от Sun Microsystems, в том числе языка Java, СУБД MySQL, смежных Java технологий, таких как SpringFramework, Catalina Tomcat, Struts, позволяют решить широчайший круг проблем при разработке приложений на основе WEB.

2.1. Основные понятия

1) ExtJS/1/ – Javascript фреймворк для разработки веб-приложений и пользовательских интерфейсов, изначально задуманный как расширенная версия Yahoo! UI Library, вылившийся затем в отдельную библиотеку. Использует адаптеры для доступа к библиотекам YUI, jQuery или Prototype/script.aculo.us. Поддерживает технологию AJAX, анимацию, работу с DOM, реализацию таблиц, вкладок, обработку событий и все остальные новшества «Web 2.0»;

2) GWT/2/ – свободный Java фреймворк, который позволяет веб-разработчикам создавать Ajax приложения на основе Java. Выпускается под лицензией Apache версии 2.0. GWT делает акцент на повторное использование и кроссбраузерную совместимость;

3) Ext-GWT/3/ – библиотека, объединяющая возможности вышеописанных фреймворков, сочетающая возможность программирования интерфейса на языке Java, с мощью библиотеки Ext;

4) Desktop/4/ – в компьютерной терминологии основное окно графической среды пользователя вместе с элементами, добавляемыми в него этой средой. Обычно на рабочем столе отображаются основные элементы управления графической средой и какое-либо фоновое изображение;

5) WEB/5/ – распределённая система на базе Интернета;

6) JAVA/6/ – объектно-ориентированный язык программирования, разрабатываемый компанией Sun Microsystems и официально выпущенный 23 мая 1995 года. Так называют не только сам язык, но и платформу для создания приложений уровня предприятий на основе данного языка;

7) тонкий клиент/7/ – широкий с точки зрения системной архитектуры ряд устройств, которые объединяются общим свойством: возможность работы в терминальном режиме. Примером тонкого клиента может служить компьютер с браузером, использующийся для работы с веб-приложениями;

8) фреймворк/6/ – термин, имеющий размытое значение. Обычно используется в программировании, обозначая «простую концептуальную структуру, используемую для решения сложной, проблемной задачи»;

9) IDE/6/ (англ. IDE, Integrated development environment) – система программных средств, используемая программистами для разработки программного обеспечения;

10) коммьюнити/8/ – группа людей со сходными интересами, которые общаются друг с другом в основном через Интернет.

2.2. ExtJS

Библиотека ExtJS написана на JavaScript и работает во всех популярных сейчас браузерах, предназначена для создания сложных пользовательских интерфейсов,

которые очень похожи на их аналоги из мира desktop-программ. Она предоставляет разработчику целый набор графических компонентов, от кнопок и расширенных элементов обычных HTML-форм, до сложнейших компонентов вроде таблиц, компонент размещения (layout) и деревьев.

В библиотеке также есть достаточно много невидимых пользователю компонентов, которые и обеспечивают работу того, что мы видим на экране. Это и получение данных с сервера в фоновом режиме (в формате JSON или XML), обновление частей страницы, локальные хранилища данных, поддержка cookie и многое другое/9/.

Каждый компонент в ExtJS позволяет себя конфигурировать путем настройки разнообразных опций, генерирует множество событий в ответ почти на любое изменение своего состояния, а также гибко настраивается через задание необходимых свойств оформления в CSS-стилях. В архитектуре библиотеки есть и такое понятие как тема оформления – это обычный CSS-файл, изменяя который можно мгновенно изменить внешний вид всех элементов интерфейса.

Один из самых развитых компонентов библиотеки – это таблица, здесь реализованы механизмы сортировки, фильтрации, группировки, всё это положено на несколько моделей хранения данных, в совокупности с различными способами доступа к данным, как удалённым, так и локальным, функциональность таблицы позволяет реализовать большинство задач, которые пользователь может решать табличным способом. На рис. 1 показан пример таблицы, реализованной на ExtJS

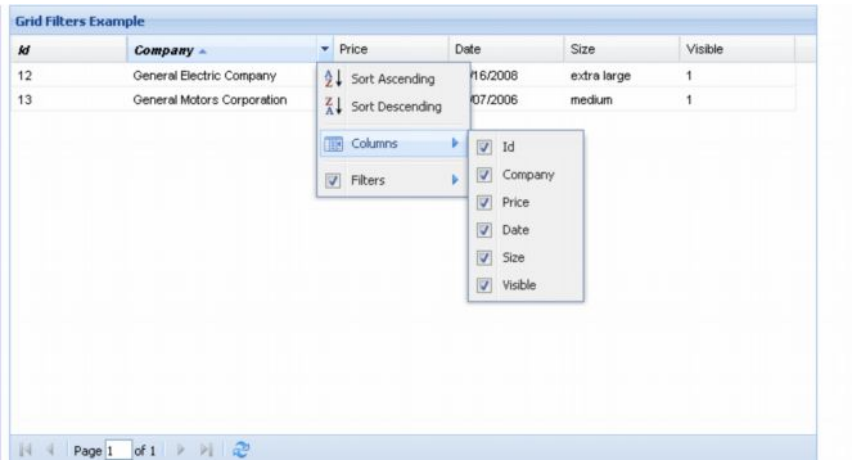


Рис. 1. Пример таблица ExtJS

2.3. Google Web Toolkit

Фреймворк GWT использует в качестве основы программирования WEB интерфейса, модель языка Java. GWT обеспечивает поддержку, в разрабатываемом приложении, клиент-серверной архитектуры, JAVA – интерфейсов, поддержку java.lang и java.util пакетов. Модель GWT – это попытка абстрагирования от HTTP-протокола и HTML DOM-модели.

Реализация данных принципов заключена в том, что GWT при помощи компилятора, Java код преобразуется в JavaScript, который работает на большинстве современных браузеров, как и ExtJS:

1) Internet Explorer 6+;
2) FireFox 1.5+;
3) Safari 2+;
4) Opera 9+.

Достоинством разработки приложения на GWT, является его поддержка наиболее популярными IDE, для разработки Java – это, например, IntelliJ IDEA, Eclipse.

3. Применение

Слиянием двух этих Фреймворков явилась библиотека GXT, расширяющая компонентные возможности GWT, при сохранении всех, ранее описанных возможностей.

Программирование интерфейсов пользователя и программной среды на GXT больше напоминает программирование интерфейсов на Swing, нежели программирование WEB интерфейсов.

По своей сути, программист, в данном случае абстрагируется от специфики создаваемого интерфейса. В данном случае реализуется модель построения интерфейса пользователя в привычных для Java принципах. Программист не конструирует WEB страничку, а пишет полнофункциональный интерфейс, не задумываясь о том, как и где он будет показан.

Прелесть баузерного подхода состоит ещё и в том, что для отображения интерфейса, у пользователя на рабочей станции не требуется никакого дополнительного программного обеспечения – только браузер, одной из требуемых ранее версий. Т.е. не нужна даже Java машина.

3.1. Примеры

В библиотеке GXT реализованы удобные и быстрые в реализации методы хранения и получения данных.

Ниже представлен пример реализации доступа к данным в таблице, с применением одной из моделей доступа к данным (листинг 1–3).

Листинг 1. Добавление столбцов в таблицу

```
List<ColumnConfig> columnConfigs = new ArrayList<ColumnConfig>();
ColumnConfig idColumn = new ColumnConfig("customerId", "Код", 70);
columnConfigs.add(idColumn);
ColumnConfig nameColumn = new ColumnConfig("mainFIO", "ФИО", 300);
columnConfigs.add(nameColumn);
```

Листинг 2. Установка механизма Proxy для получения данных

```
RpcProxy proxy = new RpcProxy() {
public void load(Object loadConfig, AsyncCallback callback) {
HashMap<String, String > map = new HashMap<String, String>();
HashMap<String, String > mapFilter = new HashMap<String, String>();
PagingLoadConfig pagingConfig = (PagingLoadConfig)loadConfig;
String sortDir = pagingConfig.getSortInfo().getSortDir().toString();
String sortField = pagingConfig.getSortInfo().getSortField();
customerManager.getCustomersPaged(pagingConfig.getLimit(),
                pagingConfig.getOffset(),
                mapFilter,
                map.get(sortField),
                sortDir, callback);}};
```

Листинг 3. Получение данных

```
customerListLoader = new BasePagingLoader(proxy, new BeanModelReader());
customerListLoader.load(0, 19);
```

Т.е. в данном случае описана идеология доступа к данным, которая реализуется, через реализацию модели внутреннего именования столбцов, в таблице. Причем, в данном примере реализован принцип постраничной загрузки данных, через загрузку объектов модели данных приложения.

Реализация асинхронности вызова удалённых процедур, реализована здесь на таком же простом уровне, как и работа с моделями данных. Пример показан в листинге 4.

Листинг 4. Асинхронный вызов удалённой процедуры

```
udcManager.getChildrenUDCsInCatalogItem(ci.getId(), new AsyncCallback<ArrayList<UDC>>() {
        public void onFailure(Throwable caught) {
        }
        public void onSuccess(ArrayList<UDC> al) {
        }
});
```

В примере асинхронного вызова удалённой процедуры (листинг 4), можно увидеть, что в имплементации интерфейса, существуют два метода, каждый из которых отвечает за окончание вызова процедуры. Метод onFailure – вызывается при неудачном завершении вызове, onSuccess – при удачном. Причем в последнем случае в качестве параметра метода, передаются полученные из вызова процедуры данные. Асинхронность же вызова заключается в том, что JavaScript реализация интерфейса не будет ждать, пока все данные будут получены, а предоставит пользователю возможность дальше работать с интерфейсом, без каких-либо задержек – это реализация асинхронного принципа AJAX.

На рис. 2 можно увидеть полноценный интерфейс пользователя, реализованный на GXT.

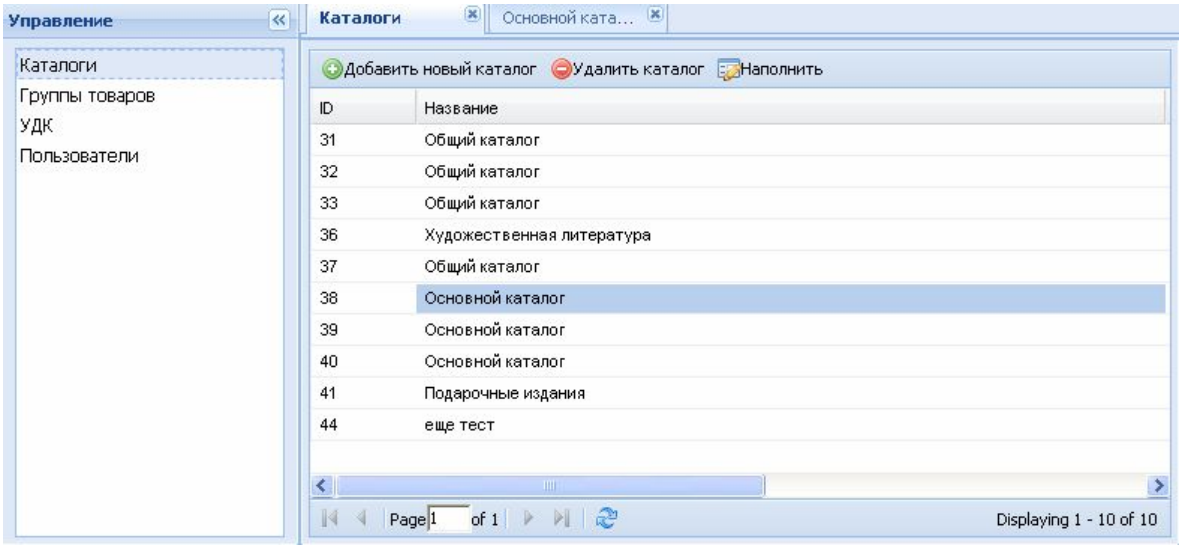


Рис. 2. Интерфейс пользователя на GXT

4. Заключение

Применение технологий ExtJS, GWT, GXT при программировании WEB интерфейсов позволяет реализовывать удобные динамические интерфейсы пользователя, предоставляющие полную функциональность Desktop приложения, в сочетании со всеми преимуществами баузерного исполнения.

При учёте постоянного роста мощностей компьютеров, и постоянному, вследствие экстенсивного расширения компаний, росту филиалов на территории государств, применение приложений, с WEB интерфейсом - это перспектива развития отрасли программирования на несколько лет вперёд, т.е. применение данного подхода будет только развиваться.

Литература

1. ExtJS overview [Электронный ресурс] / Haskell Wiki – Электрон, дан. – Режим доступа: http://extjs.com/products/extjs/ свободный. – Загл. с экрана. – Яз. англ.
2. GWT overview [Электронный ресурс] / Haskell Wiki – Электрон, дан. – Режим доступа: http://code.google.com/intl/ru-RU/webtoolkit/ свободный. – Загл. с экрана. – Яз. англ.
3. GXT overview [Электронный ресурс] / Haskell Wiki – Электрон, дан. – Режим доступа: http://extjs.com/products/gxt/ свободный. – Загл. с экрана. – Яз. англ.
4. Портянкин И.А. Swing: Эффектные пользовательские интерфейсы. Библиотека программиста. – СПб: Питер, 2005 – 524 с. ил.
5. Таненбаум Э. Компьютерные сети. 4-е изд. – СПб: Питер, 2006. – 992 с.: ил. – (Серия «Классика computer science»)
6. Хабибуллин И. Самоучитель Java 2. – СПб: БХВ-Петербург, 2005. – 720 с.: ил.
7. Крейн Д., Паскарелло Э., Джеймс Д. Ajax в действии. Пер. с англ. – М.: Издательский дом «Вильямс», 2006. – 640 с. ил. – Парал. Тит. англ.

УДК [004.4: 338.22]: 69

ИССЛЕДОВАНИЕ И РАЗРАБОТКА ПОДХОДОВ РЕИНЖИНИРИНГА БИЗНЕС-ПРОЦЕССОВ В СТРОИТЕЛЬСТВЕ

К.С. Пачурова
(Волгоградский государственный технический университет)
Научный руководитель – д.т.н., профессор А.М. Дворянкин
(Волгоградский государственный технический университет)

Проведено исследование методологий моделирования бизнес-процессов, систем построения бизнес-процессов, алгоритмов и средств реинжиниринга и систем управления проектами. В работе описаны задачи, решаемые с помощью реинжиниринга, его принципы, процесс реорганизации деятельности бизнес-системы и предложения по совершенствованию этой деятельности.

Ключевые слова: реинжиниринг, бизнес-процессы, управление проектами, автоматизированная система, реинжиниринг бизнес процессов, управление бизнес-процессами

В период увеличения добычи нефти и газа неуклонно растет потребность в развитии сети трубопроводного транспорта. Развитие транспортной системы нефтегазового комплекса связано, прежде всего, со строительством новых объектов: газопроводов, нефтепроводов, компрессорных и нефтеперекачивающих станций.

Увеличение объемов строительства вызывает необходимость пересмотра существующих методов организации ведения строительства крупных объектов. Современные экономические условия поставили ряд проблем перед строительными предприятиями отрасли: ускорение темпов, сокращение затрат, ликвидация сезонности, повышение качества работ и увеличение контроля за состоянием окружающей среды.

Комплексное решение этих проблем может быть выполнено на основе системного анализа и зависит от принятия оптимальных проектных решений, принятия новых материалов и конструкций, повышения уровня механизации, разработки и внедрения современной технологии производства работ, использовании информационных технологий, а также прогрессивных форм организации строительства мощных трубопроводных систем [1].

Согласно определению М. Хаммера и Д.Чемпи реинжиниринг бизнес-процессов (BPR – Business process reengineering) определяется, как «фундаментальное переосмысление и радикальное перепроектирование бизнес-процессов (БП) для достижения коренных улучшений в основных показателях деятельности предприятия» [2].

Целью реинжиниринга бизнес-процессов (РБП) является целостное и системное моделирование и реорганизация материальных, финансовых и информационных потоков, направленная на упрощение организационной структуры, перераспределение и минимизацию использования различных ресурсов, сокращение сроков реализации потребностей клиентов, повышение качества их обслуживания [3].

Реинжиниринг бизнес-процессов выполняется на основе применения инженерных методов и современных программных инструментальных средств моделирования бизнес-процессов совместными командами специалистов компании и консалтинговой фирмы [4].

В соответствии с определением Е.Г. Ойхмана и Э.В. Попова: «Реинжиниринг бизнеса предусматривает новый способ мышления – взгляд на построение компании как на инженерную деятельность. Компания или бизнес рассматривается как нечто, что может быть построено, спроектировано или перепроектировано в соответствии с инженерными принципами» [5].

Реинжиниринг бизнес-процессов обеспечивает решение следующих задач:

– определение оптимальной последовательности выполняемых функций, которое приводит к сокращению длительности цикла изготовления и продажи товаров и услуг, обслуживания клиентов, следствием чего служит повышение оборачиваемости капитала и рост всех экономических показателей фирмы;
– оптимизация использования ресурсов в различных бизнес-процессах, в результате которой минимизируются издержки производства и обращения и обеспечивается оптимальное сочетание различных видов деятельности;
– построение адаптивных бизнес-процессов, нацеленных на быструю адаптацию к изменениям потребностей конечных потребителей продукции, производственных технологий, поведения конкурентов на рынке и, следовательно, повышение качества обслуживания клиентов в условиях динамичности внешней среды;
– определение рациональных схем взаимодействия с партнерами и клиентами, и как следствие, рост прибыли, оптимизация финансовых потоков.

Важнейшими принципами реинжиниринга бизнес-процессов являются представленные на рис. 1.

Реорганизация бизнес-системы есть подход перепроектирования бизнес-процессов в структурном виде, обеспечивающим увеличение количества производимой и количество потребителей продукции, а также уменьшение стоимости издержек производства при заданном количестве операций, их длительности выполнения и капиталовложениях в производство [6].

Рис. 1. Важнейшие принципы реинжиниринга

Реорганизация деятельности бизнес-системы (БС) осуществляется в два основных этапа (см. рис. 2).

На основе применения комплексов функционально-информационно-стоимостных моделей производится:
– анализ технологий реализации бизнес-процессов по показателям эффективности;
– анализ и оценка информационных потоков и документооборота [7];
– анализ деятельности структурных подразделений бизнес-системы;
– формирование информации, которая необходима для понимания происходящих в структурных подразделениях бизнес-системы процессов и для принятия обоснованных решений по их улучшению;

– определение стоимости издержек производства продукции;
– определение точного значения себестоимости производства и сбыта продукции;
– определение эффективности применения средств автоматизации в структурных подразделениях бизнес-системы;
– выделение функций, которые обеспечивают достижение стратегических целей реализации бизнес-процессов и являются наиболее прибыльными;
– обнаружение дорогостоящих функций (затратных центров) технологий реализации бизнес-процессов, которые не оправдывают затрачиваемых на них средств;
– разработка ранжированных перечней (по значениям показателей) технологических участков реализации бизнес-процессов;
– разработка ранжированного перечня технологических участков, изменение которых обеспечит улучшение значений показателей реализации бизнес-процессов.

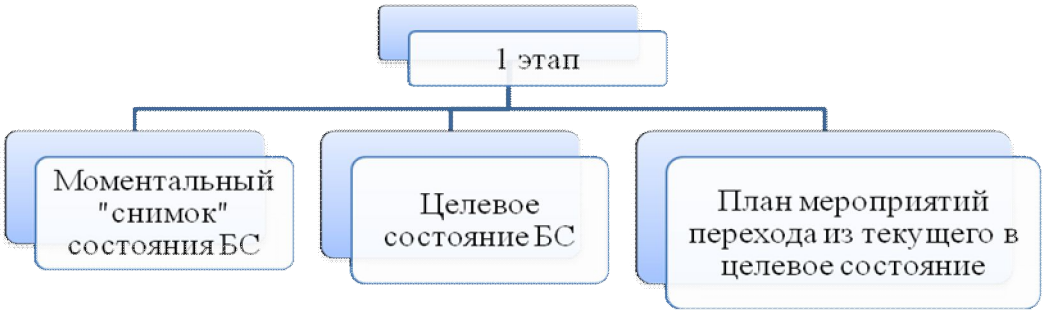


Рис. 2. Первый этап реорганизации деятельности БС

Существует большое количество различных нотаций для построения бизнес-процессов [8]. В список таких нотаций входят:
– SADT/IDEF0;
– DFD в нотациях Гейна-Сарсона и Йордона-Де Марко;
– IDEF3;
– ORACLE;
– BAAN;
– ARIS в нотации eEPC (extended Event-driven Process Chain);
– Классическая методология;
– Методология Betec;
– UML;
– BPEL;
– Workflow.

Использование таких средств моделирования позволит достичь следующих задач, представленный на рис. 3.

Основными средствами, позволяющими моделировать бизнес-процессы, являются:
– Design/IDEF;
– All Fusion Process Modeler (Bpwin);
– Power Designer;
– Бизнес-Студио;
– MS Visio;
– QPR Collaborative Management;
– Мотив;
– Oracle Designer;
– BAAN EME;
– Инструментарий ARIS;

– Бизнес – инженер Профи;
– Enterprise Architect;
– WebSphere Business Integration Modeler.

Результатом обобщения проведенного анализа существующих технологий реализации бизнес-процессов по функционально-информационно-стоимостным моделям являются предложения по совершенствованию деятельности бизнес-системы. Предложения по совершенствованию деятельности бизнес-системы, как правило, включают следующие улучшения (см. рис. 4).

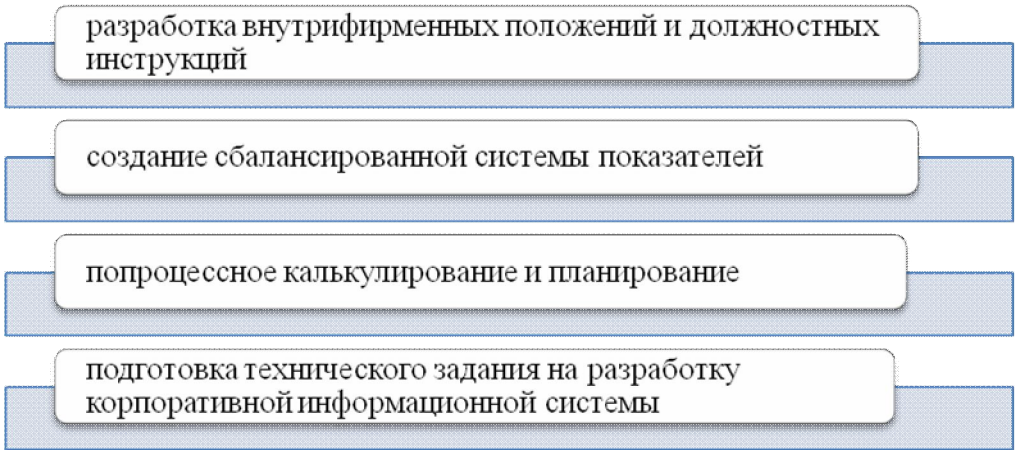


Рис. 3. Задачи, решаемые средствами построения БП

Интеграция сформированных предложений по совершенствованию деятельности бизнес-системы со взвешенным деревом целей и требований, сформулированных руководством, позволяет разработать целевую программу развития бизнес-системы [9]. Целевое состояние бизнес-системы характеризуется соответствующими комплексами функционально-информационных, функционально-стоимостных и функционально-имитационных моделей. Наличие комплексов функционально-информационно-стоимостных моделей текущего и целевого состояний бизнес-системы, а также целевой программы развития бизнес-системы позволяет создать план мероприятий по переходу бизнес-системы из текущего состояния в целевое.

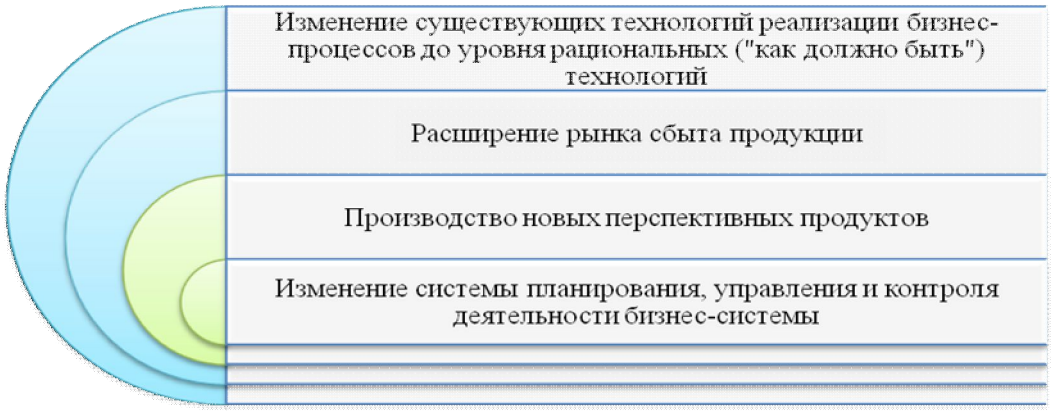


Рис. 4. Предложения по совершенствованию деятельности бизнес-системы

Таким образом, актуальным является создание автоматизированной системы анализа и поддержки методов реинжиниринга бизнес-процессов в строительстве. Система позволит выявить наиболее проблемные участки и предложить как пути изменения существующих, так и создание новых бизнес-процессов, что в свою очередь должно повлечь за собой повышение качества и скорости производства с одновременным снижением издержек, рост профессионализма сотрудников и повышение конкурентоспособности компании.

Литература

1. Ковалев С.М., Ковалев В.М. Секреты успешных предприятий: бизнес-процессы и организационная структура. – М.: Бизнес-инжиниринговые технологии. – 2004.
2. Хаммер М., Чампи Дж. Реинжинринг корпорации: Манифест революции в бизнесе. Пер. с англ. – СПб: Издательство С.-Петербургского университета, 1997. – 332 с.
3. Марка Д.А., МакГоуэн К. Методология структурного анализа и проектирования. – М. – 1993.
4. Шеер А.-В. Моделирование бизнес-процессов. – М.: Весть-метаТехнология. – 2000.
5. Ойхман Е.Г., Попов Э.В. Реинжиниринг бизнеса: Реижиниринг организаций и информационные технологии – М.: Финансы и статистика, 1997. – 336 с.
6. Маклаков С.В. Моделирование бизнес-процессов с BPWin., М.: Диалог-МИФИ. – 2002.
7. Кутелев П.В., Мишурова И.В. Технология реинжиниринга бизнеса. – М.: ИКЦ «МарТ»; Ростов-на-Дону.: Издательский дом «МарТ», 2003. – 176 с.
8. Ефимов В.В. Описание и улучшение бизнес-процессов: учебное пособие / В.В. Ефимов. – Ульяновск: УлГТУ, 2005. – 84 с.

УДК 004.27

ТРОИЧНЫЙ КОМПЬЮТЕР БРУСЕНЦОВА–СОБОЛЕВА И СУПЕРКОМПЬЮТЕРЫ

С.В. Храпов
(Санкт-Петербургский государственный университет)
Научный руководитель – к.ф.-м.н., вед.н.с. О.М. Калинин
(Санкт-Петербургский государственный университет)

В статье описывается троичный компьютер Н.П. Брусенцова «Сетунь». Рассматриваются основные преимущества троичной архитектуры компьютеров. Показано, что 75% компонент архитектуры двоичного компьютера идет на стабилизацию вычислительного процесса. Создание суперкомпьютеров требует микстурной (двоично-троичной) архитектуры в рамках теории МАБ (Математическая аналитическая биология, Санкт-Петербург) и GS (Глобальный скейлинг, Мюнхен). Микстурная архитектура компьютеров приводит к неэлектромагнитным телекоммуникациям.

Ключевые слова: троичная архитектура компьютеров, суперкомпьютер

Введение

9 декабря 2008 года на факультет ВМиК Московского государственного университета им. М.В. Ломоносова состоялась научная конференция, посвященная пятидесятилетию создания ЭВМ «Сетунь» и вопросам развития архитектур цифровых ЭВМ, а так же 55-ию научной деятельности ее главного конструктора Николая Петровича Брусенцова. Троичный компьютер «Сетунь», разработан в вычислительном центре Московского государственного университета им. М.В. Ломоносова в 1956–1958 годы под руководством академика С.Л. Соболева [1].

Для описания персональных компьютеров ПК и суперкомпьютеров СК нужна теория. Такая теория в Петербурге называется МАБ – математическая аналитическая биология (О.М. Калинин, А.Г. Барт и другие участники Биометрического семинара), а в Мюнхене GS (ГС) – глобальный скейлинг, масштабная инвариантность (Хартмут Мюллер) [2, 3].

Троичная архитектура по Брусенцову

Основные компоненты любого компьютера:
– YY (устройство управления) или ОС (операционная система);
– AY (арифметическое устройство).

С появлением 2^{32} разрядных процессоров фирмы Intel процессоры могут работать в трех режимах: реальном (R-режим, $R = 2^{16}$), защищённом (P-режим, $P = 2^{32}$) и виртуального процессора 8086 (V-режим, $V = 2^{16}$).

Архитектуру современных двоичных компьютеров следует трактовать как $2^{16} = YY = NaN = OC$ (Устройство управления) и $2^{32} = AY$ (Арифметическое устройство). Согласно этому архитектура троичной машины Брусенцова записывается следующим образом: МБ = $\left(3^{10} = YY = NaN = OC, 3^{20} = AY\right)$.

Симбиоз двоичной и троичной архитектур компьютеров по Хартмуту Мюллеру $\left(2^{16}, 2^{32}\right) \Rightarrow \left(3^{10}, 3^{20}\right)$. Символ $\Rightarrow$ означает вложение – связывание Брусенцова – Соболева. Теоремы вложения Соболева $W_p^l \Rightarrow W_{p_1}^{l_1}$ в компьютерной науке превратились в технологии OLE (объектов связывание и вложение (внедрение)). Трит Брусенцова и бит связаны законом исключающего третьего, если исключение заменить связыванием.

Фундаментальным числом в троичной машине Брусенцова является число 163. Это число описывает оперативное запоминающее устройство машины (два полкуба памяти и регистр считывания–записи). Оно имеет структуру $163 = 1^2 + 2 \cdot 9^2$ – геометрия Софьи Ковалевской, $163 = 4^2 + 3 \cdot 7^2$ – проективная плоскость. $\sqrt{-163}$ – девятая мнимость Гаусса, $\sqrt{-1}$ – первая мнимость [4].

Модернизированная микстурная машина по Дональду Кнуту описывается следующим образом: $MMIX = 2009 = 7^2 \cdot 41 = \left(\left(2^{16}, 3^{10}\right) = YY, \left(2^{32}, 3^{20}\right) = AY\right)$ [5].

Преимущества троичной архитектуры

Для вещественных архимедовых чисел Q_∞ имеем световой конус:

$$x^2 + y^2 + z^2 = c^2 t^2,$$

где x, y, z – пространственные координаты; t – время; $c = 299792458$ м/с – скорость света [6]. В неархимедовом случае (нестандартный анализ) имеем терему Минковского – Хассе и нерахимедов конус:

$$ax^2 + by^2 = cz^2 + dt^2 \qquad \left(Q_p\right),$$

состоящий из двух бинарных квадратичных форм или одной кватернарной формы (четыре переменные).

Тернарный случай (три переменные) существенно отличается от четырех переменных (трехмерье вкладывается в четырехмерье, а четырехмерье связывается с трехмерьем):

$$ax^2 + by^2 = t^2 \qquad \left(Q_p\right).$$

Если имеются нетривиальные решения, то говорят, что тернарная форма представляет нуль, в противном случае форма не представляет нуль. Для различения этих двух случаев вводится символ Гильберта $\left(a,b\right)_p = \pm 1$ [7].

В случае Q_2 имеется $64 = 36 + 28$ вариантов, 28 вариантов представляют нуль, 36 не представляют нуль. Для Q_3 и Q_p, где $p \geq 3$ имеется $16 = 10 + 6$ комбинаций, $16 = 12 + 4^{\pm}$, здесь $4^{\pm}$ различает случаи $p = 4m \pm 1$. Двоичная и троичная неархимедова математика записывается следящим образом:

$$64 + 36 + 28 \qquad \left(Q_2\right)$$

$$16 = 10 + 6 \qquad \left(Q_3\right).$$

Двоичная математика Q_2 резко сложнее троичной математики Q_3. Можно говорить об устойчивости троичных машин и неустойчивости двоичных. В архимедовом случае Q_∞ имеем $4 = 3 + 1$ – разграничение пространства и времени и 4 нуклеотида в молекулярной биологии.

Двоичные компьютеры неустойчивы по А.М. Ляпунову и 75% двоичной аппаратуры цифровой техники идет на стабилизацию вычислительных процессов – это неустойчивость. Троичный компьютер Брусенцова – Соболева устойчив. В двоичной цифровой технике не существует единого натурального кода для положительных и отрицательных чисел. Поэтому для решения проблемы представления чисел со знаком вводятся 4 типа двоичных кодов: (d – прямой код, i – обратный код, c – дополнительный код, m_i и m_c – модифицированные обратный и дополнительные коды) [8]. Числа в троичной системе счисления удовлетворяют принципу однозначности в отличии от чисел в двоичной системе счисления.

Архитектура компьютеров по Л. Эйлеру

Современные персональные компьютеры имеют архитектуру 2^{64}. Л. Эйлер установил, что число $2^{64}-1$ делится на 641 и указал второе число делящееся на 641, это $96^{10}-2$ [9]. В рамках МАБ–GS имеем число Фарадея (количество электричества):

$F = N_A e = 96484{,}56$ Кл/моль,

где N_A – число Авогадро, e – заряд электрона.

При переходе с континуума Q_∞ на кристаллическую решетку $Q_1 = Z = \{0, \pm 1, \pm 2, \ldots\}$ меняется масштаб (скейлинг) и число Фарадея превращается в число Фарадея – Эйлера $F_E = 96$. В четырехмерном пространстве появляется шестой правильный многогранник Oct_{24}^{96}, состоящий из 24 вершин и 96 ребер, 96 треугольников и 24 октаэдров, $96 = 24 \cdot 4$.

Разложим $96^{10}-2$ на множители $96^{10}-2 = 641 \cdot 2 \cdot 7 \cdot 3727 \cdot 1987773389863$, тринадцатизначное число обозначим P_{13}. Число $3 \cdot 7 \cdot P_{13} = C_{BI}^{-1}$ определим как обратную величину константы биологического взаимодействия C_{BI}. На теле человека имеем $641 = 32 \cdot 20 + 1$ биоактивную точку. Они организованны в 20 меридианов и 32 зоны. Число $3727 = 58^2 + 3 \cdot 11^2 = 47^2 + 22^2 + 47 \cdot 22$, $58 = 29 + 29 -$ половина таблицы Менделеева, 11 – цикл солнечной активности.

На 641 делится число $2^{32}+1 = 641 \cdot 6700417$, что установил Эйлер. Добавим к Эйлеру, что на 641 делится число $2^{96}+1 = 641 \cdot 6700417 \cdot \left(2^{64} - 2^{32} + 1\right)$, $641 = 2^9 + 2^7 + 1$. $96^{10} = 3^{10} \cdot 2^{50}$, где $3^{10} = YY$ – устройство управления в машине Брусенцова, $2^{49} = 2_G^{48} + 2_I^{48}$. В современных двоичных компьютерах $2^{64} = 2^{48} \cdot 2^{16}$, где $2^{48} = DT_I^G$ – регистры таблиц дескрипторов (глобальный и прерываний), $2^{16} = DT_L$ – локальная таблиц дескрипторов.

Архитектура суперкомпьютеров

В современных двоичных компьютерах имеется процессор $FPU = 2^{80}$ – флотское процессорное устройство. Суперкомпьютер Blue Gene (Голубой Ген), 2005 год США состоит из $2^{17} = 131072$ процессоров [10]. Так что можно говорить об архитектуре $2^{80} \cdot 2^{17} = 2^{97}$. У нас $2^{96} = 2^{80} \cdot 2^{16} = 2^{64} \cdot 2^{32}$ и появляется простое число $2^{64} - 2^{32} + 1$.

В машине Брусенцова устройство управления $3^{10} = YY$. Единица информации $2^{16} = W$ – называется словом, wyde (вайд) по Дональду Кнуту. Разность $2^{16} - 3^{10} = 13 \cdot 499 = \left(2^2 + 3^2\right)\left(2^8 + 3^5\right)$, где $3^5 = @$ – адресация в машине Брусенцова, $3^2 = fl = \varphi_2 \varphi_1$ – флаг переполнения, конфигурация Паскаля, $2^2 = bb$ – бибит Брусенцова, нип по Кнуту, 2^8 – байт. Астрономическая единица в секундах $\tau_A = 499{,}004782(\pm 6) \equiv 499\frac{1}{209}$, где $209 = 11 \cdot 19$, $13 \equiv 4\pi$, $499 = 3 \cdot 163 + 10$. Символ $\equiv$ – знак асимптотики, сравнение по модулю (модуляция).

Суперкомпьютер архитектуры $2^{96}-3^{60}=\left(2_I^{48}-3^{30}\right)\left(2_G^{48}+3^{20}\right)$, где 2^{48} – таблицы дескрипторов, $3^{30}=3^{10}\cdot 3^{20}$, где $3^{10}=YY$, $3^{20}=AY$. Модернизированная микстура характеризуется соотношениями:

$$\left(2^8-2^2=3^5+3^2=6^3+6^2=252=7\cdot 36\right)=MMIX=qC=\text{МБ},$$

где qC – квантовый компьютер, 6^3 – трехкварковые комбинации – барионы, 6^2 – двухкварковые комбинации – мезоны, барионы + мезоны = адроны. В квантовом компьютере $64\cdot 4-4=Q_2\cdot Q_\infty-Q_\infty$ имеем кодирование 6 кварками $6=\left(d^u,s^c,b^t\right)$, где d^u – верхний и нижний кварки, s^c – странный и очарованный, b^t – прелестный и правдивый.

В молекулярной биологии белки кодируются 4 нуклеотидами $64=16\cdot 4$ или $Q_2=Q_2\cdot Q_3:4=$ (тимин, аденин; гуацин, цитозин). 20 аминокислот кодируются 4 нуклеотидами, 64 кодона–триплета. Тимин есть метилированный урацил и четверка имеет структуру $1+3$. Превращение байта 256 в число 252 есть наличие 4 контрольных точек при отладке программ.

Заключение

Микстурная (двоично-троичная) архитектура компьютеров приводит к неэлектромагнитным телекоммуникациям на стоячей гравитационной волне $\sqrt{-163}$. Двоичная неархимедова математика в четыре раза сложнее троичной неархимедовой математики. Дальнейшее развитие двоичной архитектуры компьютеров невозможно без перехода к микстурной (двоично-троичной) архитектуре. Суперкомпьютеры должны иметь архитектуру $2^{96}-3^{60}$.

Литература

1. Брусенцов Н.П., Маслов С.П., Розин В.П., Тишулина А.М. Малая цифровая вычислительная машина «Сетунь». – М.: Изд-во МГУ, 1965. – 145 с.
2. Барт А.Г. Анализ медико-биологических систем. Метод частично-обратных функций. – СПб: Изд. СПбГУ, 2003. – 280 с.
3. Калинин О.М., Сурина К.С., Коровин И.В. Галактический год, математическая биология и компьютеры 21 века // Сборник Проблемы исследования вселенной / Под ред. Ефимова А.А. – СПб: Изд-во ЦНИИМ, – 1995. – Вып. 18. – С. 339–348.
4. Калинин О.М., Мюллер Х., Сурина К.С., Барт В.А., Храпов С.В. Троично-двоичные компьютеры и телекоммуникации на стоячей гравитационной волне // Технологии: Труды 1 международного форума «БИОФИЗТЕХНОЛОГИИ» / Под ред. Резунковой О.П. – СПб: Изд-во «Ладога-100», – 2008. – С. 62–63.
5. Кнут Д. Искусство программирования. Том 1. Выпуск 1. MMIX – RISC-компьютер для нового тысячелетия. – СПб: Вильямс, 2007. – 160 с.
6. Боревич З.И., Шафаревич И.Р. Теория чисел. – 3-е изд. доп. – М.: Наука, 1985. –504 с.
7. Касселс Дж. Рациональные квадратичные формы. – Пер. с англ. – М.: Мир, 1982. – 440 с.
8. Жмакин А.П. Архитектура ЭВМ: Учебное пособие. – СПб.: БХВ–Петербург, 2008. – 320 с.
9. Неопубликованные материалы Л. Эйлера по теории чисел. Сборник / Сост. Невская Н.Н. – СПб: Наука, 1997. – 255 с.
10. Буза М.К. Архитектура компьютеров. Учебник. – Минск: ООО «Новое знание», 2007. 560 с.

УДК 004.588

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ ПОДДЕРЖКИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ВУЗа С ПРИМЕНЕНИЕМ ТЕОРИИ РЕКОМЕНДАТЕЛЬНЫХ СИСТЕМ

Д.Н. Пиленко
Научный руководитель – к.т.н., доцент Д.Г. Штенников

В настоящее время количество образовательных ресурсов неуклонно растет, что приводит студента к проблеме выбора: что, где и как изучать. Кроме того, этот выбор становится еще сложнее, когда речь идет об учебных материалах, которые максимально подходили бы под желания и нужды студентов. Выходом из данной ситуации является создание системы, которая на основании определенных характеристик пользователя, таких как его компетенции, история обучения и предпочтения, предлагала бы ему на выбор те или иные учебные материалы, курсы или другие учебные активности.
Ключевые слова: персонализация, рекомендательные системы, экономика внимания

Введение

Во время самостоятельной работы студент использует множество источников для поиска и изучения необходимых учебных материалов. Это может быть как рекомендованная преподавателями литература, так и учебные материалы, размещенные в локальных и глобальных сетях. При поиске наиболее релевантной информации тратится достаточно много времени, которое могло быть использовано для усвоения учебного материала. Кроме того начинает проявляться эффект частичного внимания [1], который проявляется как неспособность удерживать внимание на определенной задаче в течение продолжительного времени в результате постоянного отвлечения на поиск подходящих материалов. Отсутствие «погружения» в учебный материал так же сказывается на его понимании студентом. Следовательно, предоставление студенту необходимых учебных материалов или, иначе говоря, персонализированных учебных материалов, подходящих его потребностям и есть решение вышеуказанной проблемы. Подобные материалы можно рассматривать в качестве адаптивной навигационной поддержки самостоятельной работы студента, которая не носит обязательного характера и может рассматриваться в рамках обучения только как вспомогательное средство.

Персонализация, в той или иной мере, является горячо обсуждаемой проблемой, начиная с 1990 года. Существует ряд рекомендательных информационных систем в коммерческом секторе, целью которых является на основании истории поведения пользователя предлагать пользователю системы определенные товары или услуги [2]. Наиболее известны такие порталы как Amazon и Google, которые собирают информацию о поведении пользователя в скрытые хранилища и в дальнейшем используют эту информацию. Проведя параллель в область образования, становится ясно, что индивидуальные цели, знания, предпочтения и социальное взаимодействие пользователя может быть использовано с целью адаптации информации для целевого пользователя. Персонализация может служить нескольким целям: с одной стороны это корректировка кривой обучения пользователя и помощь в поиске подходящих учебных материалов с другой стороны.

Основная часть

В идеальном случае для определения нужд и потребностей студента в рамках самостоятельной работы система должна иметь такие входные данные как история поведения пользователя внутри системы, индивидуальные цели обучения, интересы, предпочтения, социальные взаимодействия, а так же имеющийся опыт и компетенции, которыми обладает студент на конкретный момент времени. Часть этой информации мо-

жет быть получена самой системой на основе анализа действий студента, но другая часть в особенности предшествующий опыт и компетенции должны поступать в систему из внешней среды. Существует ряд стандартов позволяющих собирать, хранить и экспортировать подобную информацию, примером может служить ePortfolio, своего рода электронное портфолио студента содержащее все пройденные им учебные курсы, тесты, экзамены и прочие учебные активности, которые позволяют сделать вывод о тех компетенциях, которыми обладает студент.

В свою очередь действия студента в рамках системы, так же представляют высокую ценность. Система может отслеживать как явную, так и не явную активность студента. К явной активности можно отнести прохождение обучающих и аттестующих тестов, сообщения на форумах, заполнение различных анкет, ответы на практические задания, поисковые запросы, загрузка файлов на сервер и т.д. К неявной или имплицитной активности можно отнести переходы по разделам системы, время, проведенное на странице. На основании анализа внутренней активности так же можно делать предположения о предпочтениях пользователя и рекомендовать учебные материалы. В качестве полезной информации, помимо вышеупомянутой, следует отметить информацию о социальном взаимодействии студента с другими участниками системы. Принадлежность студента к определенной социальной группе с общими интересами так же может служить основанием для рекомендации учебных материалов. Методы анализа всей вышеприведенной активности выходят за рамки настоящей статьи. Вся собранная информация о студенте-пользователе системы является своего рода портретом пользователя или, иначе говоря, профилем пользователя. Таким образом, стандартная задача поиска

$$v = f(V, q), \qquad (1)$$

где v – множество отобранных узлов; V – множество узлов гипертекста; q – условия пользовательского запроса, преобразуется в задачу вычисления функции

$$v = f(V, q, p), \qquad (2)$$

где p – профиль пользователя, что позволит системе лучше представлять контекст формального пользовательского запроса и правильнее ранжировать результаты [3].

Логика работы системы представлена на рисунке.

Профиль можно использовать как в рамках одной системы, так и переносить в другие системы. Проблема портируемость данных не нова и частично решена с помощью стандарта APML-языка разметки профиля внимания, который представляет собой описание данных на основании языка XML и содержит предпочтения пользователя. Использование внешней информации о пользователе в формате ePortfolio и внутренней информации в формате APML позволяет достаточно точно оценить студента с точки зрения его предпочтений, навыков и компетенций и предоставить ему релевантные рекомендации учебных материалов. Под релевантностью в данном контексте понимается глубина пересечения рекомендуемых учебных материалов с потребностями и индивидуальными особенностями студентов.

Как показано выше, существует множество входных данных для рекомендательной системы, следовательно, у каждого рекомендованного объекта существует некое основание, т.е. иными словами рекомендации разделяются по их основанию на персональные, объектные, социальные и комбинированные. Персональные рекомендации это рекомендации, сделанные на основании профиля пользователя, т.е. на основании его внешней и внутренней активности относительно системы. Объектные рекомендации основываются на самом объекте, выбранном пользователем. Например, студент несколько раз перешел по ссылке на учебник по электродинамике, что является поводом для системы сделать предположение о том, что студент заинтересован в этом разделе физики и в следующий раз студенту будет рекомендована ссылка на статью по элек-

тродинамике. Социальные рекомендации формируются на основании истории поведения пользователей со схожими интересами. Комбинированные рекомендации включают все приведенные выше основания [4].

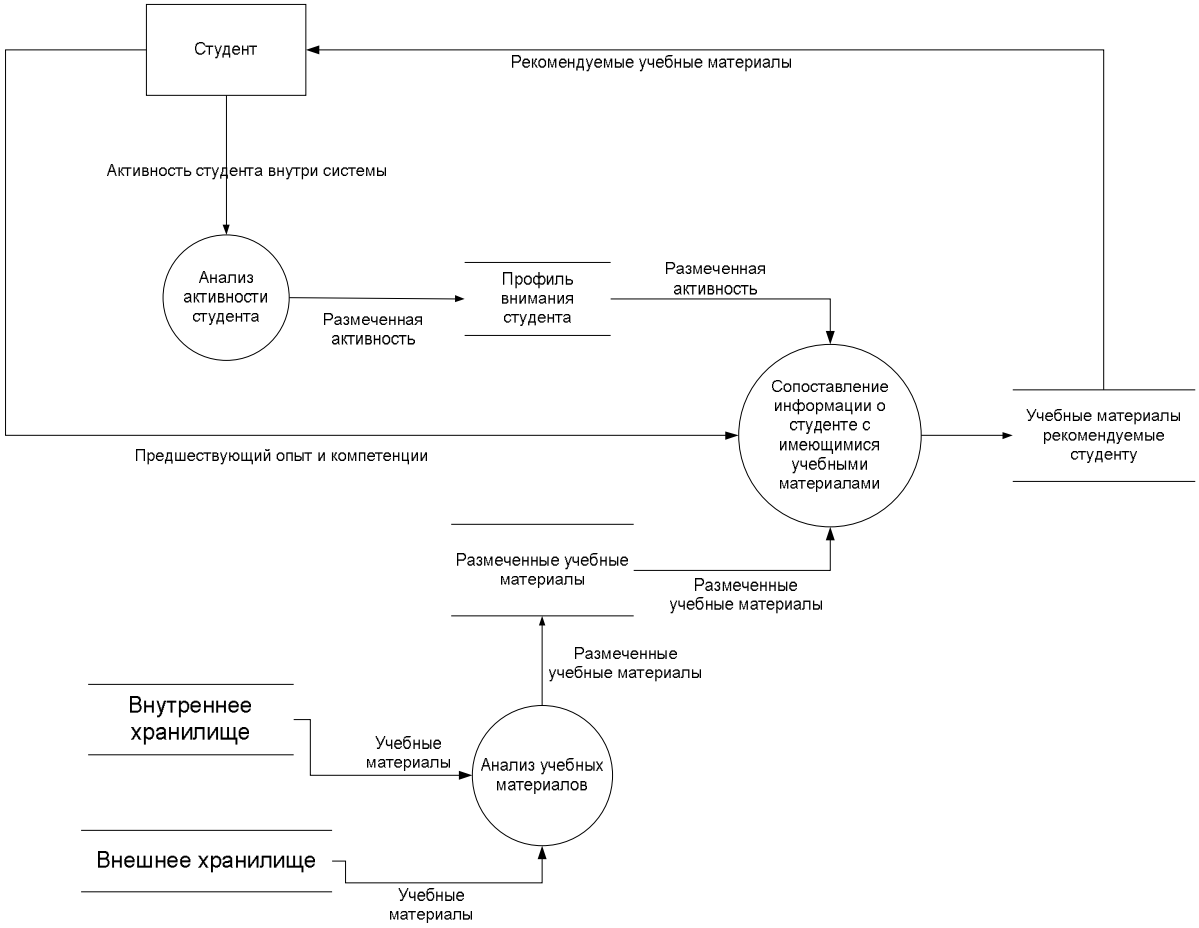


Рисунок. Рекомендательная система

Заключение

Результатом исследования является проект рекомендательной системы, в которой оценка предпочтений пользователей складывается из профиля студента, содержащего различную информацию о его предпочтениях, в формате APML и внешней относительно системы информации в формате ePortfolio, содержащей историю обучения пользователя, его навыки, знания и компетенции. Стоит отметить, что оба формата предполагают свободное перемещение в рамках ряда систем поддерживающих эти стандарты и являются собственностью студента, который сам принимает решение о предоставлении этих данных той или иной системе. Настоящий подход позволяет наиболее точно оценивать потребности студента в учебных материалах за счет анализа большого количества входных данных, покрывающих многие аспекты учебной активности студента. Качество рекомендуемых учебных материалов в большой степени зависит от методов анализа собранной информации, которые являются темой дальнейших исследований.

Литература

1. Alex Iskold Continuous Partial Attention: Software & Solutions [Электронный ресурс] / Read Write Web; The editor and publisher, MacManus R. – Электрон, дан. – SF.: Read Write Web, 2008. – Режим доступа:

http://www.readwriteweb.com/archives/rethinking_recommendation_engines.php, свободный. – Загл. с экрана. – Яз. англ.
2. Jameson, Adaptive interfaces and agents. Mahwah, NJ, USA: Lawrence Erlbaum Associates, Inc., 2003. – PP. 305–330.
3. Широков А.В. Разработка модели информационного портрета пользователя для персонифицированного поиска: тез. докл. Конкурс научных проектов в области информационного поиска «Интернет математика». – Екатеринбург. – 2007.
4. Cristobal Romero, Sebastian Ventura, Jose Antonio Delgado, Paul De Bra Personalized Links Recommendation Based on Data Mining in Adaptive Educational Hypermedia Systems. – Spain: Eindhoven University of Technology. – 2007.

УДК 004.413

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ ПОДДЕРЖКИ КОНТАКТОВ ВЫПУСКНИКОВ С ПОТЕНЦИАЛЬНЫМИ РАБОТОДАТЕЛЯМИ НА БАЗЕ САЙТА КЛУБА ВЫПУСКНИКОВ УНИВЕРСИТЕТА ИТМО

Е.И. Михайленко
Научный руководитель – д.ф.-м.н., профессор Ю.Л. Колесников

Рассмотрены вопросы организации информационной поддержки контактов выпускников с потенциальными работодателями на базе сайта клуба выпускников Университета ИТМО.
Ключевые слова: работодатели, соискатели, трудоустройство, рекрутинг, информационная система

Введение

Санкт-Петербургский государственный университет информационных технологий, механики и оптики является уникальным «оптико-компьютерным» ВУЗом. Такое уникальное сочетание и большая международная известность вызвали у множества отечественных и зарубежных вузов и фирм большой интерес к Университету. Многие выпускники работают в престижных и известных компаниях. Но этот процент выпускников не достаточно велик. Некоторые специальности, на которых обучаются студенты нашего Университета являются достаточно редкими, такие как лазерная техника и лазерные технологии, фотоника и оптоинформатика, приборы и системы ориентации, стабилизации и навигации и другие. Но это не уменьшает спрос специалистов в этих областях. Со стремительным развитием оптической, лазерной, компьютерной техники необходимость квалифицированных специалистов только возрастает. Но как показывает практика, далеко не всегда выпускник может легко найти своего работодателя, тем более, если выпускник ищет работу по своей специальности. Возникла необходимость организовать информационную поддержку связи между выпускниками, аспирантами и старшекурсниками Санкт-Петербургского государственного университета информационных технологий, механики и оптики и фирмами, заинтересованными в найме на работу молодых специалистов Университета. Такая система тесного сотрудничества позволит обеспечить оперативную и максимально простую связь выпускников с потенциальными работодателями. Целью данной работы является организация информационной поддержки контактов выпускников и старшекурсников с потенциальными работодателями на базе сайта выпускников Университета ИТМО.

Разработка логической структуры

Планируется разработать структуру раздела «Трудоустройство» на сайте клуба выпускников Санкт-Петербургского государственного университета информационных технологий, механики и оптики в соответствии с техническим заданием к разработке. Структуру раздела можно описать следующим образом:

1. Общая информация.
2. Регистрация:
   - анкета для работодателя;
   - анкета для соискателя.
3. Вход в раздел:
   - раздел для работодателей:
     - редактировать регистрационные данные;

- разместить вакансию;
- список резюме;
- поиск резюме;

- раздел для соискателей:
  - редактировать резюме;
  - разместить резюме;
  - список вакансий;
  - поиск вакансии;
  - полезная информация.

4. Контакты.
5. Компании.

Необходимо организовать информационную поддержку связи выпускников с потенциальными работодателями, значит необходимо создать такие условия их взаимодействия, при которых данная связь будет оперативна, максимально проста и удобна для обоих сторон.

Разделы общей информации, контактов, каталога компаний и подраздел полезной информации должны быть информационными. В них должна содержаться только лишь текстовая информация.

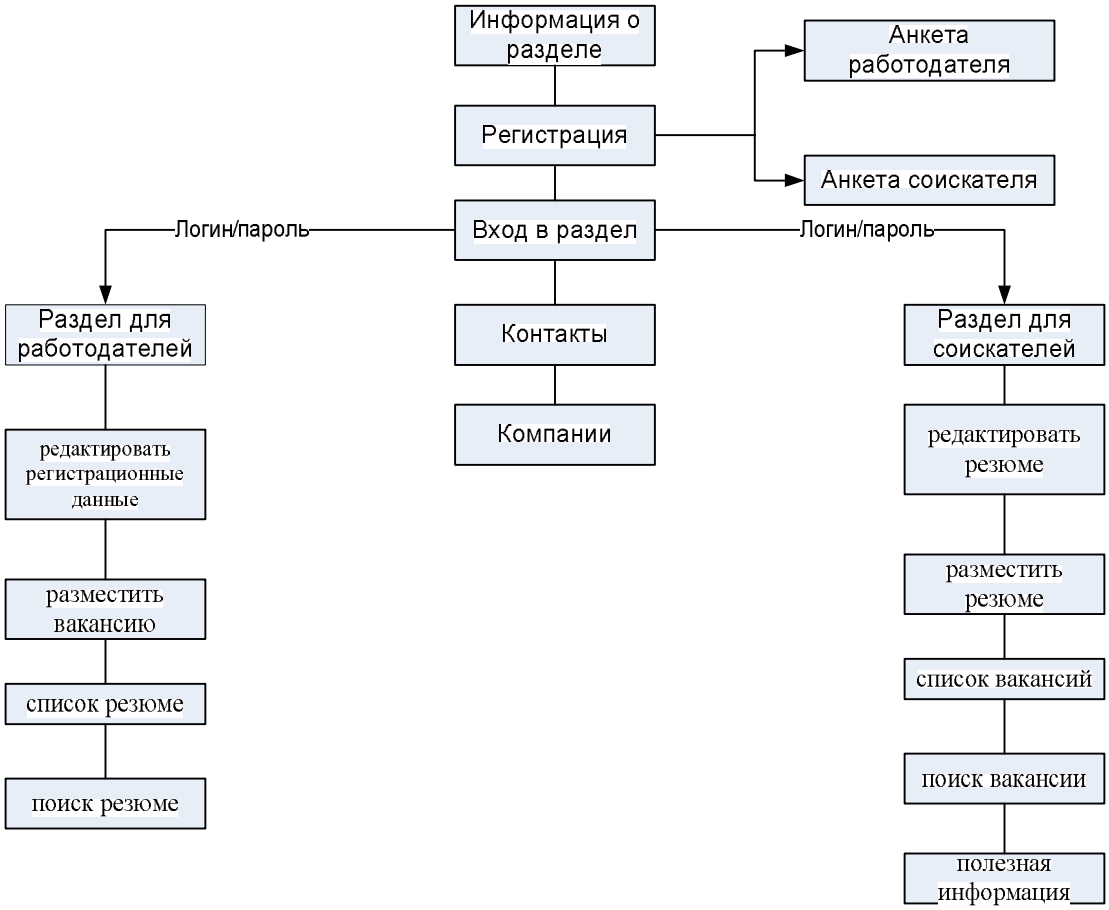


Рис. 1. Структура раздела «Трудоустройство»

Основные требования к структуре базы данных должны налагаться хранимой в ней информацией. Однако также должны соблюдаться требования построения реляционных баз данных.

Объектом хранения данной базы данных будет является информация о соискателе, т.е. о выпускнике. Необходимые поля информации для уникального описания объекта, имеющие отношение к его принадлежности к СПбГУ ИТМО:

- Фамилия Имя Отчество.

- Год выпуска.
- Специальность.

Совокупность этих полей однозначно должны описывать находящийся в базе объект и наиболее полно соответствуют концепции хранимой информации, что позволит уменьшить возможность случайного дублирования информации. Очевидно, что по этим полям удобнее всего и нужно будет делать поиск, как конкретного человека, так и совокупности людей.

Конечно, должны существовать еще некоторые поля информации, которые будут определять отношение объекта к концепции базы данных. Однако выбор именно этих полей будет обусловлен реальной информацией, предоставленной на момент написания данной программы.

Поля, которые не определяют отношение пользователя к выпускникам ИТМО и, соответственно, не хранится в архивах. Такой информации очень много, но можно выделить некоторую, соответствующую общей концепции системы:

- год рождения;
- e-mail-адрес;
- контактная информация;
- дополнительная информация.

При регистрации пользователя он должен будет заполнить анкету соискателя. Заполнение поля e-mail-адреса является обязательным, так как в дальнейшем email-адрес будет использоваться как логин пользователя для входа в раздел. Остальная дополнительная информация заполняется по желанию. Поле «Дополнительная информация» является самым информативным. В него будет помещаться персональная информация о соискателе и также ссылки на информацию в сети, сформированная на основании предоставленной информации.

Основные требования к структуре базы данных налагаются хранимой в ней информацией. Однако также должны соблюдаться требования построения реляционных баз данных.

Создание раздела «Трудоустройство» подразумевает под собой также разработку системы удаленного доступа для управления базой.

Объектом разработки является система удаленного управления базой данных раздела трудоустройства сайта клуба выпускников ИТМО посредством HTTP запросов в среде Интернет. Вся работа с базой данных будет производиться удаленно, что налагает повышенные требования к скриптам управления и системе безопасности базы данных.

Заключение

Структура раздела «Трудоустройство» спроектирована таким образом, что она сможет предоставить пользователю – соискателю работы возможность ознакомления с фирмами, сотрудничающими с ВУЗом, также возможность размещения своего резюме, возможность поиска вакансии, а также ознакомления с полезной информацией при трудоустройстве. Организации, заинтересованные найме на работу молодых специалистов из СПбГУ ИТМО, желающие сотрудничать с ВУЗом имеют возможность размещение информации о себе, возможность размещения вакансии и поиска резюме выпускника по критериям, а также просмотра всех имеющихся вакансий. Таким образом, благодаря данному проекту станет возможна быстрая связь между выпускниками СПбГУ ИТМО с потенциальными работодателями. На этой платформе перспектива повышения показателя трудоустройства выпускников становиться осуществимой. Данный показатель очень важен для такого ВУЗа как Санкт-Петербургский государственный университет информационных технологий, механики и оптики.

Литература

1. Аргерих Л., Чой В., Коггсхол Д. «Профессиональное PHP программирование», 2-е издание.– Пер. с англ.– СПб: Символ-Плюс, 2004. – 1048с., ил.
2. Аткинсон Л. «MySQL. Библиотека профессионала»: пер. с англ. – М.: Издательский дом «Вильямс», 2004. – 624. ил.
3. Бабайцев И.В., Варенков А.Н., Потоцкий Е.П. Учебное пособие по разделу «Безопасность жизнедеятельности и экология» в дипломной работе. – М.: МИСиС.
4. Бек К., Фаулер М. «Экстремальное программирование: планирование. Библиотека программиста». – СПб: Питер, 2003. – 144 с.: ил.
5. Васюхин О.В., Голубев А.А., Кустарев В.П., Тюленев Л.В. Экономическая часть дипломных разработок: Методические указания для студентов технических специальностей всех форм обучения / СПб: СПбГИТМО(ТУ). – 1998.
6. Григин И. «PHP 4». Специальный справочник. – СПб: Питер, 2003. – 672 с.

УДК 004.91

РЕШЕНИЕ ЗАДАЧИ СТРУКТУРИРОВАНИЯ МАТЕРИАЛОВ ЖУРНАЛА «НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК» НА ОСНОВЕ ПОСТРОЕНИЯ ОНТОЛОГИИ

Е.Ю. Ермакова, Г.О. Котелкова
Научный руководитель – к.т.н., доцент Н.Ф. Гусарова

Статья посвящена сравнительно новому виду развития информационных технологий – семантическим технологиям. Одним из направления развития семантических технологий являются онтологии, призванные заменить традиционно используемые рубрикаторы и классификаторы при решении задач структурирования и представления материала. В статье, как пример, рассмотрен процесс создания онтологии журнала «Научно-Технический Вестник».

Ключевые слова: информационные технологии, семантические технологии, онтология, структурирование материала

Введение

Журнал «Научно-технический Вестник» адресован студентам, преподавателям и научным сотрудникам и содержит научные и методические статьи, посвященные различным областям техники, науки, образования. На сегодняшний день электронные версии материалов, представленные в сети Интернет, структурированы по дате выхода номеров журнала. Такая организация недостаточно функциональна (кроме случая, когда необходимо найти конкретную статью), так как пользователю приходится самостоятельно искать необходимую информацию, просматривая каждый из выпусков журнала. В связи с этим встала проблема поиска нового решения для структуризации и организации Web-представления материалов журнала «Научно-технический Вестник» для обеспечения удобного и эффективного использования.

Построение онтологии журнала «Научно-технический вестник СПбГУ ИТМО»

Специфика материалов журнала такова, что один и тот же термин (группа терминов) может встречаться в нескольких статьях различного характера, в различном контексте. Поэтому использование традиционных классификаторов или рубрикаторов на основе деревьев не подходит, так как при такой организации материал включен только в один раздел, категорию, что затрудняет поиск нужной информации. Если пользователь плохо представляет себе, в каком именно разделе находится нужная ему статья, то процесс её поиска может оказаться достаточно долгим, а иногда и не плодотворным.

Для решения сложившейся проблемы, в первую очередь, необходим переход к семантически значимому представлению информации. Одним из направления развития семантических технологий являются онтологии, представляющие собой спецификацию отдельно взятой предметной области, которая включает словарь указателей на термины данной области и логические выражения, которые описывают, что эти термины означают и как они соотносятся друг с другом [1]. Таким образом, обеспечивается фильтрация и классификация данных, индексирование собранной информации, организация общей терминологии.

На первом этапе были обработаны все имеющиеся на тот момент печатные версии выпусков журнала в количестве сорок один выпуск. Каждый выпуск содержит в среднем около тридцати двух статей. Для каждой статьи были определены ключевые слова, в среднем, количество ключевых слов для одной статьи составило около семи понятий.

На следующем этапе необходимо было разработать классификацию и построить иерархию классов [1]. Для этого был проведен обзор и анализ электронных ресурсов ведущих ВУЗов страны (Бауманского технического государственного университета, Екатеринбургского государственного университета, Томского государственного университета, Новосибирского государственного университета, Таганрогского государственного университета, Дагестанского государственного университета), а также был рассмотрен образовательный портал window.edu.ru. По результатам проделанной работы решено было организовать классификацию классов на примере портала window.edu.ru.

Разработанная онтологическая структура представлена в соответствие со стандартом онтологического исследования IDEF5. Для поддержания процесса построения онтологий в IDEF5 существует специальный онтологический язык – схематический язык SL (Schematic Language). SL является наглядным графическим языком, специально предназначенным для изложения основных данных рассматриваемой области в форме онтологической информации. Этот язык позволяет естественным образом представлять основную информацию в начальном развитии онтологии. SL основан на построении диаграмм и схем разных типов [2].

Учитывая многоуровневое изложение материалов, используемое в «Научно-техническом вестнике», для визуализации структуры онтологии журнала была выбрана композиционная схема. Композиционная схема является механизмом графического отображения классов онтологии и представляет собой инструменты онтологического исследования по принципу «Что из чего состоит». Такие схемы позволяют наглядно отображать состав объектов, относящихся к тому или иному классу.

Один из разделов полученной онтологии представлен на рис. 1.

Однако, на основе анализа построенной структуры, был сделан вывод о том, что такая классификация неприемлема: учитывая специфику журнала, а именно, преимущественно научно-технический характер его материалов, распределение статей по выделенным уровням классификации будет неравномерным. Например, раздел «Медицина» будет содержать очень малый объем информации по сравнению с разделом «Техника и технологии». Данное обстоятельство проиллюстрировано на рис. 2.

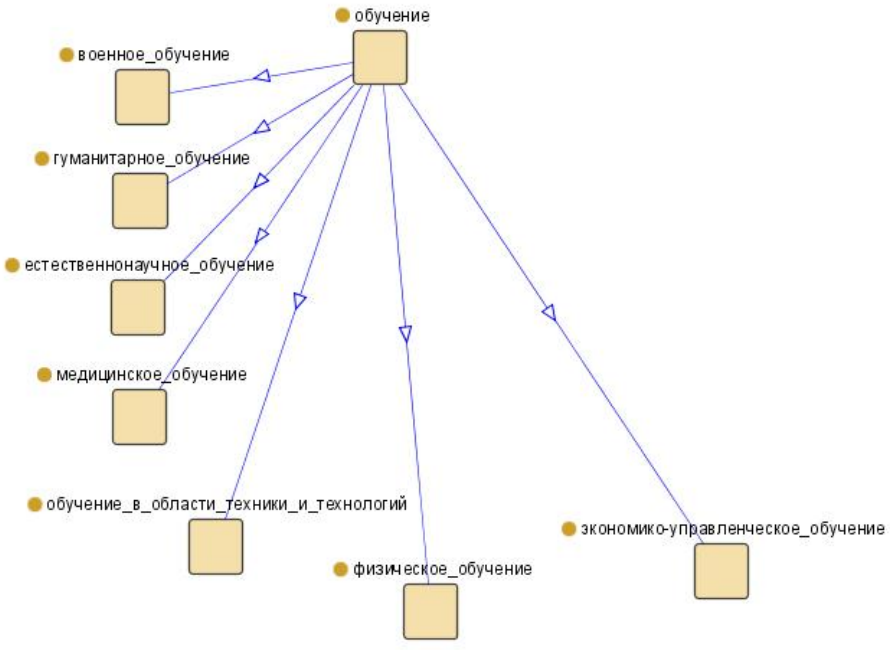


Рис. 1. Структура онтологии

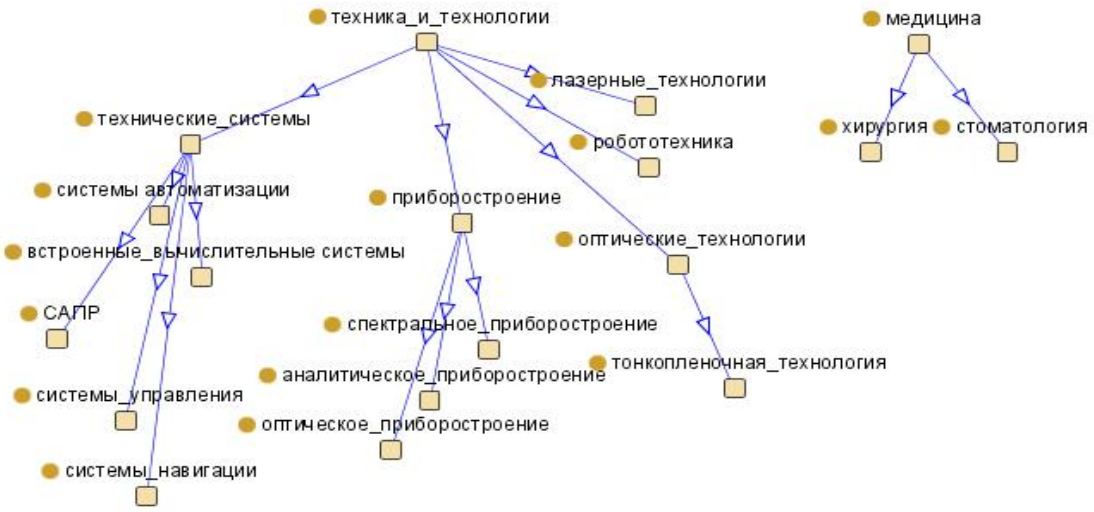


Рис. 2. Описание разделов онтологии

Заключение

Таким образом, дальнейшее развитие работы заключается в решении задачи балансировки полученной на данном этапе базы знаний онтологии: проведении факторного анализа [3], сужении размерности пространства понятий и разработке классификации для полученной области понятий.

Кроме того, так как в рамках онтологии, как показал анализ работы на данном этапе, представлены одновременно несколько предметных областей, имеющих перекрестные связи, то за основу дальнейшего создания онтологии будет взята CYC-идеология [4].

Литература

1. Ontology Development 101: A Guide to Creating Your First Ontology [Электронный ресурс] / The Protégé Ontology Editor and Knowledge Acquisition System – Электронные данные. – Стэнфорд.: Стэнфордский Университет, 2001 – Режим доступа: http://protege.stanford.edu/, свободный. – Заглавие с экрана. – Яз. англ.
2. Integrated Definition Methods [Электронный ресурс] / IDEF Family of Methods – Электронные данные. – East College Station, 2006 – Режим доступа: http://www.idef.com, свободный. – Заглавие с экрана. – Яз. англ.
3. Кельтон В., Лоу А., Имитационное моделирование. Классика CS. 3-е изд. – СПб.: Питер; Киев: Издательская группа BHV, 2004. – 847 с.: ил.
4. Cycorp, Inc. [Электронный ресурс] / Cycorp – Электронные данные. – Техас, 2008 – Режим доступа: http://www.cyc.com, свободный. – Заглавие с экрана. – Яз. англ.

УДК 519.683.8

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ РЕКОМЕНДАТЕЛЬНЫХ СЕРВИСОВ ДЛЯ УПРАВЛЕНИЯ ПРОЦЕССОМ ОБУЧЕНИЯ И ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА НА ПРИМЕРЕ СДО MOODLE

Н.Г. Силич

Научный руководитель – д.т.н., профессор С.К. Стафеев

В статье рассматривается вопрос о поиске требуемой пользователю информации, приводятся существующие варианты и их недостатки. Одним из вариантов решения проблемы является использование рекомендательных сервисов. В их основу положен принцип рекомендации того или иного объекта одним пользователем другому на основе автоматизированного сравнения их профилей предпочтений, базирующихся на выставленных оценках пользователей относительно схожих наборов одних и тех же объектов. Рассматривается вариант создания подобных сервисов в системах дистанционного обучения на основе СДО Moodle.

Ключевые слова: рекомендательный сервис, система дистанционного обучения, облако тегов, поиск по ключевым словам, рейтинг

В настоящее время активно развивается технология web 2.0. Если первоначально контент производился «немногими для многих», а большинство образовательных ресурсов представляло собой статичные сайты с недостатком обратной связи, то на этапе web 2.0. контент (статьи, дневники, видеоролики, фотоальбомы, сборники ссылок и т.п.) создают сообщества пользователей. В связи с ежедневным увеличением объемов информации в Интернет, встает вопрос об эффективном поиске необходимого контента, так как просмотр текстовой и мультимедиа-информации требует времени и дискового пространства в случае, если ресурс не поддерживает функцию просмотра потокового видео- и аудио. Таким образом, пользователю приходится сохранять на жесткий диск все большие объемы информации, тратить больше материальных средств для доступа в Интернет.

На сегодняшний день существует ряд способов поиска информации, но все они имеют существенные недостатки и не гарантируют нахождение нужной информации.

В настоящей статье были проанализированы достоинства и недостатки различных способов поиска информации и предложен иной способ поиска и структурирования информации, в основу которого положен принцип рекомендования того или иного объекта на основе автоматизированного сравнения профилей предпочтений пользователей, – рекомендательный сервис.

На сегодняшний день на практике имеет место реализация стратегии четырех «В» – все, всем, всегда, везде – информационный продукт доступен любому человеку в любой точке в любое время. Одним из вопросов, который встает перед потребителем информации на сегодняшний день, является вопрос выбора требуемой ему информации. Существует возможность использования облака тегов, обозначенным автором, но не все авторы используют тегирование; автор может указать не все теги, имеющие отношения к статье или, наоборот, указать теги, не имеющие отношения к тексту (например, для повышения посещаемости своего ресурса) [1].

Вторым вариантом поиска информации является поиск по ключевым словам. В настоящее время это долгий и трудоемкий процесс, поскольку его результат зависит от выбора поисковой системы и языка запросов каждой из них, а так же от ввода заглавных и строчных символов. Стоит отметить, что не все многообразие ресурсов проиндексировано поисковыми роботами, что сужает область поиска информации. Помимо этого, процесс поиска осложняется предумышленными вредоносными действиями

других пользователей, которые умышленно внедряют в текст Интернет-ресурса ключевые слова, по которым ведется поиск.

Создание рейтингов для сайтов так же не является панацеей от данной проблемы, так как усреднение по типу «хорошо / плохо», «нравится / не нравится» без указания причин – это один из возможных параметров в поисковом запросе, ответом на который станут новые формы автоматизированного спама [2]. Таким образом, в современных условиях, продиктованных обилием информации, существующие способы ее поиска не гарантируют нахождение требуемого контента с должной вероятностью (80% и выше). Кроме этого, отсутствует возможность поиска информации по смежной тематике, которая может быть полезна для пользователя. Так же отсутствует фильтрация по ресурсам, внутри которых осуществляется поиск, который позволил бы отсечь нежелательную информацию.

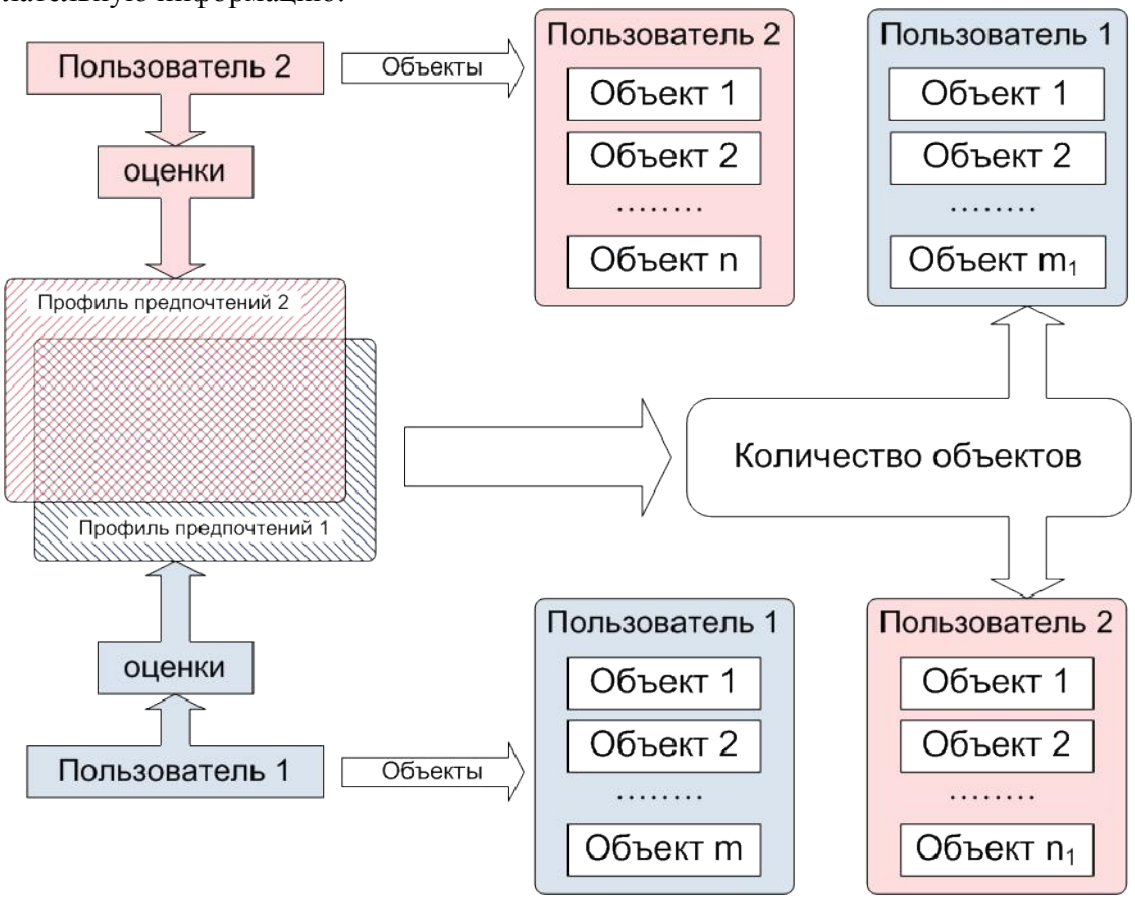


Рисунок. Рекомендательный сервис

Таким образом, становится очевидной необходимость применения социальной рекомендательной институции, в основу которой положен рекомендательный сервис, который существенно облегчит пользователю нахождение интересной и потенциально интересной информации. Рекомендательный сервис – это взаимодействие пользователей между собой, в котором составляется интегральное мнение пользователей о том или ином ресурсе, который в дальнейшем позволяет рекомендовать или не рекомендовать данный ресурс всем остальным пользователям. Интегральное мнение формируется на базе знаний, предоставленных ресурсом и за счет обмена опытом. Для того, чтобы получать рекомендации от других участников сети, пользователю необходимо оценить не менее десяти объектов, создав, таким образом, свой профиль предпочтений. Система должна обеспечивать сравнение профилей предпочтений и отбирать пользователей, выставивших сходные оценки, формируя группу экспертов (рекомендателей) по данной тематике для каждого участника сети (рисунок).

Причем группа экспертов построена таким образом, что в ней оказывается та группа пользователей, которые уже имеют информацию о данном ресурсе и являлись потребителями информации с этого ресурса.

Таким образом, их оценка того или иного объекта может послужить для пользователя прогнозом. Такой принцип предоставления рекомендаций носит название «коллаборативная фильтрация» (от англ. *collaboration* – «сотрудничество»). Он отличается от системы оценок и рекомендаций, принятых в сервисах типа Amazon, где при расчетах учитываются косвенные данные – пользователь, который купил товар А, может купить товар В, – здесь считается, что фактом покупки пользователь выразил свою оценку, хотя купленное и понравившееся не всегда одно и то же [3]. В системах, основой которых является рекомендательный сервис на основе коллаборативной фильтрации, реализован только принцип автоматизированного подбора единомышленников. Таким образом, на практике реализуется принцип «каждому –свое»: можно опубликовать все – пользователи сами отфильтруют то, что сочтут достойным, и систематизируют в соответствии со своими вкусовыми предпочтениями.

Высокая степень автоматизации систем, предоставляющих услуги рекомендательного сервиса, отличает их от ранее предоставляемых сервисов. Таким образом, речь идет уже о web 3.0 – пользователи не только сами создают контент, но и сами его сертифицируют: отмечают то, что заслуживает внимания единомышленников, сообществ, членами которых они являются. Таким образом, рекомендательный сервис – это сеть над сетью, содержащая метаданные о ресурсах, и получившая название «семантическая паутина» [4]. Примерами реализации рекомендательного сервиса являются ресурсы imhonet.ru, superjob.ru, flixter.com, kinopoisk.ru.

Применение рекомендательного сервиса с системах дистанционного обучения предоставит пользователям дополнительные возможности в организации и управлении учебным процессом. В частности, студенты курсов будут иметь возможности:

(1) Получать рекомендации от других слушателей и преподавателей по поводу литературы, обучающих фильмов, программного обеспечения, подкастов, ресурсов Интернет и т.д., помогающих более детально и глубоко изучить предмет, приобрести необходимые навыки и умения, рассмотреть смежные предметные области и т.д., а так же после проверки знаний на основе допущенных ошибок и в случае, если часть материала урока не совсем понятна слушателю (требуются большее количество примеров и т.п.);

(2) Выстраивать свой план обучения на основе опыта других слушателей курсов. После прохождения вступительного теста проверки знаний, студент может сам выстроить свой план обучения, расставив обучающие модули в нужной ему последовательности. Учитывая опыт других студентов курса, расставивших обучающие модули в похожем порядке, студент может сократить время обучения и повысить его результативность.

Помимо этого, применение рекомендательного сервиса в системах дистанционного обучения предоставит преподавателям следующие возможности:

(1) Получать рекомендации от других преподавателей по поводу дополнительных источников информации для корректировки и оптимизации существующего электронного курса;

(2) На основе рекомендательных групп предлагать дополнительные ветки обучения, создание новой учебной группы, создание новых обучающих курсов;

(3) Выстраивать иерархию рекомендательных групп в зависимости от уровня знаний обучающихся. На основе этой иерархии предлагать создание или изменение учебных курсов. Мотивировать слушателей на позицию в группе более высокого уровня, например, учитывая это положение на экзамене.

Необходимо предусмотреть службу, отвечающую за влияние репутации эксперта (аргументировано выставленные оценки). Существует ограничение, связанное с необходимостью наличия более чем трех экспертов по каждой из тематик, и эксперт с наибольшей репутацией должен иметь возможность рекомендовать тот или иной ресурс только на основе своего мнения.

Для реализации рекомендательного сервиса существует возможность выбора одной из стандартных LMS, например, Moodle (модульная объектно-ориентированная динамическая учебная среда). Moodle представляет собой систему управления обучением (LMS) и ориентирована организацию взаимодействия между преподавателем и учениками, организацию традиционных дистанционных курсов, а так же поддержку очного обучения. Данная СДО распространяется бесплатно как open source проект. Благодаря развитой модульной архитектуре, возможности Moodle могут легко расширяться сторонними разработчиками. Таким образом, для реализации рекомендательного сервиса существует возможность создания модуля с последующей его интеграцией с СДО Moodle. В настоящее время ведется разработка этого модуля.

Таким образом, в результате проведенного анализа, было выявлено, что использование рекомендательных сервисов, в частности, в системах дистанционного обучения способно предоставить пользователям дополнительные возможности поиска и улучшения структурирования информации, что с определенной степенью вероятности позволит уменьшить время поиска необходимого и потенциально интересного контента, в результате чего увеличится время на освоение учебного материала и изучение дополнительных источников информации. На основе рекомендательных групп преподаватели получат возможность создавать дополнительные ветки обучения, учебные группы, корректировать имеющиеся и создавать новые учебные курсы.

Литература

1. Anderson P. What is Web 2.0? Ideas, technologies and implications for education. − JISC Technology and Standards Watch, 2007. − 64 с.
2. Долгин А.Б. Web 3.0: Сарафанный интернет [Электронный ресурс]: Ведомости №41 (2063)/ ЗАО Бизнес Ньюс Медиа. – Электрон. текстовые дан. – М.: Издательство ЗАО Бизнес Ньюс Медиа, 06.03.2008. – С. 5–8. − Режим доступа: http://www.vedomosti.ru/newspaper/article.shtml?2008/03/06/143063, свободный. – Электрон. версия печ. публикации.
3. Андреев А.Web 3.0: Менеджеры знаний [Электронный ресурс]: Вебпланета журнал для подключенных / Вебпланета. − Электрон. журн. − Вебпланета, 20.03.2006. − Режим доступа: http://webplanet.ru/news/reading-room/2006/3/20/we_3_0.html, свободный.
4. Андреев А.Web 3.0: Живой поиск [Электронный ресурс]: Вебпланета журнал для подключенных / Вебпланета.− Электрон.журн. − Вебпланета, 26.10.2006. − Режим доступа: http://webplanet.ru/column/service/l_e_x_a/2006/10/26/livesearch.html, свободный.
5. На пути к Web 3.0 [Электронный ресурс]: Business In Web online журнал интернет-бизнеса.− Электрон.журн. − Режим доступа: http://www.businessinweb.com/blog/inteligent/na-puti-k-web-3-0, свободный.

УДК 004.896

ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ОНТОЛОГИЙ И СЕМАНТИЧЕСКИХ СРЕДСТВ В ПРОЦЕССЕ ОБУЧЕНИЯ

Я.И. Поршнев, Н.Г. Силич
Научный руководитель – к.ф.-м.н., доцент М.В. Сухорукова

В статье рассматривается вопрос более эффективного поиска и использования учебных материалов в системах электронного обучения. Одним из вариантов решения данного вопроса является использование онтологий и средств семантической сети при проектировании средств дистанционного обучения. Их использование позволяет увеличить роль компьютера при оценке и обработке информации в процессе формирования программ обучения.

Ключевые слова: семантическая сеть, онтологии, мультиагентная система, система дистанционного обучения, электронное обучение

Текущее состояние сети Интернет характеризуется слабой структурированностью данных и, практически, отсутствием их взаимосвязи. Несмотря на наличие множества всевозможных способов поиска информации, ее извлечения и доставки, отыскать нужную информацию с каждым днем становится все труднее. Современные Web-технологии поиска основаны на полнотекстовом поиске. Все поисковые запросы обслуживаются на основе индекса, содержащего некоторые описания вхождений слов из известных данной поисковой системе документов. При этом возникают различные проблемы – выбора того, что следует индексировать, обеспечения равноправного индексирования всего информационного пространства, а также решения, в контексте каких поисковых запросов следует выдавать ту или иную информацию. Следует подчеркнуть, что в настоящее время компьютеры принимают довольно ограниченное участие в формировании и обработке информации в сети Интернет. Функции компьютеров в основном сводятся к хранению, отображению и поиску информации. В то же время создание информации, её оценку, классификацию и актуализацию продолжает выполнять человек. Как включить компьютер в эти процессы? Если компьютер пока нельзя научить понимать человеческий язык, то нужно использовать язык, который был бы понятен компьютеру. То есть, в идеальном варианте вся информация в Интернете должна размещаться на двух языках: на человеческом языке для человека и на компьютерном языке для понимания компьютера. Эта задача должна быть решена в семантической сети. Слово «семантическая» в данном случае означает «осмысленная», «понятная». Таким образом, семантическая сеть (Semantic Web) – это концепция сети, в которой каждый ресурс на человеческом языке был бы снабжён описанием, понятным компьютеру.

Учитывая всё возрастающее использование компьютерных технологий и сети Интернет в процессе обучения, вопрос применения семантической сети в средствах электронного обучения является на данный момент весьма актуальным и привлекает внимание ряда международных исследовательских проектов.

Цель данной статьи – рассмотреть, в чем может быть полезно использование средств семантической сети и онтологий в процессе дистанционного обучения. Используя эти средства, мы можем улучшить взаимодействие между различными компонентами обучающих систем и более гибко подбирать сценарии обучения для каждого учащегося. В статье рассмотрены некоторые существующие принципы и разработки в данной области и приведены варианты дальнейшего развития.

Одной из проблем в процессе электронного обучения (e-learning) является необходимость выбора подходящих учебных материалов для гибкого создания учебного программы наиболее подходящей конкретному учащемуся. Эта проблема связана с определением и представлением уже имеющихся у человека знаний и желаемого уровня знаний и их использование для формулирования личного учебного плана. Существует

несколько подходов к решению этих вопросов, но всё большую важность сейчас приобретают два из них: использование стандартов (таких как набор спецификаций электронного обучения от IMS) и использование онтологий и средств семантической сети для описания и классификации предметной области [1].

Семантическая сеть или семантический веб – новая концепция развития сети Интернет, принятая и продвигаемая Консорциумом сети (World Wide Web). Автором идеи является Тим Бернерс-Ли впервые использовавший данный термин в статье в 2001 году. Семантическая сеть – это надстройка над существующей сетью, которая призвана сделать текстовую информацию более понятной для компьютеров. Целью этого проекта является внедрение в Web таких технологий, которые позволят существенно повысить уровень интеграции информации, обеспечить развитую машинную обработку данных, дать возможность выдавать более адекватные ответы на поисковые запросы. Семантическая сеть предполагает наличие у любой информации, находящейся в сети, связанного с этой информацией точного смысла, который нельзя было бы перепутать даже в случае совпадения фраз или слов, встреченных в разных контекстах. Фактически это означает, что любая информация связывается с некоторым неотделимым от нее контекстом [2].

В семантической сети можно находить и объединять данные из самых различных источников, а также использовать правила логического вывода для оценки ценности и качества найденных источников, преобразовывать результаты в пригодную для анализа форму.

Фундаментом семантической сети являются три основные технологии:

(1) спецификация XML (eXtensible Markup Language), позволяющая определить синтаксис и структуру документов;
(2) система онтологий, позволяющая определять термины и отношения между ними;
(3) механизм описания ресурсов RDF (Resource Description Framework), обеспечивающий модель кодирования для значений, определенных в онтологии.

В семантической сети используются также другие технологии и концепции, в частности, универсальные идентификаторы ресурсов URI (Uniform Resource Identifier), цифровые подписи, системы логического вывода.

Онтологии определяют термины, используемые для описания и представления знаний той или иной предметной области, в частности – базовых понятий этой области и связей между ними. Можно сказать, что основная цель онтологий заключается в представлении смысла понятий, используемых в конструкциях RDF (фактически, RDF – это язык общения программных систем, работающих в среде Интернет, а онтологии составляют его словарь-тезаурус). Онтология необходима для людей, для приложений систем баз данных и различных других информационных систем, которые совместно используют специфическую информацию в какой-либо предметной области. Онтологии включают доступные для компьютерной обработки определения основных понятий предметной области и связи между ними. Они обеспечивают возможности повторного использования знаний, могут быть использованы для поиска информационных ресурсов в Интернет и управление знаниями в этой среде [3].

Онтология определяет общее соглашение о семантике конкретной области и способствует установлению корректных связей между значениями элементов области, тем самым, создавая условия для их совместного использования. Онтологии используются для поддержки автоматизированного обмена данными и для интеграции приложений, механизмы поиска также применяют онтологии для выборки страниц с синтаксически различными, но семантически одинаковыми словами.

Базовая составляющая онтологии определяет классы объектов и взаимодействие между этими классами. Ключевыми понятиями здесь являются понятия подкласса, су-

перкласса и наследования. Например, класс Студент является подклассом класса Человек (а Человек – суперкласс класса Студент), поскольку для любого объекта, если этот объект является студентом, то он является и человеком. Средствами семантического программирования классы определяются как подмножества наследственно-конечной надстройки, обладающие специальными качествами.

Онтологии используются как механизм выражения и распределения знаний для определения общего словарного запаса и поддержки интеллектуальных запросов в разнообразных базах данных. Онтологии и метаданные описывают организацию и содержание ресурсов.

Онтология кодирует объекты и свойства в понятном для компьютера формате. Конечно, за описанием объектов и их свойств должна лежать простая и понятная логика. С другой стороны эта логика должна иметь строгое определение и корректную семантику, что позволяет делать автоматическую обработку знаний, заложенных в онтологию.

Рисунок. Архитектура мультиагентной системы дистанционного обучения

Основные задачи, которые успешно решаются на базе онтологий, включают предоставление знаний для вывода информации, соответствующей запросу пользователя, фильтрация и классификация информации, индексирование собранной информации, организация общей терминологии, которой могут пользоваться для коммуникации программные агенты и пользователи.

Наряду с использованием онтологий в семантической сети ведутся исследования по переходу от клиент-серверной архитектуры к мультиагентным системам при разработке средств дистанционного обучения [4]. Рассмотрим вариант архитектуры системы, которая не зависит от платформы и предоставляет доступ обучаемым в любое время, с любого компьютера без потери важной информации, собранной системой о них в их профилях.

Чертой данной архитектуры является реализация распределенности и персонализации с помощью мультиагентного онтологического подхода. Распределенность обеспечивается за счет программных агентов территориально рассредоточенных на различных компьютерах. Например, персональные агенты создаются для каждого обучаемого на портале дистанционного обучения, агент-координатор осуществляет управление системой на сервере, на котором хранится текущая информация процесса обучения в виде профилей, а также агент обучающих ресурсов осуществляет доступ к учебным материалам с компьютеров различных поставщиков образовательных услуг (*рисунок*).

Алгоритм функционирования системы при индивидуальном подборе учебного материала с использованием онтологических моделей для работы с профилями обучаемого и обучающего ресурса состоит из следующих этапов:

(1) Посредством web-интерфейса производится регистрация пользователя в системе. Персональный агент собирает необходимые данные о пользователе и на основе этих данных и онтологической модели обучаемого создает профиль с информацией о человеке, упорядоченной в соответствии с используемыми стандартами. Получившийся профиль сохраняется в системе для дальнейшего использования.

(2) Агент-координатор, используя профиль обучаемого и онтологические модели обучающих ресурсов, формирует запрос на получение профилей учебных материалов PR.

(3) Агент обучающих ресурсов на основании полученного запроса проводит поиск метаданных учебных ресурсов, формирует и передает агенту-координатору профили учебных материалов.

(4) Агент-координатор производит анализ на основе пересечения профилей обучаемого и учебных материалов и формирует запрос на получение необходимых учебных ресурсов

(5) Агент обучающих ресурсов в соответствии с запросом формирует множество учебных материалов и передает их агенту-координатору

(6) На заключительном этапе агент-координатор передает персональному агенту учебные материалы для отображения обучаемому.

Для реализации подобных систем и более успешного использования принципов семантической сети помимо развития средств описания онтологий требуется дальнейшее развитие стандартов и спецификаций в области дистанционного обучения, касающихся единообразного представления информации об учебных материалах и обучаемых. Надо отметить, что развитие принципов семантической сети и спецификаций в области электронного обучения осуществляется не раздельно, а активно взаимодействуя между собой [5]. Так при разработке онтологий для улучшения взаимодействия и повторного использования часто принимают во внимание существующие стандарты и спецификации. Сами же онтологии позволяют более четко формализовать предметную область, что помогает в последующем создавать более проработанные стандарты.

Таким образом, в результате проведенного анализа, были выделены возможности использования семантической сети и онтологий в области электронного обучения для создания и более гибкого использования учебных ресурсов при формировании учебных программ, учитывающих персональные характеристики пользователей. Применение подобных принципов при проектировании систем дистанционного обучения могут обеспечить более высокую степень взаимодействие систем, более быстрый и точный поиск нужных материалов, их повторное использование.

Литература

1. Todorova C., Stefanov K. Selection and use of domain ontologies in Learning Networks for Lifelong Competence Development. [Электронный ресурс]: Proceedings of International Workshop in Learning Networks for Lifelong Competence Development, TEN-Competence Conference. March 30th-31st, Sofia, Bulgaria – Режим доступа: http://dspace.ou.nl/bitstream/1820/762/1/Paper25.pdf, свободный.
2. Мальков М.В. Технологии семантической сети и дистанционное обучение [Электронный ресурс]: Образовательные технологии – Электрон.журн. – Образовательные технологии, 2007 – Режим доступа: http://www.naukapro.ru/ot2007/1_003.htm, свободный.
3. Мальков М.В. Онтологии в учебном процессе [Электронный ресурс]: Образовательные технологии – Электрон.журн. – Образовательные технологии, 2007 – Режим доступа: http://www.naukapro.ru/ot2007/3_003.htm, свободный.
4. Келеберда И.Н., Лесная Н.С., Репка В.Б. Использование мультиагентного онтологического подхода к созданию распределенных систем дистанционного обучения. [Электронный ресурс]: Образовательные технологии и общество – Электрон.журн. – Образовательные технологии и общество, апрель 2004 – Режим доступа: http://ifets.ieee.org/russian/depository/v7_i2/html/3.html, свободный.
5. Kravčík M. & Gašević D. Leveraging the Semantic Web for Adaptive Education. [Электронный ресурс]: Journal of Interactive Media in Education (Adaptation and IMS Learning Design. Special Issue, ed. Daniel Burgos), 2007/06. – Режим доступа: http://dspace.ou.nl/bitstream/1820/1080/1/kravcik-2007-06.pdf, свободный.

УДК 004.588

ИНТЕРАКТИВНАЯ ДИАГРАММА АББЕ – ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ ДЛЯ ИЗУЧЕНИЯ ПРОБЛЕМ ОПТИЧЕСКОГО МАТЕРИАЛОВЕДЕНИЯ

Е.Е. Селявка
Научный руководитель – д.т.н., профессор С.К. Стафеев

Одна из важнейших традиционных задач оптики – получение изображений, соответствующих оригиналам, как по геометрической форме, так и по распределению яркости. Она решается, главным образом, с помощью разнообразных оптических систем и оптических приборов, для создания которых в свою очередь, используется огромное множество специальных оптических стекол. Все эти стекла, которых насчитывается только в России порядка четырех сотен, обладают уникальными физическими, химическими и оптическими свойствами. Изучение «сухих» цифр не очень интересная задача. В связи с широким применением ЭВМ как одного из инструментов в образовании, было предложено представить данный материал в виде программного продукта, обладающего удобным графическим интерфейсом, возможностью интерактивного взаимодействия и звуковым сопровождением, с целью повышения эффективности обучения.

Ключевые слова: Оптическое стекло, оптическое материаловедение, диаграмма Аббе, показатель преломления, дисперсия, флинты, кроны, информационные технологии, flash, образование

Введение

Для построения качественных оптических систем существенна технология изготовления оптических стекол с требуемыми свойствами. В силу исключительно высоких требований, предъявляемых к современным изображающим системам, естественно, возникла необходимость в изготовлении широкого ассортимента специальных сортов стекол, различных по своим химическим, физическим и оптическим свойствам.

Условия, необходимые для производства широкого класса сортов оптического стекла, появились впервые в середине XIX века в Германии в Иене, где молодой физик Эрнст Аббе, занявшись проблемой оптического приборостроения, сумел вовлечь в свою деятельность две небольшие мастерские: оптическую – Карла Цейса и стекловаренную – Отто Шота [1]. Таким образом, под руководством Аббе возникло первоклассное производство, которое почти целое столетие сохраняло положение мирового монополиста в создании новых оптических приборов и необходимых для них оптических стекол. Со временем количество создаваемых стекол с уникальными свойствами постепенно возрастало. С расширением номенклатуры выпускаемых стекол и применением в качестве стеклообразующих новых веществ возникла задача разграничения стекол на типы, а те, в свою очередь, на марки.

Эта задача была успешно решена Аббе, положившим в основу классификации стёкол модель зависимости основного показателя преломления (n_e) оптического стекла от средней дисперсии (ν_e), позже названной числом Аббе.

В соответствии с классификацией Аббе оптические стекла, имеющие большее значение показателей преломления и малое значение коэффициента дисперсии, располагаются в правой верхней части диаграммы и называются *флинтами*. В свою очередь стекла, имеющие меньшее значение показателя преломления и большее значение коэффициента дисперсии, располагаются в нижней левой ее части и называются *кронами*. Эти две основные группы, на которые делятся оптические стекла, принято обозначать на специальной диаграмме с равномерно возрастающей осью n_e и логарифмически убывающей осью числа Аббе (рис. 1).

Позднее с развитием стекловарения стекла стали классифицироваться внутри групп на типы, а внутри типов на марки. Марка присваивается стеклам определенного типа, имеющим различный химический состав и оптические характеристики.

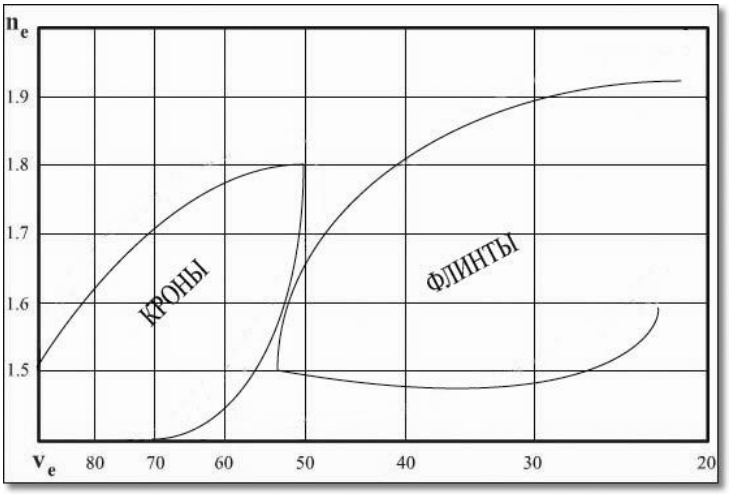


Рис. 1. Диаграмма Аббе, общий вид

Для полного владения светом нужны новые оптические материалы, в том числе, и новые стекла, нужны новые способы их получения.

Благодаря работе ГОИ-ЛенЗОС диаграмма оптических стекол производимых в России на сегодняшний день, насчитывает собой номенклатуру из около 400 марок шестнадцати различных типов, что видно из рис. 2, таблица [2].

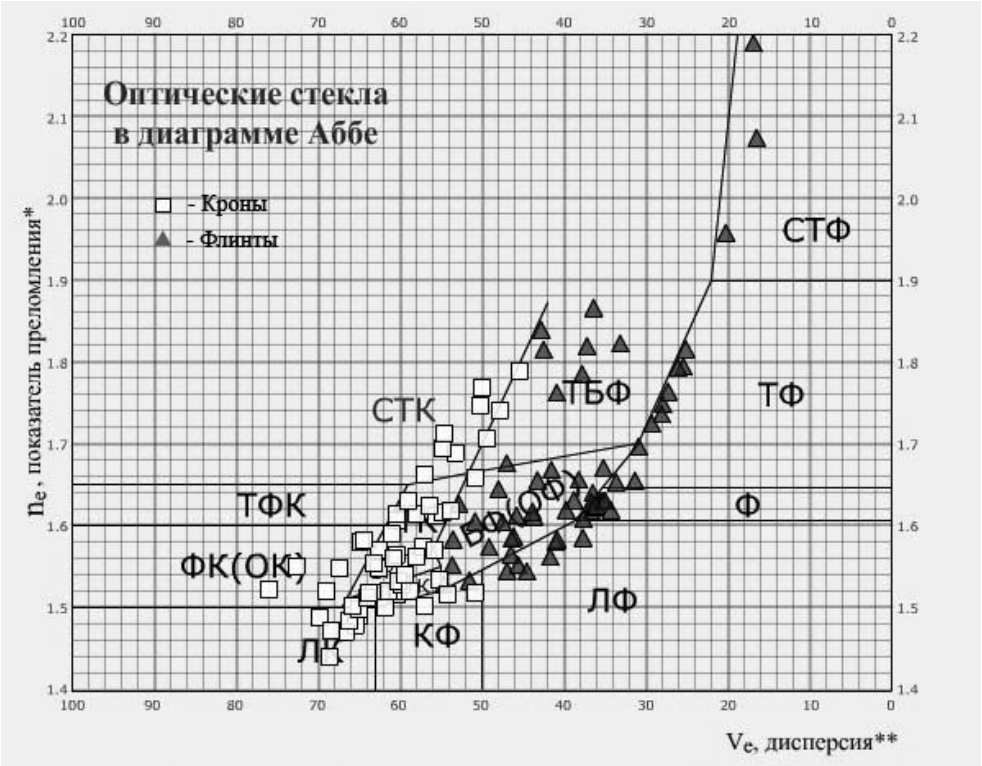


Рис. 2. Диаграмма Аббе, каталог ГОСТ

Изучение диаграммы Аббе является одним из важных учебно-методических разделов, преподаваемых студентам всех оптических специальностей в рамках дисциплины «Оптическое материаловедение». Весьма актуальным является применение современных компьютерных образовательных технологий для повышения мотивации учащихся при освоении этой достаточно трудной и «скучной» темы. По

сути, необходимость изучения будущими оптиками диаграммы Аббе можно сравнить с потребностью изучения химиками периодической системы элементов Д.И. Менделеева.

Легкий крон	ЛК	Кронфлинт	КФ
Фосфатный Крон	ФК	Баритовый флинт	БФ
Тяжелый фосфатный крон	ТФК	Тяжелый баритовый флинт	ТБФ
Крон	К	Легкий флинт	ЛФ
Баритовый крон	БК	Флинт	Ф
Тяжелый крон	ТК	Тяжелый флинт	ТФ
Сверх тяжелый крон	СТК	Сверх тяжелый флинт	СТФ
Особый крон	ОК	Особый флинт	ОФ

Таблица. Типы оптического стекла

Создание обучающей модели «Интерактивная диаграмма Аббе» позволит в удобной графической форме и с элементами интерактивного взаимодействия представить довольно сложный материал по классификации рефракционных и иных свойств различных марок стекол.

Целью данной демонстрационной программы является создание компонента интерактивной музейно-образовательной экспозиции по оптике.

Пользовательский интерфейс модели

Система может функционировать как настольное приложение, для этого достаточно иметь компьютер с любой установленной на него операционной системой и программой flash-плеером.

Благодаря тому, что flash легко интегрируется в web система может функционировать по технологии «клиент-сервер», последняя представляет собой наиболее удачную модель взаимодействия, так как пользователь может получить необходимую информацию из любого места, где есть доступ в Интернет.

Проектирование модели проходило таким образом, чтобы она могла использоваться не только в лекционном процессе, но и при самостоятельной работе студентов.

Вся работа системы, строится на графическом интерфейсе. С его помощью пользователь может наблюдать, осмысливать, непосредственно участвовать во всех процессах системы.

Обязательные элементами графического интерфейса пользователя при решении задачи интерактивности должны быть:

- всплывающие подсказки;
- управляющие кнопки;
- возможность масштабирования модели;
- наличие соответствующего графического и аудио материала на диаграмме.

При запуске системы компьютерная обучающая модель интерактивная диаграмма Аббе, пользователь попадает на главное окно (рис. 3).

Как видно из рис. 3, слева располагается непосредственно сама диаграмма, в осях n_e и ν_e. На диаграмме для осей имеются подписи, градуировка. Внизу системы пользователь может наблюдать небольшое текстовое дополнение, о том какова длина волны для показателя преломления по которому классифицируются стекла, так же подробно расписана формула дисперсии, называемой также числом Аббе.

Справа располагаются шесть управляющих кнопок. Две системные кнопки (звук и картинки) для управления выводом графического и аудио сопровождения на диаграмму. Четыре кнопки для каталогов стекол. Две для каталога ГОСТ, специально

разбитые на группы, кроны и флинты. Две кнопки для основных стеклопроизводящих компаний Shott (Германия) и Hoya (Япония). При клике мышью на соответствующие кнопки, они подсвечиваются, а на диаграмму выводится стекла из выбранных каталогов.

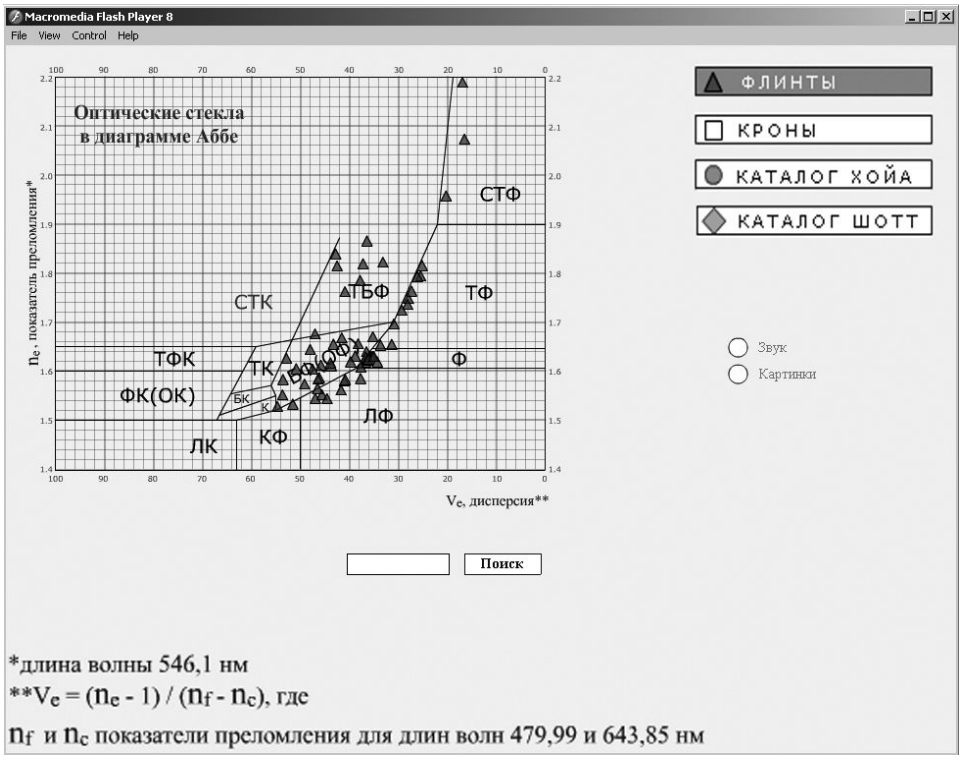


Рис. 3. Главное окно компьютерной модели

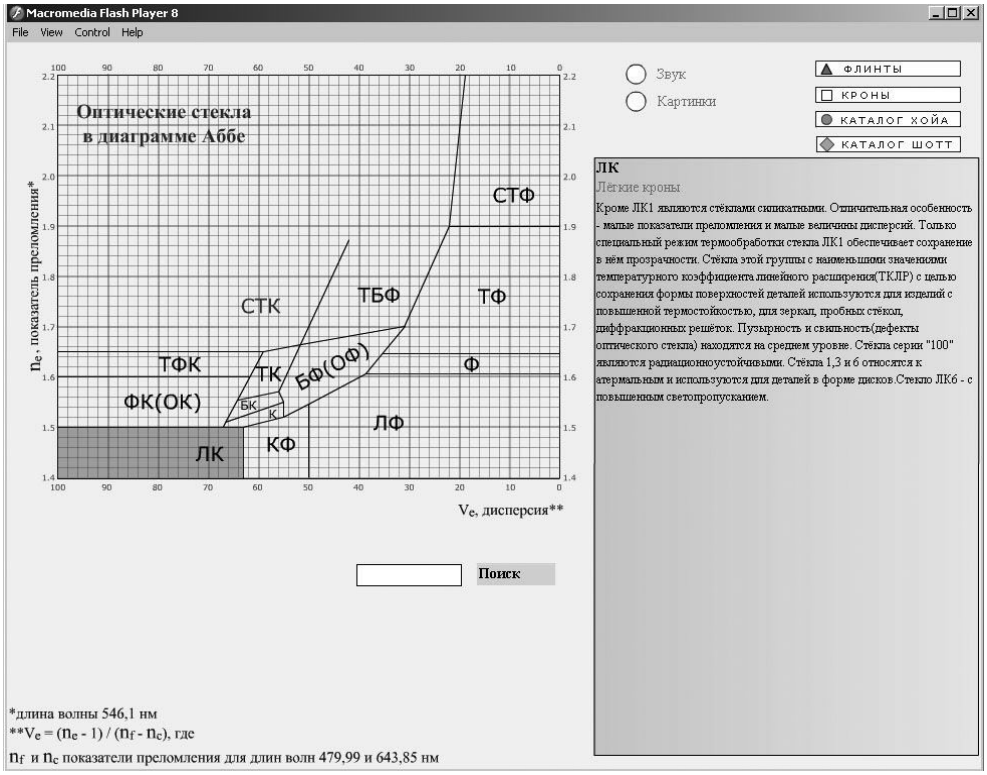


Рис. 4. Всплывающая подсказка при выделении области диаграммы

Для наглядного сравнения стекол предоставляется возможность увеличить любую область на диаграммы. При наведении на соответствующую область справа выводится всплывающая подсказка, в которой дано подробное описание интересующей пользователя группы стекол. Общие свойства этой группы, ее химический состав, применение и.т.п. Эта функция системы продемонстрированы на рис. 4.

Вывод на диаграмму аудио и графического материала осуществляется после того, как нажата соответствующая кнопка в основном окне. Информация выводится только после увеличения интересующей пользователя области. Информация графического характера иллюстрирует какие-либо свойства выбранной группы стекол, а аудио, в свою очередь, проигрывает звуковую дорожку с полным названием выбранной группы стекол.

Заключение

Основная задача модели интерактивность, в качестве инструмента для создания использовался flash. Этот программный пакет специально разработан для создания интерактивных приложений [3].

Ориентация на векторную графику в качестве основного инструмента разработки flash-программ позволила реализовать все базовые элементы мультимедиа: движение, звук и интерактивность объектов. При этом размер получающейся программы минимален, а результат работы не зависит от разрешения экрана у пользователя.

Программа насыщена большим количеством графического и аудио материала, который в свою очередь облегчает процесс восприятия модели конечным пользователем, а пользователем может быть любой человек, программа будет интересна как школьнику, студенту так и человеку, который непосредственно занимается оптическим материаловедением, в качестве справочного материала.

Система в дальнейшем может быть использована:

- Как наглядное пособие по курсу физики «Оптика», для студентов и учащихся старших классов в схеме дистанционного обучения;
- В учебном процессе в качестве иллюстрационного материала.

Литература

1. 50 лет Государственного Оптического Института имени С.И. Вавилова (1918–1968) // Издательство «Машиностроение». Ленинград. 1968. – 707 с.
2. Качалов Н.Н. Стекло. // Издательство Академии наук СССР. Москва 1959. – 465 с.
3. Гурский Д.А. Flash MX 2004 и Action Script: обучение на примерах. // «Новое знание». 2003. – 448 с.

УДК 004.414.28

ПЕРВИЧНАЯ СЕЛЕКЦИЯ ВХОДЯЩЕГО ПОТОКА ЗАЯВОК В РАМКАХ ИДЕОЛОГИИ ITIL (НА ПРИМЕРЕ ОРГАНИЗАЦИИ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ ИТ-СИСТЕМ)

А.Е. Михайленко
Научный руководитель – к.т.н., доцент Н.Ф. Гусарова

В статье рассматриваются вопросы организации подразделения технической поддержки ИТ-систем и первичной селекции в нем входящего потока заявок на обслуживание по уровням поддержки на основе идеологии ITIL.

Ключевые слова: техническая поддержка ИТ-средств, селекция заявок, единая точка доступа, иерархия ролей, должностная матрица ответственности, ITIL

Введение

Развитие современного бизнеса невозможно без поддержки со стороны ИТ-средств. Внедрение ИТ-средств во все этапы бизнес-процессов влечет за собой увеличение числа персонала, вовлеченного в использование компьютерной техники.

Сбои в предоставлении информационных сервисов и неполадки оборудования могут повлечь за собой нарушение функционирования критически важных для компании бизнес-процессов и, в связи с этим, большие финансовые потери, поэтому, существует необходимость поддержки работоспособности ИТ-средств для выполнения операций в соответствии с заданными техническими характеристиками.

Проблемы, связанные с большим контингентом пользователей и широким модельным рядом устройств, с их быстрым развитием и устареванием, требуют специализированной высококвалифицированной технической поддержки и обслуживания соответственно.

Зачастую такая поддержка в организации создается стихийно: входящие заявки нигде не фиксируются, а их исполнение не контролируется. Кроме того заявки могут выполняться на основе межличностных отношений, что может не учитывать интересов бизнеса в целом. Для парирования этих недостатков предлагается рассмотреть рекомендации, изложенные в библиотеке передового опыта в области информационных технологий ITIL [1].

Разработка подходов для первичной селекции потока входящих заявок

При управлении запросами клиентов, согласно ITIL, наиважнейшую роль играет понятие единой точки доступа. Подразделение технической поддержки (ПТП), являясь единой точкой доступа, должно представлять собой последовательный интерфейс между пользователями и техническими специалистами ИТ-отдела [2]. Осуществление взаимодействий в нём должно происходить посредством традиционных видов связи: телефон, e-mail, факс, вэб-форма и др. При этом, успешная работа подразделения поддержки возможна только при четком понимании каждого участника процесса своей роли[1] и ее важности в общем деле.

При создании ролей на этапе проектирования информационной системы по обработке заявок пользователей необходимо исходить из предпосылок о размерах самого предприятия, ИТ-инфраструктуры и ИТ-отдела. Так небольшие и малые организации

[1] Подробнее – книга «Service Support» / Раздел «Service Desk» / Пункт «Service Desk responsibilities, functions, staffing levels etc».

могут использовать схему «одна линия поддержки (операторы) + одна группа реагирования (в данном случае – технические специалисты)».

Для устранения неопределенностей, связанных с отсутствием закрепления должностного функционала за конкретными сотрудниками, в ИТ-системе необходимо организовать систему ролевых функций, которая позволит создать конечную матрицу должностных обязанностей в ПТП и поставить ее в соответствие каждой роли (набору функций) конкретного сотрудника ПТП.

Кроме того, для совершенствования модели обслуживания в ПТП целесообразно организовать динамическое разделение и совмещение ролей в зависимости от состояния базы знаний ИТ-системы и других факторов. Формами такой организации могут являться совмещение ролей и введение второй линии поддержки пользователей. Рассмотрим эти сложные функции управления[2] информационной поддержкой, которые помогают не только повысить эффективность ИТ-инфраструктуры, но и вывести предприятие на более высокий уровень взаимоотношений с клиентами [3, 4].

Совмещение ролей

Такая форма организации может встречаться, например, на начальных этапах внедрения ИТ-системы, когда происходит начальное накопление базы знаний и поток входящих заявок является небольшим [5]. В этом случае технические специалисты (класса «Эксперт») выполняют функции по приему, регистрации и разрешению заявок пользователей, т.е. выполняют функции оператора ИТ-системы и технического специалиста как такового (рис. 1).

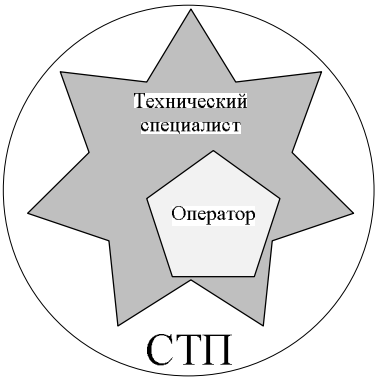


Рис. 1. Пример совмещения ролей

При росте количества сотрудников в компании увеличивается поток заявок, направляемых в ПТП. Это может вызвать задержки в обслуживании вновь поступающих заявок. В такой ситуации становится очевидным, что введение роли оператора разгрузит технических специалистов от выполнения рутинных операций и позволит им заниматься техническими вопросами заявок.

Кроме того, при достаточном накоплении информации в базе знаний, как и в ситуации, описанной выше, целесообразно переложить часть функций на сотрудника с ролью «оператор». Даже не имея высокой квалификационной подготовки в предметной области, он, используя сформированную базу знаний, сможет разрешать входящие заявки и, тем самым, отсеивать поток заявок, решения по которым уже имеются.

Именно эти показатели говорят о необходимости перехода в стадию эксплуатации по схеме «оператор + технические специалисты». Однако при эксплуатации

[2] Сложная функция управления – функция управления (ФУ), основанная на других ФУ.

ИТ-системы происходит усложнение входящих запросов. Эти запросы могут быть не в компетенции оператора, но могут быть разрешены, с большой долей вероятности, более опытными операторами, поэтому, при наличии расширенного штата сотрудников ПТП, рекомендуется введение второй линии поддержки.

Введение второй линии поддержки пользователей

Разделение функций и многоступенчатая обработка входящей заявки предполагает, что задачей команды первой линии является попытка разрешить поступивший запрос либо при первом контакте, либо используя известные обходные решения[3], а также собственные опыт и знания [5]. Если запрос не будет разрешен описанными способами, то будет сформирована заявка и передана в группу реагирования – вторую линию поддержки, которая попытается решить вопрос, а при невозможности это сделать присвоит заявке соответствующие классификаторы и отправит ее в работу к техническим специалистам. Структуры группы реагирования могут различаться в зависимости от конкретного предприятия и быть организованы, например, по платформам и приложениям (группа серверов, десктопов, сетей или баз данных).

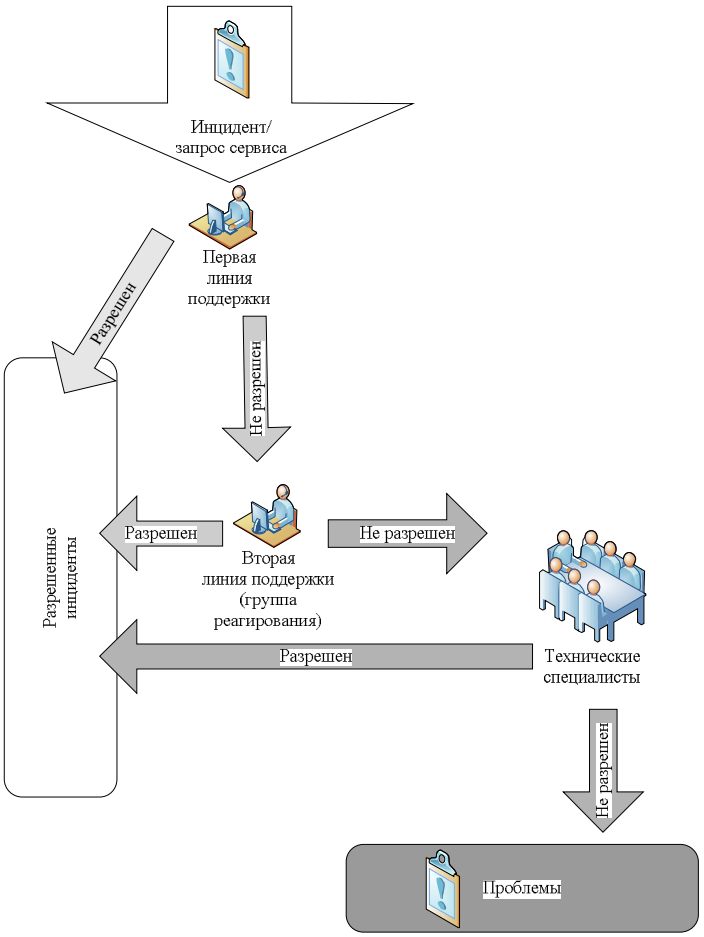


Рис. 2. Рекомендуемая структура службы поддержки

Таким образом, в ИТ-отделе динамично развивающейся компании можно будет выделить 3 ступени поддержки (рис. 2): первая линия поддержки, вторая (группа реа-

[3] обходное решение – временное решение, не устраняющее причины инцидента или проблемы.

гирования) и технические специалисты (заметим, что рекомендации ITIL не запрещают введения и большего числа уровней поддержки).

Следует отметить, что могут возникать ситуации, когда операции по каким-либо функциям могут быть временно переподчинены, переданы или упразднены, а, следовательно, и роли, в чью ответственность входили соответствующие работы. В первом случае снова может возникать совмещение ролей.

Для реализации перечисленных выше форм организации ПТП для селекции входящего потока заявок в системе должны быть предусмотрены механизмы динамического управления ролями:

- механизм для создания и изменения структуры и иерархии ролей в службе поддержки в целях её более эффективной организации;
- механизм динамического изменения роли, который будет использоваться, например, в случае совмещения ролей (роль более высокого уровня иерархии может быть изменена на разрешенную роль более низкого или смежного, для совершения необходимых функций поддержки).

Работа механизма отслеживания позволит контролировать выполнение заявки в разрезе информации о том, кем она была выполнена и в какой роли был исполнитель, а также даст возможность динамически регулировать количество персонала в той или иной роли, выделять новые роли, исходя из потребностей ИТ-инфраструктуры.

Таким образом, создание четкой иерархии ролей и матрицы должностных обязанностей в ПТП позволяет выполнять первичную селекцию входящего потока заявок на обслуживание в ПТП.

Заключение

Использование рекомендаций раздела Service Desk библиотеки ITIL применительно к разрабатываемой ИТ-системе помогает наиболее целесообразно организовать работу в ПТП, распределить работы по ролям и создать четко формализованную матрицу ответственности в привязке к конкретным сотрудникам ПТП, что позволяет осуществлять первичную селекцию входящего потока заявок на обслуживание в ПТП.

Литература

1. The Official ITIL ® Website [Electronic resource]. – Electronic data. – APM Group Ltd., cop. 2007-2008. – Mode access: http://www.itil-officialsite.com/
2. Service Management – ITIL® Version 2. – London.: Office of Government Commerce (OGC): TSO (The Stationery Office), 2000. – 312 pp.
3. ГОСТ Р ИСО 9001-2001. Системы менеджмента качества. Требования. Введ. 31.08.2001. – М.: Госстандарт России: Изд-во стандартов, 2001. – V. – 22 с.
4. ГОСТ Р ИСО 9004-2001. Системы менеджмента качества. Рекомендации по улучшению деятельности. Введ. 31.08.2001. – М.: Госстандарт России: Изд-во стандартов, 2001. – VI. – 48 с.
5. Иванов Р.В., Маятин А.В., Михайленко А.Е. Моделирование процесса обработки заявок в службе технической поддержки сложных технических систем / Научно-технический вестник СПбГУ ИТМО. – 2007. – Вып. 44. Современные технологии. – С. 268–274.

УДК 004.522

РАСПОЗНАВАНИЕ ОТДЕЛЬНЫХ СЛОВ В РАЗГОВОРНОЙ РЕЧИ

К.К. Гладышев
(Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича)
Научный руководитель – д.т.н., профессор Е.А. Шульгин
(Невский институт языка и культуры)

В статье представлено описание системы по поиску ключевых слов в непрерывном речевом потоке. Система является многоуровневой и состоит из нескольких модулей. Выделение информативных признаков сигнала производится на базе аппарата линейного предсказания. Поиск по словарю эталонов выполняется с использованием динамического программирования. Приведены результаты поиска нескольких слов в различных фразах.

Ключевые слова: распознавание речи, линейные спектральные корни, динамическое программирование

Введение

Одной из актуальных задач в области речевых технологий, является поиск определенных слов в потоке разговорной речи. Набор таких слов, как правило, ограничен. Необходимо определить, встречаются ли данные слова в произнесенных фразах, и зафиксировать время начала и окончания их звучания.

Автором статьи разработана экспериментальная система по распознаванию ключевых слов или целых фраз в непрерывном речевом потоке (слитной речи). Система является иерархической, основана на бионической модели восприятия речи человеком [3] и состоит из нескольких взаимосвязанных модулей.

Основная часть

Обрабатываемые речевые сигналы подаются на вход системы в оцифрованном виде. Данная операция выполняется с помощью микрофона и звуковой карты ПК. Очевидно, что использовать представление звука во временной форме для задач распознавания речи неэффективно, т.к. оно не отражает характерных особенностей звукового сигнала. Необходимо наличие блока по выделению эффективных информативных признаков речевого сигнала. К настоящему времени известны различные варианты моделей и методов выделения акустических признаков речевых сигналов. В разработанной системе используется аппарат линейного предсказания [2]. Получаемые признаки – линейные спектральные корни (ЛСК), обладают рядом полезных свойств – они просто рассчитываются, дают компактное представление речевых сигналов, наименее чувствительны к действиям помех и смене диктора. Исходный сигнал разбивается на отрезки (окна или кадры) определенной длины. Кадры перекрываются между собой. На каждом кадре производится расчет набора ЛСК. В результате речевой сигнал представляется в виде массива точек в многомерном пространстве признаков ЛСК.

На первой стадии необходимо провести обучение системы. Диктором записывается набор эталонных речевых единиц (например, слов), поиск которых необходимо будет проводить. Для всех элементов производится расчет наборов ЛСК, данные сохраняются в базе. Система обучена и готова к распознаванию.

Для обеспечения работы системы в режиме реального времени используется накопительный буфер, который позволяет сохранять отрезки сигнала определенной длительности. За это время производится распознавание предыдущего речевого фрагмента.

Таким образом, дальнейшая обработка производится на сигналах конечной длительности. Размер буфера равен средней длительности звучания эталонов из словаря. Для каждого фрагмента входного речевого сигнала производится расчет набора ЛСК.

На следующем этапе для анализируемого речевого фрагмента необходимо провести поиск ближайшего представителя по словарю. Выполняется последовательное сравнение с каждым из эталонов с помощью динамической свертки (или динамического программирования) [1]. Подсчитывается минимальное накопленное расстояние при переходе системы из состояния, соответствующего набору ЛСК одного сигнала, в состояние, соответствующее другому образцу речевого сигнала. При этом учитывается временная последовательность ЛСК. На выходе процедуры сравнения получается некоторое число (мера близости). Чем оно больше, тем более различаются эталон и входной сигнал. В качестве меры расстояния между многомерными векторами сигналов используется Евклидова метрика.

Одним из основных преимуществ динамической свертки является автоматическое масштабирование во временной области для различных по длительности образцов. В случае речевых сигналов, нет необходимости точной подгонки длительности сигналов, четкого вырезания пауз и т.д. Важно, что темп произнесения слов может быть разным, например, отдельные гласные могут тянуться человеком.

Распознанным эталоном на текущем кадре речевого сигнала будет являться тот, до которого подсчитано минимальное накопленное расстояние. Если мера близости превышает определенный порог, значит, на текущем кадре не встречается искомых ключевых слов. Величина порога определяется экспериментально и является настроечным параметром системы.

Временная последовательность анализируемых кадров соотносится с входящим РС. Благодаря этому по результатам сравнения с эталонами определяются границы искомых слов в анализируемой фразе.

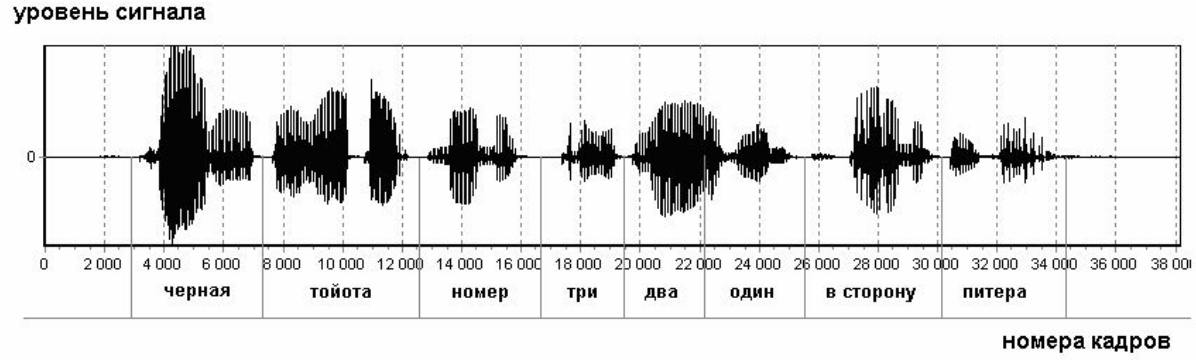


Рис. 1. Временная диаграмма фразы

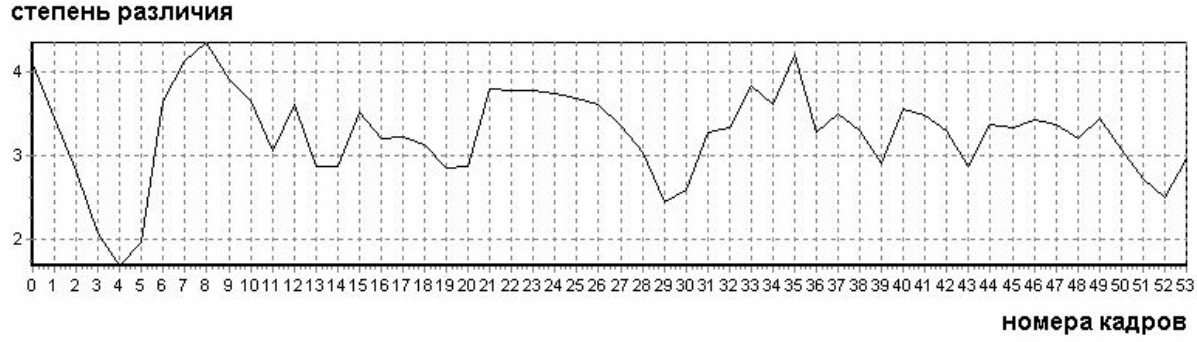


Рис. 2. Поиск слова «черная» во фразе

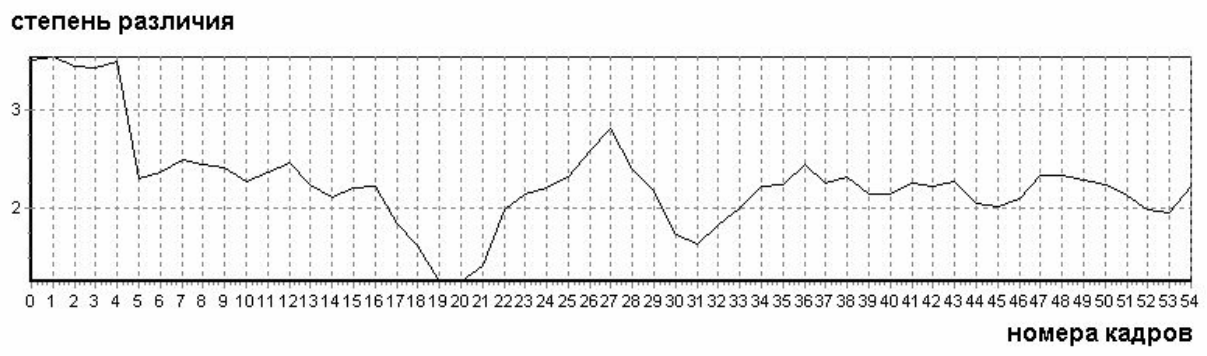


Рис. 3. Поиск слова «номер» во фразе

На рис. 1 представлена временная диаграмма фразы «черная тойта номер три два один в сторону Питера». На рис. 2–3 показаны результаты поиска различных слов в данной фразе. По горизонтальной оси отложены номера кадров, на которые разбивается входящий речевой сигнал, по вертикальной оси значения меры близости до искомого эталона. Видно, что в обоих случаях для искомых слов наблюдаются минимумы.

Заключение

По результатам тестирования системы процент правильно найденных слов составил 90% на словаре из 30 слов. На базе данной системы возможно построение более сложных систем по распознаванию слитной речи. Это потребует существенного увеличения словаря при сохранении должного качества распознавания.

Литература

1. Беллман Р. Динамическое программирование. – М.: Иностранная литература. – 1960.
2. Маркел Дж., Грей А.Х. Линейное предсказание речи – М.: Связь. – 1980.
3. Чистович Л.А. Венцов А.В. Физиология Речи. Восприятие речи человеком. – Л.: Наука. – 1976.

УДК 004.81

УПРАВЛЕНИЕ ПОВЕДЕНИЕМ ИГРОВЫХ КОМПЬЮТЕРНЫХ ПЕРСОНАЖЕЙ НА ОСНОВЕ ОРИЕНТАЦИИ В СИСТЕМЕ ОБРАЗОВ

Д.А. Иванов
Научный руководитель – к.т.н., доцент Т.А. Павловская

Неотъемлемой частью многих компьютерных игр являются персонажи, действия которых определяются самой игровой программой, так называемые «боты». Привлекательность игры, интерес к игре в значительной степени зависит от сложности поведения таких персонажей. Во многих играх действия «ботов» определяются исключительно текущим состоянием игры, соответственно, эти действия легко угадываются игроком. Значительно более сложное поведение компьютерных персонажей обеспечивается, если система управления их поведением прогнозирует развитие событий и выбирает, то или иное действие в зависимости от результатов этого прогноза. В данной работе предлагается построить такую систему управления, на основе моделирования ориентировочно-исследовательской деятельности.
Ключевые слова: компьютерные игры, моделирование поведения, психология, имитация психики

Введение

Постановка задачи. Имеется компьютерная игра, требуется разработать и реализовать систему управления персонажем компьютерной игры с использованием прогнозирования игровой ситуации.

Традиционный подход. Персонажи компьютерных игр могут обладать поведением различной сложности, но выбор необходимого действия осуществляется ими по определенным правилам, исходя из *текущего состояния*. Эти правила могут быть подобраны очень хорошо, и персонаж может произвести на пользователя впечатление адекватного оппонента. Однако, через некоторое время пользователь сможет выявить эти правила, и вести свою игру, учитывая их. Получается, что игрок-человек почти всегда может предсказать ход игрока-компьютера, и игра становится менее интересной.

Предлагаемое решение. Основная идея решения данной задачи заключается в том, чтобы выбирать действие, основываясь на результатах моделирования влияния этого действия на игровую ситуацию, а для управления компьютерным персонажем использовать принципы работы психики сложного животного.

Психологические основы. Поведение животного можно рассматривать как деятельность на основе ориентации в системе психических отражений (системе образов). Это означает, что в нервной системе животного имеется система отражений, как модель окружающего мира. Когда возникает необходимость совершить действие, оно в начале моделируется в системе отражений, и при достижении приемлемого результата выполняется попытка совершить данное действие в реальном мире. В процессе выполнения действия, при необходимости происходит корректировка модели, и в соответствии с этим, корректировка плана действия.

Основная часть

Психологические основы

Данная работа основывается на принципах работы психики сложного животного. Психикой называется особая инстанция в нервной системе, которая выполняет ориентировочно-исследовательскую деятельность.

Обязательной частью психики является психическое отражение действительности. Его функция заключается в составлении активной модели окружающего мира для ори-

ентации в нем. Эта модель обновляется каждый раз, когда в окружающей обстановке произошли какие-либо изменения.

Животное обладает некоторыми потребностями, каждая из которых может вызывать побуждение к поиску объекта удовлетворения этой потребности. Предположим, что образ этого объекта существует в психическом отражении нашего животного. Однако требуется определить – каким образом удовлетворить потребность. Ведь ни образ, ни побуждение не дают ответа на этот вопрос.

«Так, психические отражения действительно открывают новые возможности реагирования, и эти возможности обусловлены тем, что в психических отражениях содержится меньше, чем в их материальных, физиологических основах. Ни побуждения, ни образы не предопределяют конкретное содержание действий, и выяснение этого содержания становится отдельной задачей – одной из общих задач ориентировочно-исследовательской деятельности» [1].

На первый взгляд может показаться, что психическое отражение действительности используется только для выделения объектов удовлетворения потребностей, как карта местности с отмеченными предметами и местами. Однако наиболее важная функция психического отражения – *моделирование* окружающей обстановки и её изменений.

«Очевидно, в центральной нервной системе вместе с «центрами», осуществляющими психическое отражение ситуации, выделяется особый центр, «инстанция», которая представительствует индивида во всех его целенаправленных действиях. Перед ним-то и открывается содержание этих психических отражений. Эта «инстанция» располагает прошлым опытом индивида, получает и перерабатывает информацию о его «внутренних состояниях» и об окружающем его мире, намечает ориентировочно-исследовательскую деятельность, а затем, на основе ее результатов, осуществляет практическую деятельность. Организм с такой центральной управляющей инстанцией – это уже не просто организм, а субъект целенаправленных предметных действий» [2].

Постановка задачи

Реализовать систему управления поведением компьютерного персонажа (бота) на основе принципов работы психики сложного животного. Предыдущее предложение не является строгой формулировкой задачи. В действительности задача разбивается на четыре части:

1) Определение «потребностей» и «анти-потребностей» для компьютерного персонажа в контексте данной игры.
2) Реализация психического отражения игровой действительности бота.
3) Реализация алгоритма нахождения маршрута на евклидовой плоскости.
4) Реализация алгоритма принятия решения.

Реализация решения

Адаптация под контекст игры

Необходимо перевести правила игры на язык потребностей-побуждений. Например, если эта игра относится к жанру военных стратегий, то потребностями игрока будут становиться получение различных ресурсов и уничтожение противников. В то время как «анти-потребностями» будут в данном случае являться потери армий и городов.

Для сравнения результатов различных действий используется функция полезности, оценивающая состояние игры вещественным числом. Вид функции зависит от самой игры, но достаточно часто ее можно представить как линейную комбинацию изменений параметров состояния. Предпложим есть два игрока, и состояние каждого описывается двумя параметрами – X и Y. Пусть параметр X имеет позитивный характер, а

Y – негативный. Другими словами, игроки стремятся увеличить свой параметр X и уменьшить Y, при этом желая оппоненту обратного.

В таком случае функция полезности для игрока 1 будет выглядеть следующим образом:

$$u(p, p_0) = a \cdot \Delta X_1 + b \cdot \Delta Y_1 - a \cdot \Delta X_2 - b \cdot \Delta Y_2$$

или в общем виде:

$$u(p, p_0) = \sum_{i=1}^{n} a_i \cdot (\Delta X_1 - \Delta X_2). \quad (1)$$

Функция полезности оценивает изменение, основываясь на коэффициентах важности a_i параметров состояния.

Нахождение маршрута на евклидовой плоскости

Этот пункт обязателен только для игр, связанных с перемещением игрока в пространстве. На рис. 1 показан принцип работы алгоритма нахождения маршрута на евклидовой плоскости с прямоугольниками в качестве препятствий.

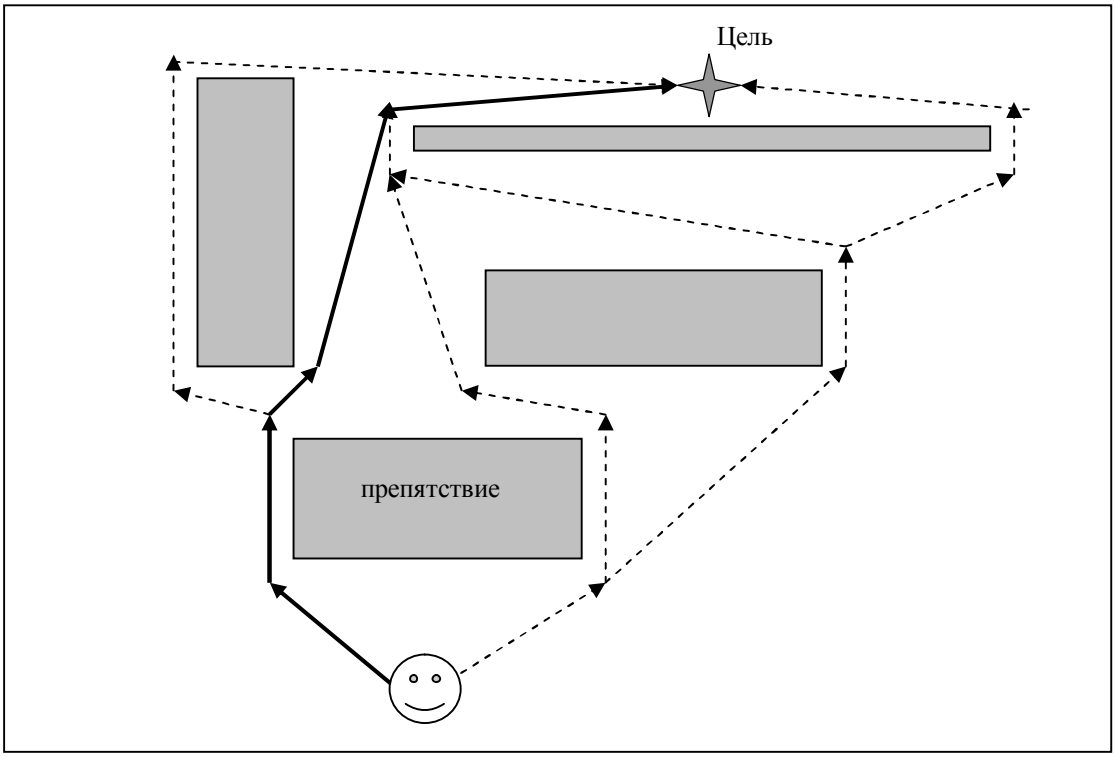


Рис. 1. Иллюстрация к алгоритму нахождения маршрута

В начале строится дерево возможных путей с узлами лежащих напротив вершин прямоугольников-препятствий. Затем определяется кратчайший путь по алгоритму Дейкстры [3].

Реализация психического отражения

Моделью психического отражения может служить упрощённая, ограниченная копия игровой обстановки.

Эта копия постепенно приближается к полной игровой обстановке в результате исследовательской деятельности компьютерного персонажа.

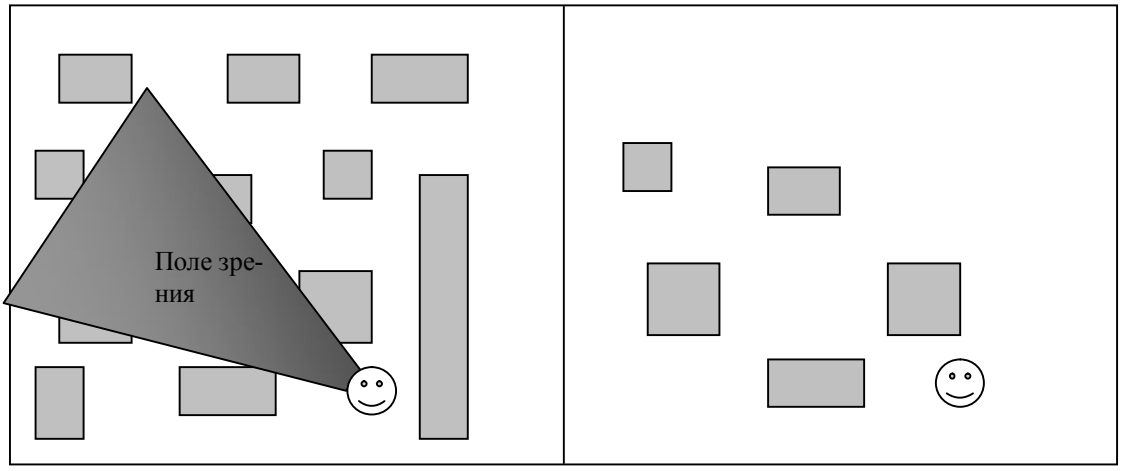


Рис. 2. Игровой мир и его психическое отражение внутри «психики» бота. Бот «видит» только те объекты, которые попали в поле его зрения

Алгоритм принятия решения

Алгоритм принятия решения, включает в себя следующие этапы:

1) ***Обновление системы образов.*** На этом этапе происходит «восприятие» окружающей обстановки ботом. В соответствии с правилами ограничения восприятия бот замечает новые объекты и добавляет их образы в свою систему образов. Далее, для всех образов, в том числе и для образа самого себя, происходит корректировка их состояния (например, координат).

2) ***Оценка внутреннего состояния.*** Бот оценивает параметры своего игрового состояния, и определяет, появились ли у него какие-либо потребности. Если потребность связана с определенным ресурсом, то она появляется при падении уровня запаса этого ресурса ниже установленного порогового значения. Каждая потребность характеризуется своей силой, которая определяется из разницы текущего и необходимого значения ресурса.

$$f_i(p) = \begin{cases} a_i \cdot (\nu_i - p_i), p_i \le \nu_i \\ 0, p_i > \nu_i \end{cases} \qquad (2)$$

где ν_i – пороговые значения *i*-го ресурса.

3) ***Поиск объектов удовлетворения потребностей.*** Для всех потребностей при помощи обновленной системы образов ищется ближайший объект, удовлетворяющий данную потребность.

4) ***Предложение вариантов действий.*** Исходя из результатов поиска объектов в предыдущем пункте, в качестве вариантов действий рассматриваются все возможные последовательности обхода объектов удовлетворения потребностей.

5) ***Выбор варианта с помощью прогнозирования и функции полезности.*** Система образов реализована как ограниченная копия игровой обстановки. Это означает, что образы в системе образов компьютерного персонажа действуют так же, как и объекты в игровой обстановке. Соответственно бот, являясь частью игрового мира, может создать свой собственный «параллельный» мир, который будет состоять из образов объектов, включая образ самого себя. С помощью системы образов и производится прогнозирование ситуации. Каждый вариант действия производится в системе образов. Каждое состояние образа бота, полученное после выполнения последовательности планируемых действий оценивается, с помощью упомянутой функции полезности (1). Она учитывает разницу между значениями параметров состояния до и после выполнения действий. В итоге выбирается и выполняется в иг-

ровой обстановке тот план, после выполнения которого, функция полезности возвратила наибольший результат.

Описание программы

Базовая часть системы

В реализации модуля используется система классов, два основополагающих из них – это «объект» и «вселенная». Каждый объект должен быть зарегистрирован в какой-нибудь вселенной. Объект обладает свойством вложенности – он может находиться внутри другого объекта и сам содержать объекты.

Объекты также могут обладать процессами, за счет которых происходит изменение состояния их владельца во времени. Процессы обеспечивают динамику игрового «мира». Также пары объектов могут быть соединены связями, наличие которых между двумя объектами обуславливает их взаимодействие.

Процессы и связи могут взаимодействовать – процесс может образовывать связь своего владельца с другим объектом, в то же время наличие связи может влиять на определенный процесс. В качестве примера можно привести процесс «движение в пространстве» и связь «столкновение». Движение может вызвать столкновение с другим объектом, но и столкновение может изменить движение.

Структура мира

Миром называется особый объект вселенной, для которого существует понятие времени. Объекты, находящиеся в нем могут изменяться во времени с помощью своих процессов.

Объекты, обладающие поведением

Если объект управляется человеком, то его действия определяются через устройства ввода компьютера. Если же объект – бот, то его поведение должна определять система управления, которая и является основной задачей данной работы.

Описание демонстрационного примера

Описание игры

Для демонстрации данной работы была разработана простая компьютерная игра в жанре Action/Shooter. Главный компьютерный персонаж – танк, выполняет важную миссию – защищает деревни и поселки от кровожадных мутантов, вылезающих из близлежащих торфяных болот. Танк должен ездить по открытой местности, отстреливая врагов. Однако ему необходимо пополнять запасы боевого снаряжения и топлива. Если у танка закончилось топливо или уничтожена хотя бы одна деревня, считается, что он проиграл.

Функция полезности

В данном примере потребностями танка являются:

1) ***Запас топлива (F).*** Принимает вещественные значения от 0 до 1. Нулевой уровень топлива означает проигрыш. Полезность нехватки топлива стремится к $-\infty$ при стремлении запаса топлива к нулю.
2) ***Боеприпасы (S).*** Без боеприпасов танк не может поражать цели, а значит – не может выполнять свое назначение. Однако их отсутствие не фатально, нужно просто съездить на ближайший склад.
3) ***Целостность городов (H).*** Когда мутант все же добрался до поселения, целостность этого поселения постепенно уменьшается. Считается, что мутанту нужно

время, чтобы разрушить всю деревню. Объектом удовлетворения потребности являются те мутанты, которые напали на эту деревню. Соответственно, *действием* будет являться атака.

Из этого можно заключить, что функция полезности в данной игре будет иметь вид:

$$u(p, p_0) = a_F \cdot \log(2F) + a_S \cdot S + a_H \cdot \log(2H). \quad (3)$$

Заключение

Представленная работа, по сути, не является оконченной. Дальнейшее ее развитие будет заключаться в создании системы управления компьютерным персонажем, умеющим играть против такого же персонажа. Это означает, что система образов будет включать в себя модель другого игрока, а значит, бот сможет предсказывать поведение оппонента – как такого же бота, так и человека. Такое расширение делает возможным создание не только ботов-противников, но и ботов-союзников.

Окончательной же целью данной работы, по мнению автора, является моделирование человеческого поведения. Это не означает создание искусственного разума, а только автомата, во многом похожего на человека.

Литература

1. Гальперин П.Я. Введение в психологию: Учебное пособие для вузов. – 4-е изд. – М.: «Книжный дом «Университет», 2002. – 336 с.
2. Гальперин П.Я. Лекции по психологии: Учебное пособие для студентов вузов. – 2-е изд. – М: КДУ, 2005. – 400 с.
3. Мозговой М.В. Занимательное программирование: Самоучитель. – СПб: Питер, 2004. – 208 с.

УДК 004.93'14

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ИССЛЕДОВАНИИ УЧЕБНЫХ ТЕКСТОВ

М.М. Невдах
(Белорусский государственный технологический университет)
Научный руководитель – д.х.н., профессор М.А. Зильберглейт
(Белорусский государственный технологический университет)

В статье рассматривается применение квантитативных методов в изучении текста как статистической совокупности, а также описываются созданные на основе данных методов отечественные и зарубежные программы, предназначенные для анализа и лингвистической обработки текстов. Выделен ряд наиболее актуальных вопросов, требующих более детального изучения: это исследования в области читабельности с использованием информационных технологий и разработка соответствующего инструментария для классификации текстов по ряду областей знаний в зависимости от подготовленности читателя.
Ключевые слова: текст, статистическая совокупность, читабельность, информационные технологии

Введение

С возникновением и развитием ряда наук, в которых центральным объектом анализа выступает текст, подтвердилось предположение о том, что текст представляет собой структуру, элементы которой подчиняются законам, определяющим статистическую упорядоченность и строгую организацию. Точный характер проявляющихся закономерностей, регулярностей в языке в целом крайне сложно уловить без применения математических методов и ЭВМ. Поэтому интерес к квантитативным методам как инструменту научного и практического познания статистических свойств языковых структур повышается и обусловлен объективной реальностью.

Исследование текстов с применением информационных технологий

Текст как статистическая совокупность может быть охарактеризован через множество количественных переменных, на основе которых текст из последовательности символов преобразуется в набор чисел. Особенностью этих переменных является то, что они по определению не отражают глубинных, сущностных сторон текста, они описывают только внешнюю, поверхностную сторону текста. При этом многие исследователи полагают, что формальные признаки каким-то опосредованным, вероятностным образом связаны с содержательной сущностью текста. В связи с этим набор количественных признаков часто является диагностическим при решении конкретной задачи (например, атрибуции текста), что, несомненно, открывает путь для проникновения в глубинную организацию текста, не доступную непосредственному наблюдению.

Замена словесного описания текста его математическим представлением в компьютерной среде позволяет, избежать бесконечного богатства ассоциаций, возникающего при «живом» общении с текстом, и при этом вскрыть характер закономерностей, присущих определенным языковым структурам.

Квантитативный анализ текстов в настоящее время позволяет решать различные научно-практические задачи. В работах, связанных с изучением текстов как статистических объектов, преобладают исследования, направленные на оценку близости и однородности стилей текстов и их классификацию.

Задача проверки близости стилей состоит в том, чтобы сравнить два или более текстов, заданных совокупностью количественных признаков, и установить различие между стилями. После попарного или множественного сравнения стилей есть возмож-

ность установить различие в виде альтернативы «да/нет» либо в виде значения степени различия стилей.

Первая работа в этом направлении принадлежит Т. Менденхоллу [1], в которой автор сравнивает стили текстов произведений различных писателей, написанных как на одном языке, так и на разных. Сравнение проводится на основе гистограмм, которые отражали частоту появления слов с разной длиной.

Похожий подход для сравнения стилей использовал Н.А. Морозов [2]. В качестве признаков стиля исследователь использовал частоту появления наиболее встречающихся слов (предлогов, союзов, частиц). На основании гистограмм распределений данных слов Н.А. Морозов проверял близость стилей.

Среди работ, написанных в последние годы, следует отметить диссертацию О.Г. Шевелева [3], в которой разработаны алгоритмы и инструментарий для сравнения стилей текстовых произведений. В частности, предложены новые подходы для сравнения стилей текстов с использованием гипергеометрического критерия (двустороннего точного критерия Фишера) и критерия хи-квадрат по отдельным частотным признакам текстов, совокупности признаков, а также по их распределению; предложен новый подход к кластеризации текстов с использованием таких мер сходства, как «частота рассогласования» и интегральная мера рассогласования; предложены модификации метода Хмелева классификации текстов по авторскому стилю с использованием для оценки расхождения частот мер Кульбака и хи-квадрат. Автором также создан программный комплекс «СтилеАнализатор» для сравнения стилей текстов.

Смежной по отношению к задаче проверки близости стилей текстов является задача проверки текстов на однородность стиля. Методы проверки текстов на однородность могут использоваться для сравнения стилей, и наоборот.

Наиболее известным методом проверки текстов на однородность авторского стиля является метод накопительных сумм [4], суть которого заключается в том, чтобы выбрать несколько характеристик, являющихся функциями предложения. Например, для английского языка А.К. Мортон использовал длину предложения и число двух- и трехбуквенных слов плюс число слов, начинающихся с гласной буквы. После этого производился расчет этих характеристик для каждого предложения, вычислялись их средние значения. По отклонениям от средних значений для каждого предложения строилась накопительная сумма. Для однородного стиля графики характеристик практически совпадали.

Для проверки однородности текста используется и метод структурного анализа текста, предложенный отечественными исследователями А.Ф. Толочко и Н.И. Миницким [5]. Разработанная авторами математическая модель на основе изучения учебного текста позволяет создать функцию возмущений частоты появлений отдельных букв алфавита на заданной выборке относительно этих же характеристик на генеральной совокупности. В качестве эталона-образца может использоваться норма русского языка или других языков, характеристика стиля автора на генеральной совокупности текста учебника, который признан в педагогическом сообществе образцовым.

Н.С. Закревская в [6] рассматривает подход к проверке однородности, основанный на проверке соответствия числовых последовательностей модели фрактального броуновского движения. Числовые последовательности получены путем замены слов текста на их длины, измеренные в слогах.

Набор алгоритмов, позволяющих производить классификацию и идентификацию изучаемых объектов, в научной литературе принято обозначать термином «распознавание образов». При этом задачей классификации является построение алгоритма классификации, т.е. правила отнесения предъявляемого объекта к тому или иному классу.

Когда в качестве объектов выступают тексты, то наиболее часто исследователи решают задачу классификации текстов по авторству. Среди методов, связанных с атри-

буцией, можно выделить энтропийный метод Д.В. Хмелева [7] и метод О. Хрулева, основанный на использовании частотного словаря [8].

Метод Д.В. Хмелева позволяет с высоким качеством (84%) классифицировать тексты по авторству на основе формальной математической модели последовательности букв текста как реализации цепи А.А. Маркова. Для выбранных текстов вычисляется матрица переходных частот употреблений пар букв. Она служит оценкой матрицы вероятностей перехода из буквы в букву. Автором анонимного текста полагается тот, у которого вычисленная оценка вероятности больше. Существуют и другие исследования Д.В. Хмелева, в которых при разработке методики определения авторства учитываются такие формальные характеристики языка автора, как число служебных слов (предлогов, союзов и частиц), используемые морфемы (приставочные, корневые, суффиксальные, флективные) и их последовательности, сложность используемых грамматических конструкций и собственно словарь, используемый автором. Каждый из параметров использован в модели ЛингвоАнализатора, позволяющей определять наиболее вероятное авторство.

Метод О. Хрулева позволяет классифицировать тексты по авторству на основе сравнения частотных словарей писателей. В словарь входят 10 000 наиболее употребительных слов русского языка. Полученные частоты для каждого писателя делятся на средние частоты в русском языке, взятые из частотного словаря С.А. Шарова. Писатель определяется по наименьшему расстоянию между словарями писателей и словарем анализируемого текста. Расстояние определяется как сумма разностей частот между отдельными анализируемыми словами. Для текстов, участвовавших в формировании словарей, частота правильных классификаций составляет 98%.

Для классификации текстов используются и другие, более сложные методы: нейронные сети; метод опорных векторов; классический дискриминантный анализ; вероятностный классификатор; метод сжатия данных; методы, основанные на извлечении правил (методы накопительного извлечения правил, деревья решений, метод «колонии муравьев»).

Перечисленные подходы и методы позволяют в настоящее время решить ряд вопросов, связанных с систематизацией и изучением текста. Благодаря точным математическим методам открываются возможности для анализа скрытых потенциальных возможностей текста. Наработки в этой области можно с успехом применить во многих сферах, в том числе и редакционно-издательской деятельности. Во-первых, появляется возможность тестировать стили авторского коллектива (в случае, когда несколько авторов пишут одну книгу) на предмет их близости, однородности. Это особенно важно в сфере учебного книгоиздания. Во-вторых, можно проанализировать лингвостатистические характеристики текстов и дать рекомендации по их корректировке. И в-третьих, можно установить атрибуцию текста, что очень важно для текстологической науки. Кроме того, важной является информация и о том, использовал ли автор при написании произведения дополнительные источники (например, сеть Интернет). Это может быть серьезным аргументом при экономических расчетах с автором.

Несмотря на разноплановые исследования в области квантитативного анализа текстов, один из важнейших вопросов остается недостаточно разработанным. Данная проблема связана с оценкой трудности текста для будущих читателей, решение которой будет являться важным шагом в повышении качества подготовки литературы, что имеет особое значение при выпуске учебных изданий.

В отечественной науке в настоящее время практически отсутствуют объективные инструменты для классификации текстов в зависимости от подготовленности читателей. В определенной степени вопросы количественного анализа текстов и выявления факторов, влияющих на усвоение материала, раскрыты в работах, связанных с читабельностью текста [9].

На данный момент существуют компьютерные программы, предназначенные для анализа и лингвистической обработки текстов. Однако следует отметить, что провести всестороннюю обработку текстов в рамках какой-то одной программы невозможно. Каждый программный продукт направлен на решение конкретных прикладных задач.

Одним из наиболее известных продуктов для классификации текстов по авторству является система «ЛингвоАнализатор» Д.В. Хмелева, доступная на сайте автора по адресу http://www.rusf.ru. Программа определяет возможного автора текста (выдает имена трех писателей) среди 128 писателей, заложенных в систему. Кроме того, ЛингвоАнализатор находит три произведения каждого из авторов, которые наиболее близки данному тексту. Применяемая методика определения авторства опирается на математическую модель, в которой учтены формальные характеристики языка автора. Набор авторов, их тексты и признаки авторских стилей для алгоритма заложены в программу. Возможность их изменения со стороны пользователя не предусмотрена.

Информационная система «СМАЛТ» (Статистические методы анализа литературного текста) [10], разработанная в Петрозаводском государственном университете, позволяет произвести настраиваемый анализ от выбора текстов до конечного представления результатов анализа. Блок-анализ состоит из трех основных модулей. Первый модуль ориентирован на выборки из базы данных, основанные на лингвостатистических параметрах (например, общее распределение длины слов и предложений, средняя длина предложения в словах, индекс разнообразия лексики и т.д.). Модуль допускает задание объема выборки, а также проверки статистических гипотез о равенстве средних на основе критерия Стьюдента и проверки данных на однородность при помощи непараметрического критерия Колмогорова-Смирнова. Второй модуль предназначен для реализации методики атрибуции, основанной на изучении закономерности расположения частей речи в рамках предложения. Третий модуль позволяет измерять близость текстов на основе методов кластерного анализа: иерархической кластеризации, метода корреляционных плеяд и т.д.

В автоматизированной системе обработки лингвостатистических данных «ЛинДа» [11], разработанной на кафедре структурной, прикладной и математической лингвистики Санкт-Петербургского государственного университета, решаются следующие задачи:

а) первичная обработка лингвистических данных (построение рядов распределения, вычисление статистик, статистических оценок др.);

б) лексикографическая обработка текстовых данных: создания частотных и алфавитно-частотных словарей, словарей-конкордансов, словоуказателей, обратных словарей, словарей ключевых слов и т.п.;

в) информационно-поисковые задачи, включая поиск текстовых единиц, обладающих определенным набором количественных и качественных характеристик для решения стилистических и грамматических проблем; автоматический поиск текстов (авторский, жанровый, историко-хронологический и др.);

г) систематико-таксономические задачи, включая обработку многомерных данных с использованием стандартных алгоритмических процедур (кластерного, факторного и других методов многомерного анализа); обработку лингвистических данных с помощью специальных лингвистических методов (дешифровочных алгоритмов, методов датировки, атрибуции, диагностики и типологии текстов и др.);

д) теоретико-статистические исследования: изучение статистических закономерностей в символьных последовательностях, изучение проблем устойчивости и вариативности лингвостатистических чисел, проблемы однородности текстов, условий действия закона больших чисел, оптимизация выборочных исследований и др.

Одной из самых мощных систем аналитической обработки, позволяющей работать с текстами, является PolyAnalyst [12]. Основная функциональность программы

предназначена для извлечения знаний из больших баз данных. В аналитический инструментарий системы входят модули для построения числовых моделей и прогноза числовых переменных, алгоритм кластеризации, алгоритмы классификации, алгоритмы ассоциации, модули визуализации данных.

Для работы с текстом в PolyAnalyst предусмотрен модуль TextAnalyst, являющийся средством формализации неструктурированных текстовых полей баз данных. В модуле предусмотрены построение семантической сети понятий, выделенных в обрабатываемом тексте, со ссылками на контекст; смысловой поиск фрагментов текста с учетом скрытых в тексте смысловых связей со словами запроса; анализ текста путем построения иерархического дерева тем/подтем, затрагиваемых в тексте; реферирование текста.

Система DICTUM (система для универсальной обработки и анализа словарей и текстов) разрабатывается и используется лабораторией общей и компьютерной лексикологии и лексикографии филологического факультета МГУ с 1991 г. Эта система позволяет создавать, расширять, сравнивать, объединять словари, осуществлять по ним сложный поиск, включающий грамматические, частотные и другие характеристики, делать привязку словарных статей к определенным местам какого-либо текста. Подсистема обработки текстов производит разметку текстов как признаками, заданными извне (например, название, жанр), так и извлеченными в процессе анализа его внутренней структуры. Подсистема позволяет производить лексический, морфологический и синтаксический анализ. Аналитические инструменты включают в себя морфолемматизатор, поиск повторяющихся фраз, инструмент для пополнения и использования семантических характеристик слов и фраз, и некоторые другие. Среди баз данных DICTUM имеются базы синонимов, омонимов, идиом, тезаурус, морфем, грамматически размеченных слов.

Следует также отметить семейство программных продуктов, выпускаемых под торговой маркой RCO, которое предназначено для решения задач, требующих автоматического анализа текста на русском языке. Разработанное лингвистическое и алгоритмическое обеспечение позволяет решать такие прикладные задачи как составление содержательного портрета текста, извлечение именованных объектов, связей и фактов из массивов неструктурированных данных, анализ тональности текста, выявление заимствований и дубликатов.

Экспертная система «ВААЛ» производит количественный анализ текстов, но для решения психолингвистических задач: прогноза эффекта неосознаваемого воздействия текста на массовую аудиторию, анализа текстов с точки зрения такого воздействия, генерации текста с заданным вектором воздействия, выявления личностно-психологических качеств автора текста. Система позволяет оценивать слова с точки зрения их фоносемантического воздействия на человека; задавать желаемые фоносемантические характеристики текстов и редактировать их в диалоговом режиме с использованием словаря синонимов; производить лексический анализ текстов, оценивая нагрузку на сенсорные каналы восприятия информации; настраиваться на лексически определенные группы людей посредством анализа характерных для них текстов.

Ценным является и отечественный программный продукт «Текстоанализатор», разработанный А.Ф. Толочко и Н.И. Миницким [5]. Среди функций программы можно отметить следующие: возможность точного математического описания авторского речевого стиля; наличие методов и процедур, позволяющих корректировать авторский стиль и обеспечить его единообразие по всему тексту; наличие технологии создания норм любых языков на основе кириллицы либо латиницы (белорусского, украинского, польского, английского и др.); оценка текста на минимальных объемах и сравнение результатов этой оценки с образцами-эталонами; использование звуко-цветовых соответствий для проведения психолингвистической диагностики; проведение сравнительного анализа национальных учебников с аналогичными учебниками зарубежных стран.

Что касается компьютерных программ по изучению читабельности текста следует отметить, что первые программы появились в начале 80-х го-дов XX века: Readability Calculations, Intext, Nisus Writer и др. Разработанные продукты предназначены для анализа английского, немецкого и других языков (но не русского).

Заключение

Исходя из вышеизложенного, можно сделать вывод, что в настоящее время отсутствуют исследования в области читабельности с использованием современных информационных технологий и необходимого инструментария для классификации русскоязычных текстов по ряду областей знаний в зависимости от подготовленности читателя. Это дает основание выделить ряд наиболее актуальных направлений, требующих детального изучения:

1. Исследование и разработка количественных критериев трудности понимания текста интересующей группой читателей. В этой связи проанализированы основные методы для определения трудности понимания различных текстов данной группой лиц и проведены эксперименты, которые позволили получить информацию относительно трудности текста в зависимости от подготовленности не только выбранной группы, но и потенциальных читателей [13].

2. Выбор структурных элементов исследуемых текстов, которые поддаются точному измерению, и их детальное изучение. С этой целью следует использовать методы многомерного статистического анализ (кластерный и факторный анализы, метод корреляционных плеяд, многомерное шкалирование), которые позволят выявить связь между изучаемыми текстовыми признаками, и на этой основе существенно сократить их количество.

3. Проведение дискриминантного анализа, который на основании наиболее информативных признаков текста позволит предсказать принадлежность объектов к двум непересекающимся группам, т.е. классифицировать исследуемые тексты в зависимости от их трудности для читателей. Результатом проведения дискриминантного анализа станет вывод дискриминантных функций, которые станут основой для разработки соответствующего программного инструментария для автоматической классификации текстов.

4. Создание компьютерной программы для классификации текстов в зависимости от трудности их восприятия читателями. Эта программа должна включать:

- поиск необходимых параметров текста и их вычисление;
- функции предварительной обработки, сохранения и загрузки данных;
- расчет на основе текстовых характеристик дискриминантных функций, необходимых для классификации текстов;
- принятие решения относительно трудности текста для потенциальных читателей.

Исследования по данным направлениям позволят поставить и в определенной степени решить вопрос о внедрении в редакционно-издательскую подготовку изданий автоматизированных систем, выполняющих информационные, логические, аналитические и другие задачи, решение которых до сих пор связывают иногда с деятельностью живого мозга. Полная или частичная замена человека (редактора) сложной специализированной системой позволит добиться не только невозможного для человека быстродействия, но и необходимого качества изданий благодаря объективной оценке трудности текста на основе его информационных характеристик.

Литература

1. Mendenhall T.A. The characteristic curves of composition / T.A. Mendenhall // Science, 1887. – № 11. – P. 237–249.
2. Морозов Н.А. Лингвистические спектры: средство для отличения плагиатов от истинных произведений того или иного неизвестного автора. Стилеметрический этюд / Н.А. Морозов // Известия отд. русского языка и словесности Имп. Акад. наук. – Т. XX. – Кн. 4. – 1915.
3. Шевелев О.Г. Разработка и исследование алгоритмов сравнения стилей текстовых произведений: автореф. дис. … канд. техн. наук / О.Г. Шевелев. – Томск, 2006. – 20 с.
4. Morton A.Q. The authorship of greek prose / A.Q. Morton // Journal of the Royal Statistical Society (A), 1965. – № 128. – P. 169–233.
5. Миницкий Н.И. Психолингвистические и информационные аспекты восприятия и обработки учебного текста / Н.И. Миницкий, А.Ф. Толочко // Белорусский психологический журнал. – 2004. – № 3. – С. 57–61.
6. Закревская Н.С. Исследование однородности текста с помощью модели скользящего среднего / Н.С. Закревская // Квантитативная лингвистика: исследования и модели: материалы Всероссийской научной конференции (6–10 июня 2005 г.). – Новосибирск: НГПУ, 2005. – С. 26–33.
7. Хмелёв Д.В. Распознавание автора текста с использованием цепей А. А. Маркова / Д.В. Хмелёв // Вестник МГУ. – Сер. 9. Филология. – 2000. – № 2. – С. 115–126.
8. Хрулев О. Определение автора по тексту на естественном языке [Электронный ресурс]. Режим доступа: http://www.socionic.ru/ articles/psycholingvist_author.htm, свободный.
9. Невдах М.М. Формулы читабельности как критерий эффективного взаимодействия автора и читателя / М. М. Невдах // Материалы II Международной студенческой конференции «Научный потенциал студенчества – будущему России» (18–19 апреля). Т. 2. Лингвистика и межкультурная коммуникация. – Ставрополь: СевКавГТУ, 2008. – С. 102–103.
10. Король А.В. Компьютерная обработка текстов при помощи ИС «СМАЛТ» / А.В. Король, А.А. Рогов, Ю.В. Сидоров, А.И. Солопова // Проблемы развития гуманитарной науки на Северо-Западе России: опыт, традиции, инновации: Материалы научной конференции (ПетрГУ, 29 июня – 2 июля 2004 г., Петрозаводск). – С. 122–124.
11. Гринбаум О.Н. Проект «ЛИНДА» – автоматизированная система обработки лингвостатистических данных / О.Н. Гринбаум, Г.Я. Мартыненко, С.Я. Фитиалов // Прикладная лингвистика и автоматический анализ текста. – Тарту: ТГУ, 1988. – С. 31–33.
12. Система Polyanalist. Описание [Электронный ресурс]. Режим доступа: http://www.megaputer.ru, свободный.
13. Невдах М.М. Разработка количественных методов оценки трудности восприятия учебного текста для высшей школы / М.М. Невдах // Труды Белорусск. гос. технолог. ун-та. Сер. IX, Издательское дело и полиграфия. – 2008. Вып. XVI. – С. 87–90.

УДК 808.2:159.937

АНАЛИЗ ИНФОРМАЦИОННЫХ И ЭКСПРЕССИВНЫХ ХАРАКТЕРИСТИК ТЕКСТА

Ю.Ф. Шпаковский
(Белорусский государственный технологический университет)
Научный руководитель – к.филол.н., профессор Л.И. Петрова
(Белорусский государственный технологический университет)

В статье предложены варианты анализа информационных и экспрессивных характеристик текста. Для анализа информационных характеристик текста разработана математическая модель, на основе которой создана программа для анализа авторского стиля. Для анализа экспрессивных характеристик текста предложена технология, основанная на применении звуко-цветовых соответствий вербального представления информации. Данный метод может быть применен для определения психолингвистической характеристики автора, установления авторства, создания адекватных переводов с различных языков.

Ключевые слова: информационные и экспрессивные характеристики текста, читабельность, звуко-цветовой анализ

Введение

В настоящее время, несмотря на существующую систему контроля над качеством учебников, исследователи отмечают недостатки языка и стиля учебной литературы. Учебники не всегда соответствуют существующим стандартам и превышают объем допустимой учебной нагрузки. Ранее эти задачи решались за счет многократной переработки и экспериментальной проверки учебной литературы в школах. Это удлиняло время процесса изготовления и выпуска учебной литературы. Реалии сегодняшнего дня в нашей стране совершенно иные: резко увеличилось количество типов учебных заведений, происходят существенные изменения в средней школе, меняются формы обучения в высшей школе. В этой связи применение старых архаичных методов оценки качества учебной литературы, которая базируется на основе использования человеческого фактора, проблемы не решает, и нарекания на низкое качество учебной литературы продолжаются.

Это порождает необходимость создания специальных технологий, способствующих росту качественного уровня учебников, активизации научных исследований в этой области. В частности, существует актуальная потребность в разработке диагностических показателей качества, ориентированных на объективные, воспроизводимые методы контроля. Важно, чтобы данные методы основывались на количественных критериях оценки текста, проведении систематической и регулярной процедуры сбора данных по важным образовательным аспектам.

Проблема трудности восприятия учебного текста связано со следующими противоречиями: 1) растущим разрывом между объективно увеличивающимся объемом научного знания и тем объемом, который может быть усвоен учащимися; 2) применением сложных логических конструкций знания и игнорированием учета возрастного уровня мышления; 3) применением слишком сложных конструкций предложений в тексте; 4) отсутствием согласования между вербально-логической и знаково-символьной информацией. В итоге следует констатировать, что современные учебники порой превышают допустимые объемы, им характерны логическая и стилистическая сложность, психологический дискомфорт в восприятии текста.

Исследование характеристик текста

Обработка текстовой информации привлекала внимание исследователей и ранее. А.М. Сохор одним из первых предпринял серьезную попытку использовать математические методы для построения логической структуры учебного материала [6]. Для моделирования логических отношений им была применена теория графов. Важнейшую проблему свертывания и развертывания информации исследовал Д.И. Блюменау [2]. Он дал подробное описание синтаксической, коммуникативной, семантической и информативной структуры текста, а также средств внутритекстовой связности. Изложением путей оптимизации сложности учебного текста занимался Я.А. Микк. Ученый исследовал методы измерения трудности текста, его компоненты, а также критерии оптимальности [5]. Для определения сложности текста применялся метод регрессивного анализа. В рамках информативно-целевого подхода Т.М. Дридзе предложила методику выделения логико-фактологической цепочки для расчета гипотетического коэффициента информативности текста [3]. Л.П. Доблаев провел анализ смысловой структуры текста с учетом решения проблемы его понимания [4]. Вопрос сложности текста учебника стал одним из центральных в работе В.П. Беспалько, посвященной теории учебника [1]. Автор применил математический аппарат для исчисления дидактических качеств учебного текста. С учетом зарубежных достижений [9–14] по читабельности текста в отечественной науке была предложена количественная методика для оценки трудности восприятия учебного текста для высшей школы (на примере материала по химии) [8].

Отметим, что даже на первом этапе обработки текстовой информации для определения ее качества оказалось необходимым использование математического инструментария, в частности, вероятностных и статистических методов анализа.

Существующие ранее и разработанные в самое последнее время технологии обработки текста и представления учебного знания уже сегодня позволяют приступить к позитивному решению названной проблемы.

Известно, что любой текст кроме чисто информационной (содержательной) части имеет и инструментарий для его отображения. В нашем случае задача состоит в поиске таких критериев, которые наиболее полно отобразили бы вторую, несодержательную часть текста. Эта часть представляет собой своего рода дискретную информационную последовательность. По сложившейся практике наиболее полной характеристикой такой последовательности являются частотные (вероятностные) характеристики знаков, которые являются нормой конкретного языка по определенной генеральной совокупности. Для современного русского языка эта норма в справочной форме изложена в приложении 4 к ГОСТу 3489.1-71 «Шрифты типографские (на русской и латинской графических основах). Группировка. Индексация. Линия шрифта. Емкость».

Далее возникает новая задача: как распорядиться этими вероятностными характеристиками после того, как они определены для конкретного исследуемого текста? Это может быть и наиболее распространенный метод определения среднеквадратического отклонения от нормы, методы определения энтропии из теории информации, спектрального анализа, разложения в ряд и др. Кроме того, большое значение будет иметь и масштаб проводимых измерений, который должен наиболее полно отразить интересующие нас факторы. Например, при большом разбросе исследуемых параметров наиболее предпочтительным и широко распространенным на практике является логарифмический масштаб.

Можно отметить также, что на практике без существенного снижения качества анализа зачастую используют различного рода свертки информации либо исключают из анализа отдельные характеристики. Такие технологии характерны для телекоммуникационных систем (например, при обработке сигналов). Широкое распространение в

мировой практике и системе стандартизации получил также метод сравнения с образцами-эталонами.

Для обработки указанных аспектов информации потребовалось соответствующее математическое обеспечение. Было решено остановиться на модели, основные принципы которой изложены в монографии А.А. Харкевича [7, с. 27–34]. Модель предусматривает ситуацию, когда имеются два случайных процесса (в нашем случае это норма языка *S* и вероятностные характеристики исследуемого текста *X*). Результат математически можно представить так:

$X = S + \zeta$,

где ζ – отклонение *X* от *S*, т.е. по аналогии с телекоммуникационными системами – помеха. В этом случае мера корреляции S и ζ, выражается формулой

$E_{S\zeta} = \sum S \cdot \zeta_i$.

На основе этой формулы произведены необходимые инвариантные преобразования с учетом принятой выборки и определены требуемые характеристики для последующего принятия решений.

В условиях, когда имеется электронная версия текста и ПЭВМ для его отработки, вопрос о выборке репрезентативного объема текста принципиального значения не имеет.

В связи со сложностью процедур обработки, когда на первом этапе проведения работ используется полуавтоматический режим и исследуется много вариантов, создание дорогостоящего программного продукта нецелесообразно. В этих условиях ограничение исследований только гласными оказалось достаточным для практических целей, что в последующем не исключает полных исследований по всему алфавиту. На основе полученной модели исследования текстового материала по отклонениям частоты появлений отдельных букв алфавита можно в принципе проводить анализ текста и давать рекомендации потенциальным авторам.

Умение писать изначально с незначительными отклонениями от статистической структуры языка, делает всех авторов близкими по стилю изложения и легкости восприятия. Если же это условие выполнить невозможно, то возникает необходимость разработки методов проведения оценки степени авторской совместимости. Степень отклонений от собственной лингвистической характеристики можно проверить на малых объемах, например, на одной странице текста.

На основе математической модели была разработана программа, которая позволяет произвести детальный анализ любого текста. В качестве эталона-образца может быть принята норма русского или других языков, характеристика стиля автора на генеральной совокупности текста учебника, который признан в педагогическом сообществе образцовым. Вне зависимости от объемов исследуемого текста общая его характеристика по генеральной совокупности должна обязательно учитываться.

Данную программу можно использовать и для редактирования текста. Для этого при дешифровке результатов моделирования необходимо иметь базу данных образцов-эталонов. Подобный подход принципиально возможен, но достаточно сложен в осуществлении. Для упрощения решения задачи можно предложить принцип среднестатистической обработки текста дополнить технологией, основанной на применении звукоцветовых соответствий вербального представления информации. Подобный прием может быть также применен для определения психолингвистической характеристики автора, установления авторства, создания адекватных переводов с различных языков.

Данный аспект позволяет создать новый вариант технологии обработки текста. Само явление колористического восприятия текста как смыслонесущей категории было известно еще со времени древних цивилизаций.

Феномен человеческого восприятия звуков в цвете (цветовой слух), являющийся психологической характеристикой звуков (букв), позволяет в нашем случае определить

статус цвета как самостоятельную смыслонесущую категорию. Интегральная обработка различных материалов звуко-цветовых соответствий, учет того, что лингвисты считают гласные А, О, Е, И основными, а физики главными считают соответствующие им цвета: красный, желтый, зеленый, синий, позволяет составить графики звуко-цветовых соответствий.

Методика звуко-цветового анализа текста основана на частоте встречаемости звуков в речи (тексте). Как установили психологи, стандартную статистическую структуру мы в эмоционально-психологическом плане воспринимаем ровно и спокойно. Если звуки находятся в пределах нормы, то они не несут дополнительной нагрузки и, как бы не замечаются нами, а их значимость остается скрытой. Но если доля каких-то звуков заметно превышает норму, то доминирующим цветом анализируемого текста будет цвет звуко-букв, количественно превышающий норму своей частотности. Текст – это сложная и упорядоченная многоуровневая структура. Восприятие его тоже характеризуется многоуровневостью представления. Сюда входят сознательное осмысление и бессознательное восприятие, которое в психолингвистике рассматривается не как самостоятельная психическая реальность, противостоящая сознанию, а как низлежащий уровень сознания, характеризующийся меньшей расчлененностью и рефлексивностью. В последнее время понимание значимости бессознательного в восприятии действительности возрастает.

Как уже указывалось, воспринимая окраску звуков, мы рефлексируем интуитивно, подсознательно. Но это не умаляет значимость интеллектуальной рефлексии. Текст, окрашенный в определенные цвета, вызывает ряд эмоций на подсознательном уровне помимо сознательного его осмысления. Эмоции соответственно определяют возможные формы поведения субъекта, направленность его в принятии решения. В связи с этим и тексты в зависимости от назначения имеют разную цветовую окраску. Ранее отмечалось, что текст, имеющий минимальное отклонение от статистической структуры языка, наиболее пригоден в качестве образца – эталона для учебной литературы. В этом случае окраска звуков не превышает привычной нормы и не вызывает дополнительных эмоций на подсознательном уровне.

Иное дело поэзия. Художник слова стремится как можно полнее, ярче, живее выразить у слушателя и читателя нужные впечатления, переживания, размышления. Достигается эта цель всеми языковыми средствами, главное из которых – смысловая сторона языка с тонкой и бесконечно разнообразной игрой оттенков значения слов и их сочетаний. В стихотворении важны все аспекты формы: и ритм, и рифма, и композиция. И, конечно же, звуки – живая плоть стиха. Поэт со свойственной его таланту глубиной тонко чувствует содержательность звуков и точно оперирует ею, создавая звуковую ткань стиха, творя музыку речи. Эта потенциальная сила во многом проявляется через нелингвистические характеристики звуков, одной из которых является их цветовая окраска. В результате эмоциональная и цветовая экспрессия поэтического текста потенциально значительно выше прозаического.

Трактовка воздействия одного и того же цвета на человека в различных источниках и у разных авторов выглядит весьма разнообразно и противоречиво. Но более глубокий анализ говорит о следующем. В зависимости от ситуации и целей авторы отражают близкую им часть проблемы с определенной эмоциональной оценкой. В самом деле, лечение цветом, влияние цвета на физическом, психическом, метафизическом уровнях, ассоциативное воздействие, музыка и цвет – все эти факторы делают актуальной ту или иную сторону многогранного колористического восприятия мира. Для учебного книгоиздания должны быть проведены свои исследования, после чего выработаны критерии воздействия цвета на учащегося. По результатам исследований различных авторов представляется целесообразным использовать следующие исходные интегральные психологические значения цвета.

Красный цвет вызывает наиболее сильную физиологическую реакцию. Эмоции в данном случае могут быть, как положительные, так и отрицательные, в любом случае реакция на красный цвет – реакция возбуждения. Этот цвет по психологическому воздействию беспокойный, при длительном воздействии слишком долгое возбуждение переходит в раздраженное утомление.

Желтый цвет воздействует легко и возбуждающе, привлекает внимание и сигнализирует о чем-то новом. Иногда этот цвет может вызвать раздражение и утомляет.

Зеленый – это прочность, надежность, долговечность, благополучие и уверенность.

В окружении синего человек чувствует себя в гармонично-ненапряженном состоянии. Синий цвет считается деловым, профессиональным и авторитетным. Однако если синий излишне доминирует, то он может быть подавляющим и даже депрессивным.

Фиолетовый цвет подчеркивает незаурядность и оригинальность. Сочетает в себе энергию красного и элегантность синего.

Звуко-цветовой анализ этих характеристик с использованием фактора различного психолингвистического воздействия цвета на человека показывает высокую степень совпадения их с содержанием материала. Значимость имеющихся и полученных результатов психолингвистического анализа дают все основания полагать, что они найдут применение в сфере учебного книгоиздания. Созданный инструментарий, по сути дела, может послужить действенным и эффективным технологическим средством реализации издательских норм и рекомендаций. Кроме того, возможен учет этой технологии в издании литературы для обучаемых с различного рода девиациями в психофизиологическом развитии.

Заключение

Обобщая изложенное, можно высказать следующее предположение. Применение современных информационных технологий создает возможности для эффективного использования скрытых потенциальных возможностей текста (скрытой информативности и экспрессивности языка), что важно в системе учебного книгоиздания и уменьшения степени субъективности экспертиз учебной литературы.

Разработанная математическая модель уже сегодня позволяет решать ряд следующих задач системы учебного книгоиздания:

1) тестирование авторского коллектива на предмет психолингвистической совместимости;

2) определение психолингвистических характеристик авторских текстов, после чего могут быть даны рекомендации по их корректировке;

3) редактирование текста в направлении максимального приближения его к стандартной статистической структуре языка изложения с целью создания естественной языковой среды для учащегося, как наиболее оптимальной.

Литература

1. Беспалько В.П. Теория учебника: дидактический аспект / В.П. Беспалько. – М.: Педагогика. – 1988.
2. Блюменау Д.И. Проблемы свертывания научной информации / Д.И. Блюменау. – Л.: Наука. – 1982.
3. Дридзе Т.М. Текстовая деятельность в структуре социальной коммуникации / Т.М. Дридзе. – М.: Наука. – 1984.

4. Доблаев Л.П. Смысловая структура учебного текста и проблемы его понимания / Л.П. Доблаев. – М.: Педагогика. – 1982.
5. Микк Я.А. Оптимизация сложности учебного текста: в помощь авторам и редакторам / Я.А. Микк. – М.: Просвещение. – 1981.
6. Сохор А.М. Логическая структура учебного материала / А.М. Сохор. – М.: Педагогика. – 1974.
7. Харкевич А.А. Борьба с помехами / А.А. Харкевич. – М.: Гос. изд-во физ.-мат. литры. – 1963.
8. Шпакоўскі Ю.Ф. Распрацоўка колькаснай методыкі ацэнкі цяжкасці ўспрымання вучэбных тэкстаў для вышэйшай школы / Ю.Ф. Шпакоўскі // Вес. Нац. акад. навук Беларусі. Сер. гуманіт. навук. – 2008. – № 1. – С. 111–115.
9. Chall J.S. Readability: an appraisal of research and application / J.S. Chall. – Columbus, OH: Ohio State University Press. – 1958.
10. Flesch R. The art of readable writing / R. Flesch. – New York: Harper. – 1949.
11. Entin E.B. Relationships of measures of interest, prior knowledge, and readability to comprehension of expository passages / E.B. Entin, G.R. Klare // Advances in reading/language research. – 1985. – № 3. – P. 9–38.
12. Klare G.R. The measurement of readability / G.R. Klare. – Ames, Iowa: Iowa State University Press. – 1963.
13. Paul T. Guided Independent Reading / T. Paul. – Madison, WI: School Renaissance Institute. – 2003.
14. Stenner A.J. The objective measurement of reading comprehension in response to technical questions raised by the California department of education technical study group / A.J. Stenner, D. S. Burdick. – Durham, NC: MetaMetrics. – 1997.

АВТОМАТИЗИРОВАННАЯ СИНХРОНИЗАЦИЯ МЕЖДУ CAD И PDM-СИСТЕМАМИ ДЛЯ КОМПЛЕКСНЫХ СОСТАВНЫХ ИЗДЕЛИЙ. ПРОТИВОРЕЧИЯ. ПРЕДЕЛ АВТОМАТИЗАЦИИ

Т.Д. Голицына, Т.А. Павловская

Работа посвящена некоторым проблемам, возникающим при интеграции систем управления данными об изделии (PDM) и систем автоматизированного проектирования (CAD). Анализируются варианты решения таких проблем.

Введение

В настоящее время существует множество различных систем, автоматизирующих взаимодействие PDM и CAD систем, разработанных для конкретных предприятий. Их общая черта – это частность предлагаемых решений, т.е. такая система обычно представляет собой интеграцию конкретной PDM системы с конкретной CAD системой. При этом проблемы, возникающие при интеграции, решаются в каждом случае различными способами. Кроме того, поскольку такие системы являются коммерческими, конкретная программная реализация зачастую скрыта, поэтому провести анализ существующих решений с целью выбора лучшего или более универсального не представляется возможным.

В то же время в направлении решения описанной проблемы сделаны серьезные шаги. Так, международный стандарт ISO 10303 (ГОСТ Р ИСО 10303 [3]) призван определить единый способ обмена информацией между всеми системами, содержащими данные о модели изделия [2]. Это позволит автоматизировать взаимодействие любых PDM и CAD систем, поддерживающих стандарт, в общем случае, без дополнительных интегрирующих программ.

Тем не менее, простое следование этому стандарту может оказаться недостаточным, поскольку он не определяет, каким образом, например, отражать в PDM системе изменения между переданной и уже имеющейся в системе информацией не в рамках конкретного изделия, а с точки зрения всей системы в целом.

В рамках построения унифицированной модели взаимодействия PDM и CAD систем [1] необходимо определить общую стратегию решения подобных вопросов, поскольку их решение возложено на центральный модуль, осуществляющий взаимодействие PDM и CAD систем. На рис. 1 приведена принципиальная схема унифицированной модели.

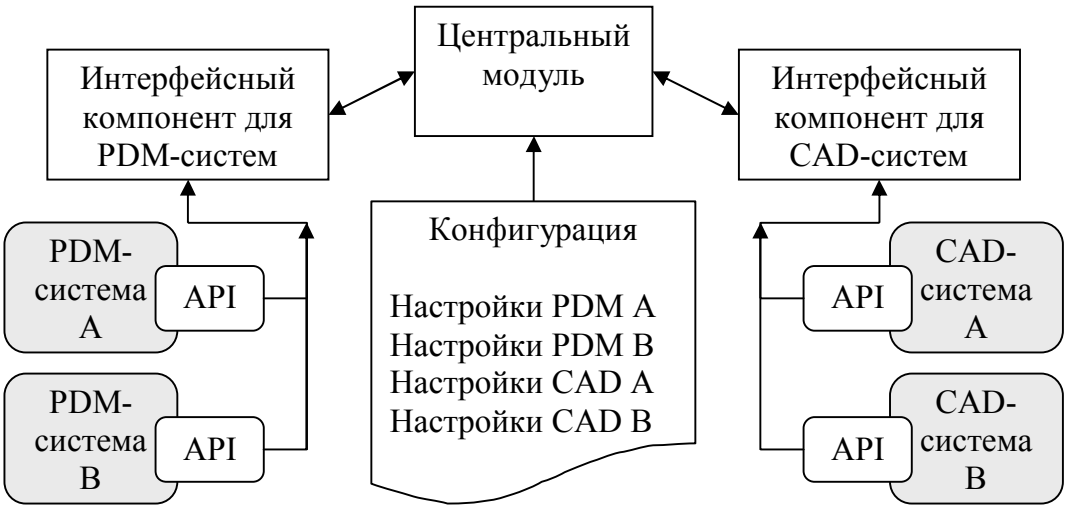


Рис. 1. Архитектура программного комплекса

На текущем этапе проработки унифицированной модели принципиальные вопросы решено ограничить следующим списком:

1) каким образом и насколько автоматизировать отражение изменения информации о некотором изделии в PDM системе в тех изделиях, в которые оно входит в качестве составного элемента?
2) как поддерживать и допускать ли в принципе разные версии одинаковых изделий в составе некоторого изделия в PDM системе?
3) в какой момент создавать новую версию изделия в PDM системе, и каким образом нотифицировать пользователей об этом?

Рис. 2 содержит условную схему состава некоторого изделия, на основании которой рассмотрены перечисленные вопросы.

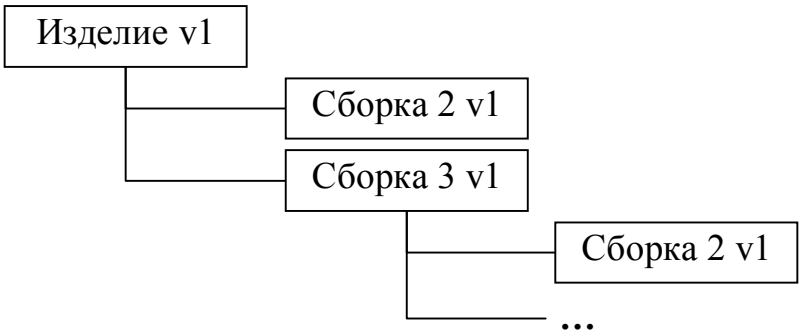


Рис. 2. Условная схема состава изделия

Степень автоматизации отражения изменений

Создание новой версии какого-либо изделия в принципе должно найти отражение во всех изделиях, в состав которых оно входит. В настоящее время большинство PDM систем поддерживают автоматическое уведомление об этом событии (так, в PDM Step Suite [4] можно настроить автоматическую рассылку сообщений заинтересованным пользователям). Но это не всегда удобно, так как включение новой версии в состав изделия придется производить вручную.

Рассмотрим возможные способы решения этой проблемы.

I. «Полная автоматизация»: появление новой версии какого-либо изделия (например, Сборка 2 v2) приводит к автоматической замене всех версий этого изделия во всех сборках, в состав которых оно входит (Изделие v1 и Сборка 3 v1), на новую версию.

К достоинствам данного способа стоит отнести очевидное отсутствие участия человека в процессе обновления версий, то есть при появлении новой версии изделия (например, после его согласования и утверждения) все вхождения предыдущей версии этого изделия заменяются на новую версию. В то же время, данное обстоятельство является и недостатком, поскольку, во-первых, автоматическая замена версий не всегда приемлема, а данный способ сделает эту замену неподконтрольной, а во-вторых, на этапе создания новой версии нет информации, в какое количество сборок данное изделие входит, а соответственно и объем последующих изменений (а значит и время на эти изменения) непредсказуем.

II. «Отсутствие автоматизации»: появление новой версии не вызывает никаких автоматических изменений в сборках, в состав которых оно входит. Так работает большинство существующих PDM систем. В данном варианте отсутствуют бесконтрольные изменения – их придется проводить вручную.

III. Предлагаемый для реализации способ «Управляемая автоматизация» призван объединить достоинства предыдущих двух методов. Его суть состоит в том, что при попытке изменить изделие (например, забрать на редактирование в CAD систему)

предлагается список новых версий всех составляющих его изделий, то есть версий, сделанных позже уже включенной в состав изделия. Пользователь имеет возможность выбрать ту или иную версию для любого изделия, входящего в состав данного, или отказаться от внесения изменений. Чтобы ограничить объем изменений, предлагается выводить список возможных замен только для первого уровня иерархии относительно данного изделия.

После выбора интересующей версии составляющего изделия пользователю предоставляется информация об отличиях используемой и выбранной версией, на основании чего он принимает решение о замене существующей версии на новую, при этом сама замена производится автоматически.

Стратегия обработки одинаковых изделий

Поскольку в состав изделия могут входить одинаковые составные части, причем на разных уровнях иерархии, встает задача определения стратегии работы в этом случае. Рассмотрим возможные способы решения этой проблемы на примере рис. 3.

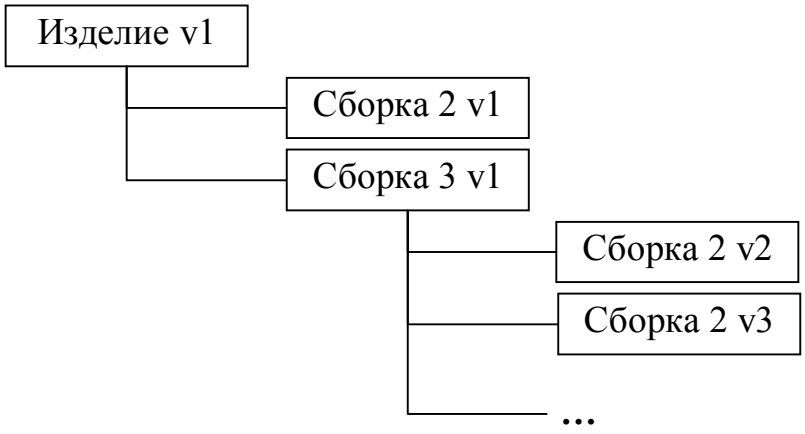


Рис. 3. Условная схема состава изделия для иллюстрации вариантов работы с одинаковыми изделиями

I. Такие составные части можно рассматривать независимо друг от друга, то есть в составе одного изделия могут находиться одинаковые изделия разных версий (Сборка 2 v1, Сборка 2 v2 и Сборка 2 v3). К каждой версии привязывается файл в CAD системе, соответственно изменение идет независимо.

Этот вариант позволят гибко подходить к вопросу состава изделия и может быть полезен во многих специфических случаях. Однако сложность реализации и сложность поддержки и понимания такой структуры не позволяют использовать его повсеместно.

II. Можно рассматривать все одинаковые изделия совместно, то есть все изделия, входящие в состав данного и имеющие название Сборка 2, будут всегда иметь одинаковую версию. Только один файл привязывается ко всем таким изделиям и его изменение с созданием новой версии приводит к одновременному изменению всех таких изделий. При таком способе возможны несколько вариантов понимания слова «одинаковые» – так, например, одинаковыми можно считать изделия, непосредственно входящие в состав данного, то есть находящиеся на следующем уровне иерархии, или рассматривать в качестве таких изделий все изделия на всех уровнях иерархии относительно данного.

III. Существует и третий способ, который позволяет считать изделия одинаковыми, если они ссылаются на один файл с моделью в CAD системе, и разными, если файлы различны. Таким образом, можно совместить положительные стороны первых двух методов.

Стратегия создания новых версий

Задача выбора времени создания новой версии только на первый взгляд кажется простой. Рассмотрим этот вопрос детальнее.

I. Можно создавать новую версию при каждом изменении изделия, например каждый раз, когда мы завершаем редактирование в CAD и обнаруживаем какие-либо изменения. Но при таком способе в системе будет храниться большое количество версий, являющихся промежуточными, что затрудняет управление версиями.

II. Можно также вводить другие критерии создания версий – например, по истечении определенного времени (новая версия появляется раз в неделю) или по какому-либо событию (все изменения попадают в новую версию, если предыдущая уже согласована).

III. Но наиболее гибким видится способ, при котором создание новой версии запрашивается у пользователя. При таком способе после завершения редактирования изделия в CAD пользователь должен указать, хочет ли он изменить текущую версию или создать новую. И, соответственно, количество версий ограничено реальной потребностью пользователя, а не внешними причинами.

Реализация

По результатам анализа для реализации были выбраны способы решения, учитывающие требования большинства пользователей, и, соответственно, позволяющие сделать систему более гибкой. Они были реализованы в рамках системы интеграции CAD и PDM систем и явились продолжением разработки унифицированного подхода.

В настоящее время интерфейсный компонент для PDM систем позволяет работать с PDM Step Suite, а в качестве интерфейсного компонента для CAD систем в состав комплекса включена библиотека GSCADLink [5], поддерживающий работу с SolidWorks, Pro/E, SolidEdge, Unigraphics, Inventor, Компас 3D, AutoCAD, PCAD и CATIA.

Обновление версий изделий проводилось по методу «управляемой автоматизации». Единственным недостатком данного метода по сравнению с остальными описанными в статье является сложность его программной реализации.

Работа с одинаковыми изделиями была реализована с возможностью обрабатывать их совместно или раздельно, в зависимости от того, на одинаковые ли файлы описания модели они ссылаются. Такой подход оказался очень удобен, поскольку данная реализация является прозрачной для пользователя и не вносит дополнительной сложности для большинства случаев, когда работа с одинаковыми изделиями ведется совместно, и в то же время позволяет в случае необходимости включать в состав изделия разных версий.

Новая версия в системе создается только тогда, когда это действительно необходимо – т.е. по желанию пользователя. Подход оказался очень удобен при наличии в проекте большого количества несущественных изменений.

Заключение

В настоящей работе были рассмотрены некоторые проблемы, возникающие при интеграции PDM и CAD систем, предложены методы их решения. Для каждого метода были рассмотрены его достоинства и недостатки. В заключение приведены результаты реализации выбранных решений в рамках разработки унифицированного подхода к интеграции PDM и CAD систем.

Литература

1. Голицына Т.Д. Проблемы интеграции PDM и CAD систем. Унифицированный подход. // Научно-технический вестник СПбГУ ИТМО. Выпуск 39. Исследования в области информационных технологий. Труды молодых ученых. – СПб: СПбГУ ИТМО, 2007. – С. 164–168.
2. Mason H. ISO 10303 – STEP A key standard for the global market. // ISO Bulletin. Апрель 2002. – С. 9–13.
3. ГОСТ Р ИСО 10303 «Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными». М.: Госстандарт России. – 2000.
4. PDM STEP Suite. Техническое описание. // Официальный сайт НИЦ CALS-технологий «Прикладная логистика» http://pss.cals.ru/DOC/PSS_TD_2_1.pdf
5. GSCADLink. Описание. // Официальный сайт ООО «Глосис-Сервис» http://glosys.ru/products/cad/GSCADLink.htm

ВОПРОСЫ ИНТЕГРАЦИИ СИСТЕМ УПРАВЛЕНИЯ ДАННЫМИ ОБ ИЗДЕЛИИ (PDM) И САПР

Т.Д. Голицына, Т.А. Павловская

Работа посвящена интеграции систем управления данными об изделии (PDM) и систем автоматизированного проектирования (САПР). Рассматриваются характеристики PDM-систем и САПР, существенные для их интеграции. Предлагается архитектура программного обеспечения.

Введение

В настоящее время разработано достаточно большое число систем, позволяющих автоматизировать работу предприятия на различных (но часто разрозненных) участках производства: системы автоматизации проектирования, системы хранения и версионного контроля данных, автоматизированной технологической подготовки производства, систем управления производством и др. Основной и наиболее актуальной проблемой является связывание этих систем в единое целое, единое информационное пространство предприятия или группы предприятий, что позволит избежать избыточности данных, хранимых в каждой из систем, уменьшить временной цикл их передачи между подразделениями, а также обеспечить непротиворечивость и своевременное обновление данных.

На рис. 1 [3] показано распределение видов деятельности промышленного предприятия. Основными являются интеллектуальная и собственно производственная деятельность, что позволяет рассматривать вопросы интеграции систем, автоматизирующих работу в этих областях, как наиболее приоритетные.

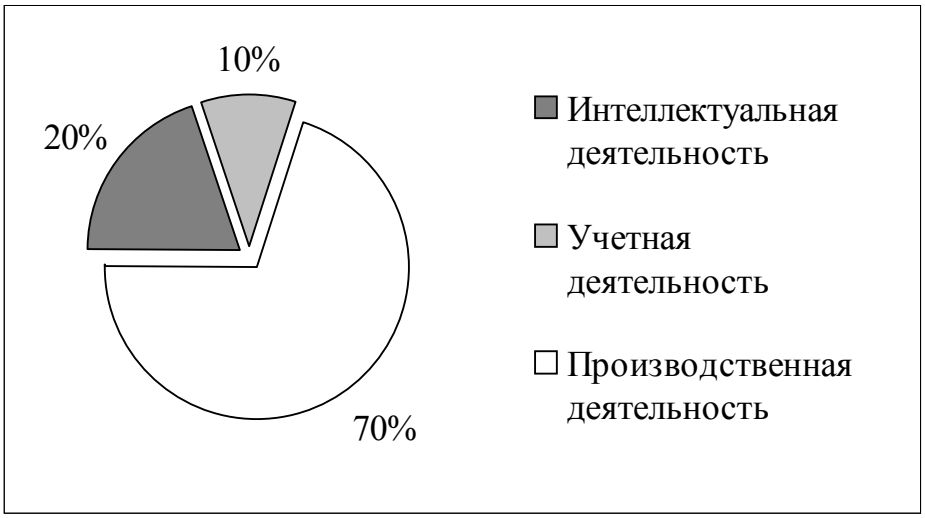


Рис. 1. Временные и материальные издержки промышленного предприятия

Системы автоматизированного проектирования (САПР) и системы управления данными об изделии (Product Data Management, PDM-системы) обеспечивают автоматизацию в области интеллектуальной деятельности и производственной деятельности. Вопросы и проблемы, связанные с интеграцией этих систем, и будут рассмотрены в настоящей работе.

PDM-системы

PDM-система – организационно-техническая система, обеспечивающая управление всей информацией об изделии и связанных с ним процессах на протяжении всего его жизненного цикла – начиная с проектирования и производства до снятия с эксплуа-

тации. При этом в качестве изделий могут рассматриваться различные сложные технические объекты (например, корабли или компьютерные сети). Она включает в себя управление хранением данных (в том числе и графическими изображениями изделия) и документами, управление конфигурацией изделия, автоматизацией создания выборок и отчетов, а также механизмы авторизации. Основным принципом хранения данных в PDM-системе является то, что любые данные хранятся только один раз (без избыточности) в защищенной системе, называемой хранилищем данных.

К настоящему времени существует несколько стандартов для PDM-систем. Наиболее распространенным является стандарт STEP (ISO 10303) (в 2000 вышел русскоязычный вариант этого стандарта – ГОСТ Р ИСО 10303 [2]). Он описывает структуры данных PDM-системы и методы доступа к ним. Введен специальный язык EXPRESS для описания объектов, хранящихся в PDM-системе. Наличие стандарта значительно облегчает взаимодействие внешних приложений с поддерживающими его PDM-системами – это и единообразность представления данных в системе, и единый интерфейс доступа к ним.

Согласно стандарту изделие в PDM-системе идентифицируется следующими параметрами:

- обозначение изделия;
- наименование изделия;
- описание изделия;
- контекст изделия (конструкторский, технологический, финансовый и т.д.).

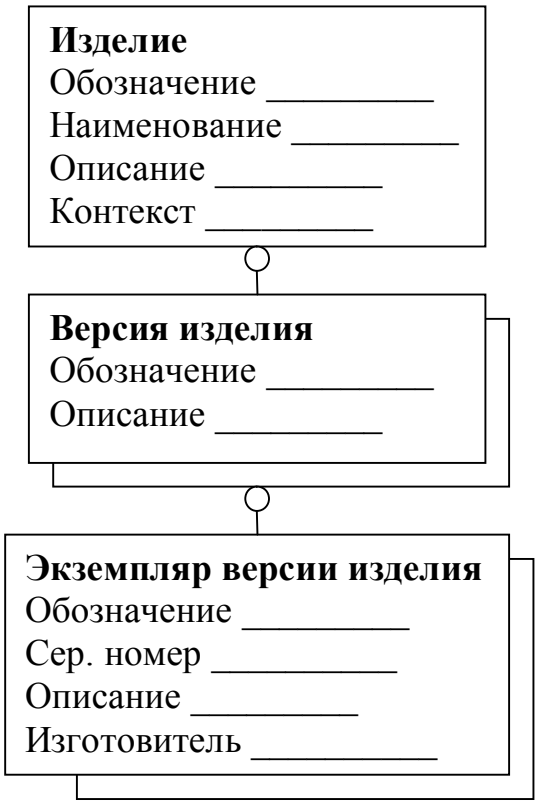


Рис. 2. Схема идентификации изделия

Каждое изделие может иметь одну или несколько версий, описываемых, в свою очередь, следующими параметрами:

- обозначение версии;
- описание версии;
- изделие, версией которого является данный объект.

Для описания конкретного изделия на этапе его эксплуатации используется понятие экземпляра изделия, который характеризуется:

- серийным номером;
- организацией-изготовителем;
- наименованием версии изделия, экземпляром которой он является.

Рис. 2 иллюстрирует приведенную структуру.

Все отношения между изделиями определяются в определенном контексте. Между изделиями возможны следующие отношения:

- «входит в состав сборки как единица»;
- «входит в состав в количестве …»;
- «изготовлен из материала».

Кроме того, в PDM-системе можно определить правила применяемости отношений между изделиями (например, временной интервал или партия изделия, на котором данное правило действует), зависящие от времени характеристики изделий, версий и экземпляров, состава экземпляра версии изделия на конкретный момент времени и т.п.

САПР

САПР – организационно-техническая система, предназначенная для выполнения проектной деятельности и позволяющая создавать конструкторскую и технологическую документацию. САПР охватывает создание геометрических моделей изделия (трехмерных, составных), а также генерацию чертежей изделия и их сопровождение.

Изделие может быть деталью или сборкой, т.е. изделием, состоящим, в свою очередь, из других изделий.

Каждая модель изделия определяется в САПР следующими характеристиками:

- тип (сборка или деталь);
- масса, объем, плотность;
- компоненты (изделия, составляющие данное);
- список размеров (наименование, значение и статус валидности);
- список параметров (наименование, значение и статус валидности).

Для каждого из компонентов определяются те же характеристики. Таким образом, в САПР изделие описывается иерархической структурой.

Схема интеграции

Задача интеграции конкретной PDM-ситемы с конкретной САПР для конкретной задачи в принципе технически осуществима – достаточно использовать прикладные программные интерфейсы (Application Programming Interface, API) обеих систем. Но в настоящее время, когда и PDM-системы, и САПР исчисляются десятками, желательно и актуально иметь такое решение, которое помогло бы легко заменять одну систему другой или использовать параллельно несколько PDM-систем или САПР.

Основная задача интеграции PDM-систем и САПР состоит в том, чтобы сделать их взаимодействие единообразным и легко расширяемым. Для этого предлагается разработать программные компоненты, организующие единый интерфейс для взаимодействия с различными PDM-системами и, аналогично, единый интерфейс для взаимодействия с различными САПР.

Для PDM-систем, поддерживающих стандарт STEP, задача упрощается, поскольку интерфейс системы во многом регламентирован стандартом.

Интерфейсные компоненты должны реализовывать следующие функции:

- организация взаимодействия с широким набором PDM-систем/САПР;

– локализация информации об особенностях конкретной системы;
– поддержка единого набора функций API для доступа к PDM-системам/САПР.

Интерфейсные компоненты взаимодействуют и с PDM-системами, и с САПР. Функциональность собственно интеграции реализует центральный модуль. Общая схема программного комплекса представлена на рис. 3.

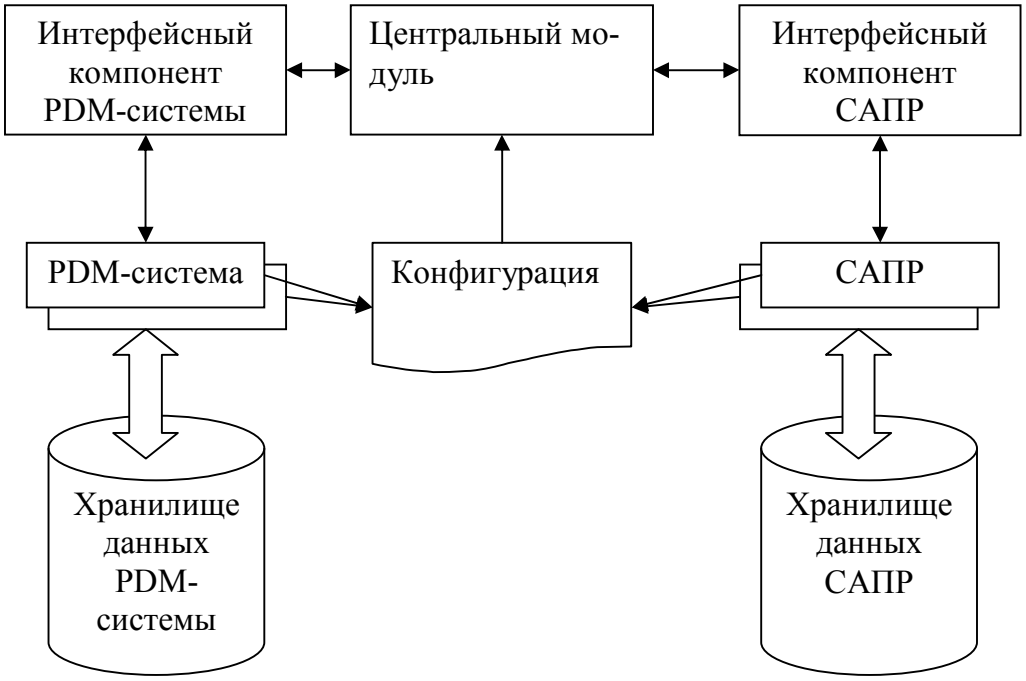


Рис. 3. Архитектура программного комплекса

Задачами центрального модуля являются:

1. Организация сеанса взаимодействия между конечными PDM-системой и САПР. Это подразумевает авторизацию и подключение к обеим системам с соответствующими правами.
2. Обмен данными между PDM-системой и САПР. Так, модель изделия из САПР должна преобразоваться в иерархическую структуру изделия, его составляющих и их параметров в PDM-системе. И, наоборот, структура изделия в PDM-системе, имеющая описание геометрии каждой компоненты изделия и их взаимного расположения, должна передаваться в САПР.
3. Синхронизация данных между моделью изделия в САПР и его параметрами в PDM-системе. При синхронизации необходимо указать направление синхронизации, т.е. систему, которая содержит наиболее актуальную информацию об изделии. Результаты сравнения данных, находящихся в каждой из систем, должны визуализироваться, чтобы пользователь мог понять, что изменилось в параметрах изделия в результате обновления.
4. Интерпретация данных, полученных в результате выгрузки или синхронизации. Предлагаемая схема интеграции предполагает использование различных PDM-систем и различных САПР, поэтому необходимо обеспечить корректную интерпретацию полученных данных, поскольку наименование одного и того же по смыслу параметра в различных PDM-системах или САПР может отличаться. Минимально необходимо корректно интерпретировать обозначение и авторство (для предотвращения ошибок идентификации изделия), а также его размеры и массу (для предотвращения ошибок в расчетах). Для реализации этой задачи предполагается использовать настраиваемый конфигурационный файл, позволяющий определить, как интерпретировать тот или иной параметр в каждой системе.

5. Обеспечение обработки запросов на модификацию с резервацией (check-in/check-out) для поддержки одновременной работы нескольких пользователей. Так, параметры изделия в PDM-системе не должны быть доступны для изменения, если модель этого изделия в этот момент модифицируется в САПР. И наоборот, модификация модели должна быть запрещена на то время, пока идет модификация соответствующего изделия в PDM-системе.

Преимуществом данной архитектуры являются унификация интерфейсов для взаимодействия с PDM-системами и САПР, а следовательно, легкость расширения. Особой проработки при реализации данной архитектуры требуют вопросы методологии разработки модели изделия в САПР для полноценного переноса информации об изделии в PDM-систему.

Заключение

В настоящей работе рассмотрены особенности PDM-систем и САПР, существенные для их интеграции. Приведены результаты исследования вопросов PDM-систем и САПР. Предлагается вариант архитектуры программного комплекса, позволяющего унифицировать интеграцию различных PDM-систем и САПР.

Литература

1. Бубнов А. CATIA 5 для проектирования промышленных объектов, оборудования и систем. //САПР и графика. 2003. – №2.
2. ГОСТ Р ИСО 10303 «Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными». – М.: Госстандарт России. – 2000.
3. Зыков О. Промышленная автоматизация: движение от САПР к PLM. //IT News. 2005. – №05.
4. Интегрированное решение Lotsia PLM 4.0. //Официальный сайт Lotsia PLM http://www.lplm.ru/ (http://www.lplm.ru/index.php?option=com_content&task=category&sectionid=2&id=7&Itemid=26)
5. Технические характеристики Lotsia PDM PLUS. //http://www.cadgroup.ru/product/78/
6. AutoCAD 2007. //http://www.cadgroup.ru/product/81/
7. CAD/CAM/CAE система Pro/ENGINEER. //Официальный сайт компании Эврика http://www.eureca.ru/products/pro-engineer/
8. PDM STEP Suite. Техническое описание. //Официальный сайт НИЦ CALS-технологий "Прикладная логистика" http://pss.cals.ru/DOC/PSS_TD_2_1.pdf

АВТОМАТИЗИРОВАННАЯ СИНХРОНИЗАЦИЯ МЕЖДУ CAD И PDM-СИСТЕМАМИ ДЛЯ КОМПЛЕКСНЫХ СОСТАВНЫХ ИЗДЕЛИЙ. ПРОТИВОРЕЧИЯ. ПРЕДЕЛ АВТОМАТИЗАЦИИ

Т.Д. Голицына, Т.А. Павловская

Работа посвящена некоторым проблемам, возникающим при интеграции систем управления данными об изделии (PDM) и систем автоматизированного проектирования (CAD). Анализируются варианты решения таких проблем.

Введение

В настоящее время существует множество различных систем, автоматизирующих взаимодействие PDM и CAD систем, разработанных для конкретных предприятий. Их общая черта – это частность предлагаемых решений, т.е. такая система обычно представляет собой интеграцию конкретной PDM системы с конкретной CAD системой. При этом проблемы, возникающие при интеграции, решаются в каждом случае различными способами. Кроме того, поскольку такие системы являются коммерческими, конкретная программная реализация зачастую скрыта, поэтому провести анализ существующих решений с целью выбора лучшего или более универсального не представляется возможным.

В то же время в направлении решения описанной проблемы сделаны серьезные шаги. Так, международный стандарт ISO 10303 (ГОСТ Р ИСО 10303 [3]) призван определить единый способ обмена информацией между всеми системами, содержащими данные о модели изделия [2]. Это позволит автоматизировать взаимодействие любых PDM и CAD систем, поддерживающих стандарт, в общем случае, без дополнительных интегрирующих программ.

Тем не менее, простое следование этому стандарту может оказаться недостаточным, поскольку он не определяет, каким образом, например, отражать в PDM системе изменения между переданной и уже имеющейся в системе информацией не в рамках конкретного изделия, а с точки зрения всей системы в целом.

В рамках построения унифицированной модели взаимодействия PDM и CAD систем [1] необходимо определить общую стратегию решения подобных вопросов, поскольку их решение возложено на центральный модуль, осуществляющий взаимодействие PDM и CAD систем. На рис. 1 приведена принципиальная схема унифицированной модели.

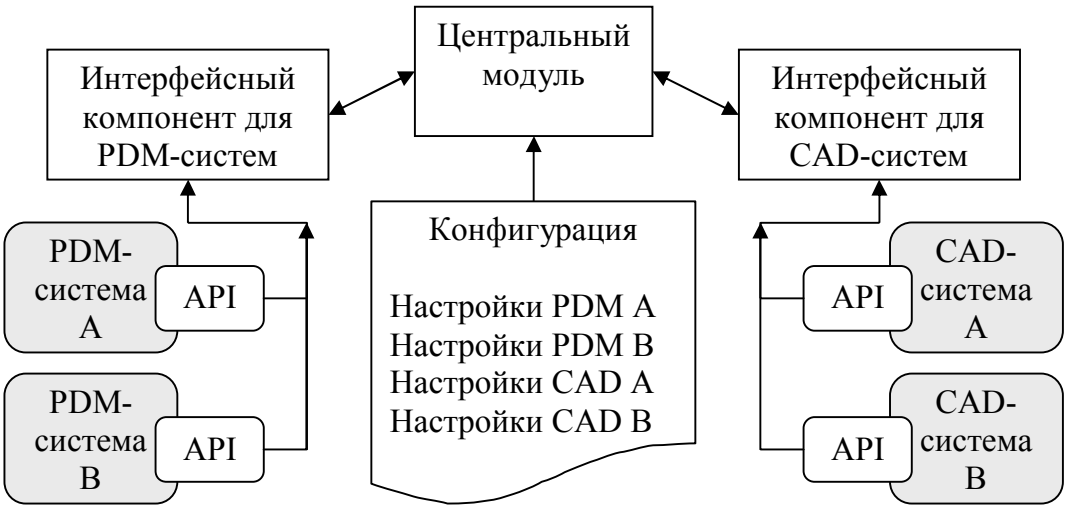


Рис. 1. Архитектура программного комплекса

На текущем этапе проработки унифицированной модели принципиальные вопросы решено ограничить следующим списком:

1) каким образом и насколько автоматизировать отражение изменения информации о некотором изделии в PDM системе в тех изделиях, в которые оно входит в качестве составного элемента?
2) как поддерживать и допускать ли в принципе разные версии одинаковых изделий в составе некоторого изделия в PDM системе?
3) в какой момент создавать новую версию изделия в PDM системе, и каким образом нотифицировать пользователей об этом?

Рис. 2 содержит условную схему состава некоторого изделия, на основании которой рассмотрены перечисленные вопросы.

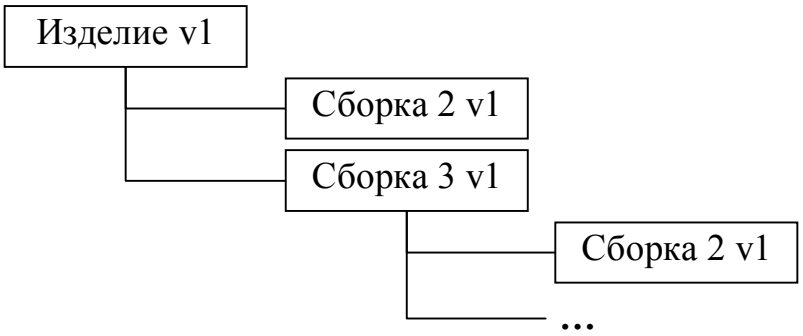


Рис. 2. Условная схема состава изделия

Степень автоматизации отражения изменений

Создание новой версии какого-либо изделия в принципе должно найти отражение во всех изделиях, в состав которых оно входит. В настоящее время большинство PDM систем поддерживают автоматическое уведомление об этом событии (так, в PDM Step Suite [4] можно настроить автоматическую рассылку сообщений заинтересованным пользователям). Но это не всегда удобно, так как включение новой версии в состав изделия придется производить вручную.

Рассмотрим возможные способы решения этой проблемы.

I. «Полная автоматизация»: появление новой версии какого-либо изделия (например, Сборка 2 v2) приводит к автоматической замене всех версий этого изделия во всех сборках, в состав которых оно входит (Изделие v1 и Сборка 3 v1), на новую версию.

К достоинствам данного способа стоит отнести очевидное отсутствие участия человека в процессе обновления версий, то есть при появлении новой версии изделия (например, после его согласования и утверждения) все вхождения предыдущей версии этого изделия заменяются на новую версию. В то же время, данное обстоятельство является и недостатком, поскольку, во-первых, автоматическая замена версий не всегда приемлема, а данный способ сделает эту замену неподконтрольной, а во-вторых, на этапе создания новой версии нет информации, в какое количество сборок данное изделие входит, а соответственно и объем последующих изменений (а значит и время на эти изменения) непредсказуем.

II. «Отсутствие автоматизации»: появление новой версии не вызывает никаких автоматических изменений в сборках, в состав которых оно входит. Так работает большинство существующих PDM систем. В данном варианте отсутствуют бесконтрольные изменения – их придется проводить вручную.

III. Предлагаемый для реализации способ «Управляемая автоматизация» призван объединить достоинства предыдущих двух методов. Его суть состоит в том, что при попытке изменить изделие (например, забрать на редактирование в CAD систему)

предлагается список новых версий всех составляющих его изделий, то есть версий, сделанных позже уже включенной в состав изделия. Пользователь имеет возможность выбрать ту или иную версию для любого изделия, входящего в состав данного, или отказаться от внесения изменений. Чтобы ограничить объем изменений, предлагается выводить список возможных замен только для первого уровня иерархии относительно данного изделия.

После выбора интересующей версии составляющего изделия пользователю предоставляется информация об отличиях используемой и выбранной версией, на основании чего он принимает решение о замене существующей версии на новую, при этом сама замена производится автоматически.

Стратегия обработки одинаковых изделий

Поскольку в состав изделия могут входить одинаковые составные части, причем на разных уровнях иерархии, встает задача определения стратегии работы в этом случае. Рассмотрим возможные способы решения этой проблемы на примере рис. 3.

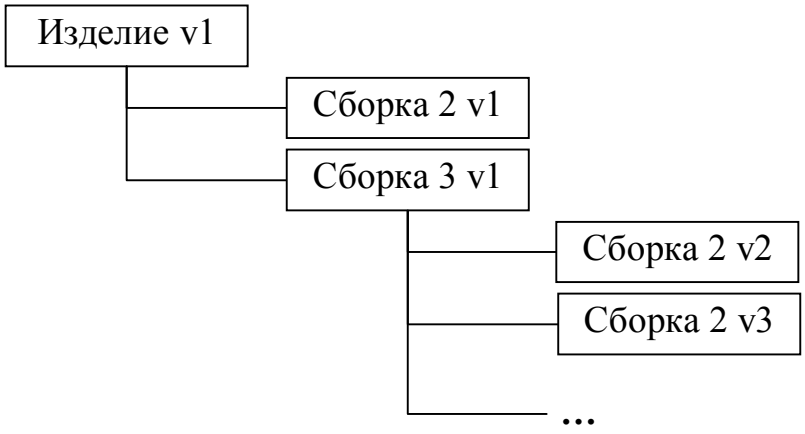


Рис. 3. Условная схема состава изделия для иллюстрации вариантов работы с одинаковыми изделиями

I. Такие составные части можно рассматривать независимо друг от друга, то есть в составе одного изделия могут находиться одинаковые изделия разных версий (Сборка 2 v1, Сборка 2 v2 и Сборка 2 v3). К каждой версии привязывается файл в CAD системе, соответственно изменение идет независимо.

Этот вариант позволят гибко подходить к вопросу состава изделия и может быть полезен во многих специфических случаях. Однако сложность реализации и сложность поддержки и понимания такой структуры не позволяют использовать его повсеместно.

II. Можно рассматривать все одинаковые изделия совместно, то есть все изделия, входящие в состав данного и имеющие название Сборка 2, будут всегда иметь одинаковую версию. Только один файл привязывается ко всем таким изделиям и его изменение с созданием новой версии приводит к одновременному изменению всех таких изделий. При таком способе возможны несколько вариантов понимания слова «одинаковые» – так, например, одинаковыми можно считать изделия, непосредственно входящие в состав данного, то есть находящиеся на следующем уровне иерархии, или рассматривать в качестве таких изделий все изделия на всех уровнях иерархии относительно данного.

III. Существует и третий способ, который позволяет считать изделия одинаковыми, если они ссылаются на один файл с моделью в CAD системе, и разными, если файлы различны. Таким образом, можно совместить положительные стороны первых двух методов.

Стратегия создания новых версий

Задача выбора времени создания новой версии только на первый взгляд кажется простой. Рассмотрим этот вопрос детальнее.

I. Можно создавать новую версию при каждом изменении изделия, например каждый раз, когда мы завершаем редактирование в CAD и обнаруживаем какие-либо изменения. Но при таком способе в системе будет храниться большое количество версий, являющихся промежуточными, что затрудняет управление версиями.

II. Можно также вводить другие критерии создания версий – например, по истечении определенного времени (новая версия появляется раз в неделю) или по какому-либо событию (все изменения попадают в новую версию, если предыдущая уже согласована).

III. Но наиболее гибким видится способ, при котором создание новой версии запрашивается у пользователя. При таком способе после завершения редактирования изделия в CAD пользователь должен указать, хочет ли он изменить текущую версию или создать новую. И, соответственно, количество версий ограничено реальной потребностью пользователя, а не внешними причинами.

Реализация

По результатам анализа для реализации были выбраны способы решения, учитывающие требования большинства пользователей, и, соответственно, позволяющие сделать систему более гибкой. Они были реализованы в рамках системы интеграции CAD и PDM систем и явились продолжением разработки унифицированного подхода.

В настоящее время интерфейсный компонент для PDM систем позволяет работать с PDM Step Suite, а в качестве интерфейсного компонента для CAD систем в состав комплекса включена библиотека GSCADLink [5], поддерживающий работу с SolidWorks, Pro/E, SolidEdge, Unigraphics, Inventor, Компас 3D, AutoCAD, PCAD и CATIA.

Обновление версий изделий проводилось по методу «управляемой автоматизации». Единственным недостатком данного метода по сравнению с остальными описанными в статье является сложность его программной реализации.

Работа с одинаковыми изделиями была реализована с возможностью обрабатывать их совместно или раздельно, в зависимости от того, на одинаковые ли файлы описания модели они ссылаются. Такой подход оказался очень удобен, поскольку данная реализация является прозрачной для пользователя и не вносит дополнительной сложности для большинства случаев, когда работа с одинаковыми изделиями ведется совместно, и в то же время позволяет в случае необходимости включать в состав изделия разных версий.

Новая версия в системе создается только тогда, когда это действительно необходимо – т.е. по желанию пользователя. Подход оказался очень удобен при наличии в проекте большого количества несущественных изменений.

Заключение

В настоящей работе были рассмотрены некоторые проблемы, возникающие при интеграции PDM и CAD систем, предложены методы их решения. Для каждого метода были рассмотрены его достоинства и недостатки. В заключение приведены результаты реализации выбранных решений в рамках разработки унифицированного подхода к интеграции PDM и CAD систем.

Литература

1. Голицына Т.Д. Проблемы интеграции PDM и CAD систем. Унифицированный подход. // Научно-технический вестник СПбГУ ИТМО. Выпуск 39. Исследования в области информационных технологий. Труды молодых ученых. – СПб: СПбГУ ИТМО, 2007. – С. 164–168.
2. Mason H. ISO 10303 – STEP A key standard for the global market. // ISO Bulletin. Апрель 2002. – С. 9–13.
3. ГОСТ Р ИСО 10303 «Системы автоматизации производства и их интеграция. Представление данных об изделии и обмен этими данными». М.: Госстандарт России. – 2000.
4. PDM STEP Suite. Техническое описание. // Официальный сайт НИЦ CALS-технологий «Прикладная логистика» http://pss.cals.ru/DOC/PSS_TD_2_1.pdf
5. GSCADLink. Описание. // Официальный сайт ООО «Глосис-Сервис» http://glosys.ru/products/cad/GSCADLink.htm

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПРОЕКТИРОВАНИЕ, ТЕХНОЛОГИЯ ЭЛЕМЕНТОВ И УЗЛОВ КОМПЬЮТЕРНЫХ СИСТЕМ

УДК 681.78

РАЗРАБОТКА СТАНДАРТНОЙ ПРОЦЕДУРЫ КОНТРОЛЯ ОБЪЕКТОВ ПРИРОДНОЙ СРЕДЫ НА БАЗЕ МЕТОДА ГРВ

Д.В. Орлов, Е.Н. Петрова
Научный руководитель – д.т.н., профессор К.Г. Коротков

Данная работа направлена на разработку стандартной процедуры проведения измерений объектов природной среды на ГРВ камере. В ходе исследований были выявлены дестабилизирующие факторы измерений и найдены пути их устранения. Предложена последовательность действий при проведении измерений, необходимая для обеспечения наиболее стабильных и адекватных результатов.
Ключевые слова: ГРВ, стандартная процедура, контроль, природная среда

Введение

Принципы регистрации цифровых газоразрядных изображений с последующей их компьютерной обработкой и анализом были развиты в работах д.т.н. Короткова К.Г. [1–4]. На этом принципе были созданы различные модификации приборов газоразрядной визуализации (ГРВ). Эти приборы используются для экспресс-диагностики состояния здоровья людей [1, 3], а также для исследования объектов природной среды [4]. С помощью ГРВ оборудования можно зарегистрировать динамику изменения исследуемого объекта или объектов природной среды, но нельзя оценить абсолютное значение параметров исследуемого объекта, например, электрической емкости или другой физической характеристики.

На получаемые во время проведения измерений результаты может влиять множество факторов, большая часть которых не представляют интереса для исследования и, более того, увеличивают погрешность измерений. К тому же при проведении подобных исследований не было сформулировано научно обоснованных методических правил проведения измерений. Это приводило к проблемам при трактовке, статистической обработке и обосновании достоверности полученных результатов.

Целью данной работы является выявление дестабилизирующих факторов, оказывающих влияние на получаемые результаты, выработка путей их устранения и разработка стандартной процедуры проведения измерений и обработки получаемых данных.

Методы исследований

Процедура формирования ГРВ-изображений с помощью прибора ГРВ заключается в следующем. Исследуемый объект помещается на кварцевый электрод, на обратную сторону которого нанесено прозрачное токопроводящее покрытие, на которое в течение заданного времени подаются импульсы напряжения от специализированного генератора. Мощность импульсов и длительность воздействия задаются программно в контуре управления. При высокой напряженности поля в пространстве между объектом и пластиной развивается лавинный и/или скользящий газовый разряд, характеристики которого определяются свойствами объекта. Пространственное распределение разряда фиксируется специализированной

видеокамерой (на базе ПЗС-матрицы), расположенной непосредственно под прозрачным электродом. Видеопреобразователь осуществляет оцифровку изображения и передачу его в компьютер для дальнейшей обработки. ГРВ-граммы обрабатываются в специально разработанном программном комплексе, где осуществляется расчет параметров изображений, таких как площадь и средняя интенсивность разряда.

Как было показано в целом ряде работ, именно эти параметры наиболее сильно коррелируют с физическими характеристиками исследуемого объекта, например, электрической емкостью [5].

В данной работе использовались приборы ГРВ серии "Компакт" с аналоговой видеокамерой (www.kti.spb.ru). Приборы ГРВ с цифровыми камерами требуют более длительного времени разогрева при проведении прецизионных исследований по сравнению с аналоговыми камерами [5]. Эксперименты производились при стандартных условиях: температура воздуха 21–25ºС, относительная влажность 26–30%.

Для проведения измерений на электрод помещался металлический цилиндр (1 см в диаметре и высотой 2 см) – тест-объект, который, в свою очередь, подключался к платиновому электроду, помещенному в сосуд с жидкостью, или к металлической антенне, расположенной в исследуемой области. Антенна используется для исследования газообразных сред.

Схема экспериментальной установки приведена на рис. 1.

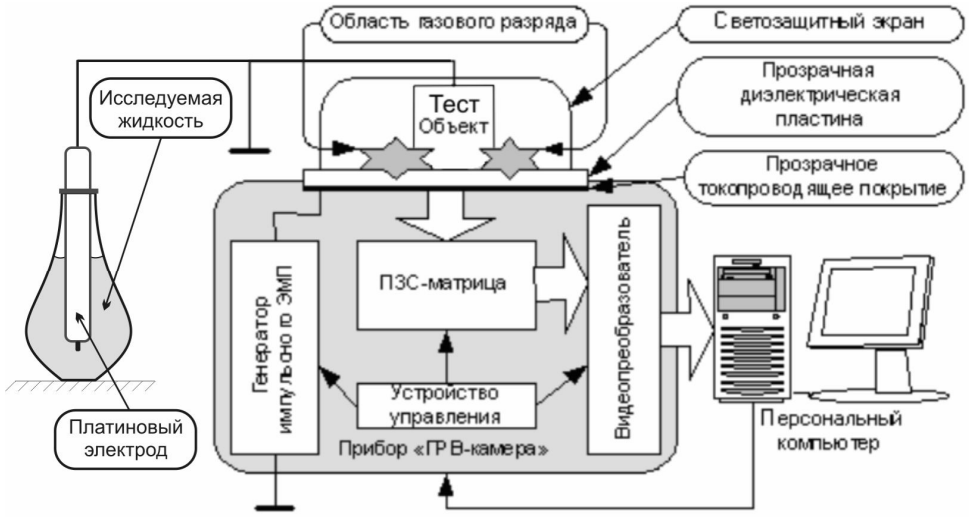


Рис. 1. Принципиальная схема экспериментальной установки

Обработка данных производилась в специально разработанном программном обеспечении "GDV Scientific Laboratory" производства компании "Kirlionics Technologies International"®.

Результаты и их обсуждение

Основные дестабилизирующие факторы

Плохое заземление

При отсутствии надлежащего заземления прибора и компьютера, подключённого к нему, происходит накопление на них статического заряда, что с течением времени может приводить к разрядке накопившегося заряда, что при длительных сериях измерений иногда приводит к самопроизвольному выключению или перезагрузке компьютера. Накапливающийся заряд также влияет на стабильность газового разряда, а, следовательно, и получаемых ГРВ-грамм. На рис. 2 приведен пример съемки при наличии и отсутствии заземления прибора ГРВ и персонального компьютера. Очевидна разница в разбросе значений площади ГРВ-грамм внутри серии.

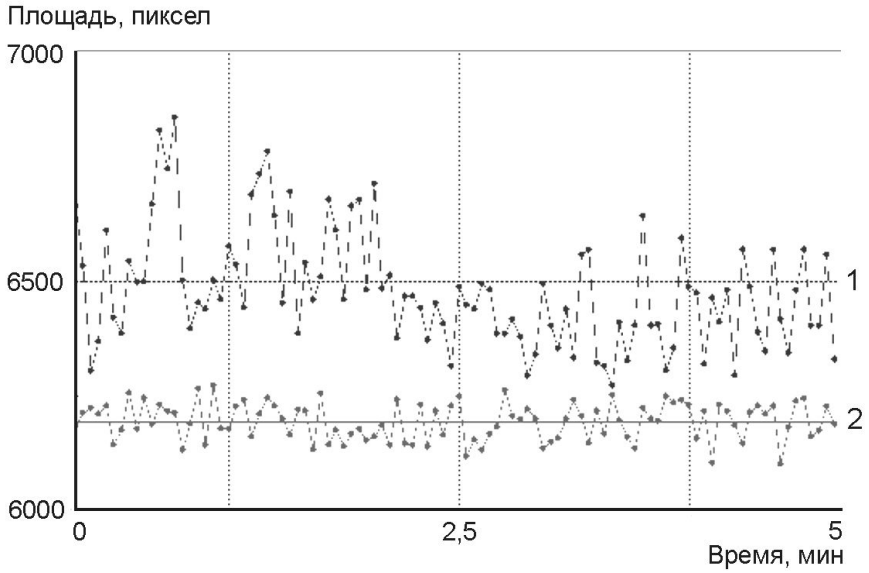


Рис. 2. Влияние заземления на разброс значений площади ГРВ-грамм:
1 – съемка без заземления; 2 – съемка с заземлением

Недостаточная вентиляция

При использовании стандартной для ГРВ приборов крышки, закрывающей электрод, не происходит необходимой вентиляции воздушного промежутка между крышкой и электродом, в результате чего происходит накопление озона. Накопление озона в значительной степени влияет на получаемые ГРВ-граммы и их параметры. На рис. 3 приведены результаты сравнения измерений с вентиляцией и без нее. Вентиляция осуществлялась при помощи вентилятора, стоящего рядом с прибором ГРВ. На графике отображены средние значения площади ГРВ-грамм в сериях, разделенных на 4 группы. Каждая группа состоит из четырёх последовательных серий измерений с различными значениями емкостей подключенных конденсаторов по возрастанию: 14пФ, 23пФ, 53пФ и 75пФ. Группы 1А и 2А сделаны последовательно без вентиляции, а группы 1Б и 2Б – с вентиляцией.

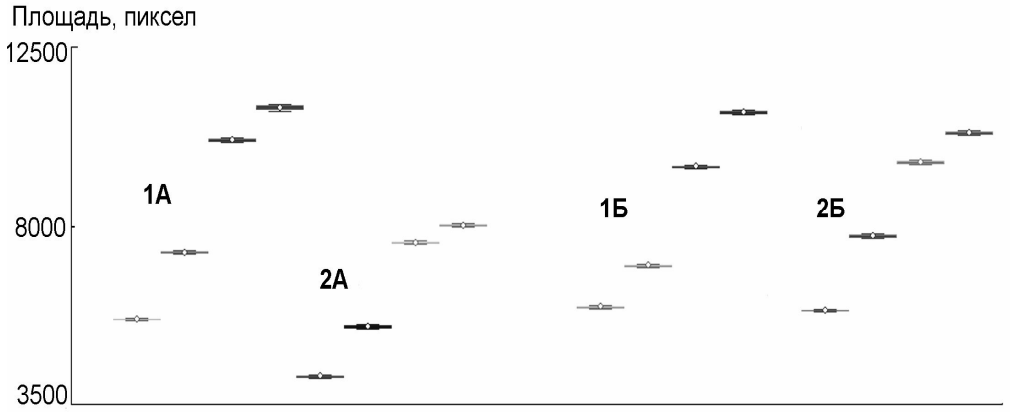


Рис. 3. Влияние вентиляции воздушного промежутка между сериями съёмок
на площадь ГРВ-грамм. 1А, 2А – последовательные серии без вентиляции;
1Б, 2Б – последовательные серии с вентиляцией

Как видно из представленных результатов, вентиляция оказывает существенное влияние на площадь ГРВ-грамм. Видно, что в группе Б воспроизводимость данных при последовательных измерениях существенно выше, чем в группе А. Это объясняется тем, что в отсутствии вентиляции в промежутке между крышкой и прозрачной пластиной накапливается озон, что значительно снижает площадь разряда.

Разогрев прибора

Прибору ГРВ требуется некоторое время для выхода на режим работы, при котором параметры ГРВ-грамм наиболее стабильны. Для исследованного нами образца прибора ГРВ серии «Компакт» стабильному уровню работы соответствует разброс значений средней интенсивности, не превышающий 1,35% от среднего значения в серии, а по площади – 2,95%. Явление "разогрева" прибора заключается в постепенном плавном увеличении значения средней интенсивности и уменьшении площади газового разряда после включения прибора до достижения стабильного уровня (рис. 4).

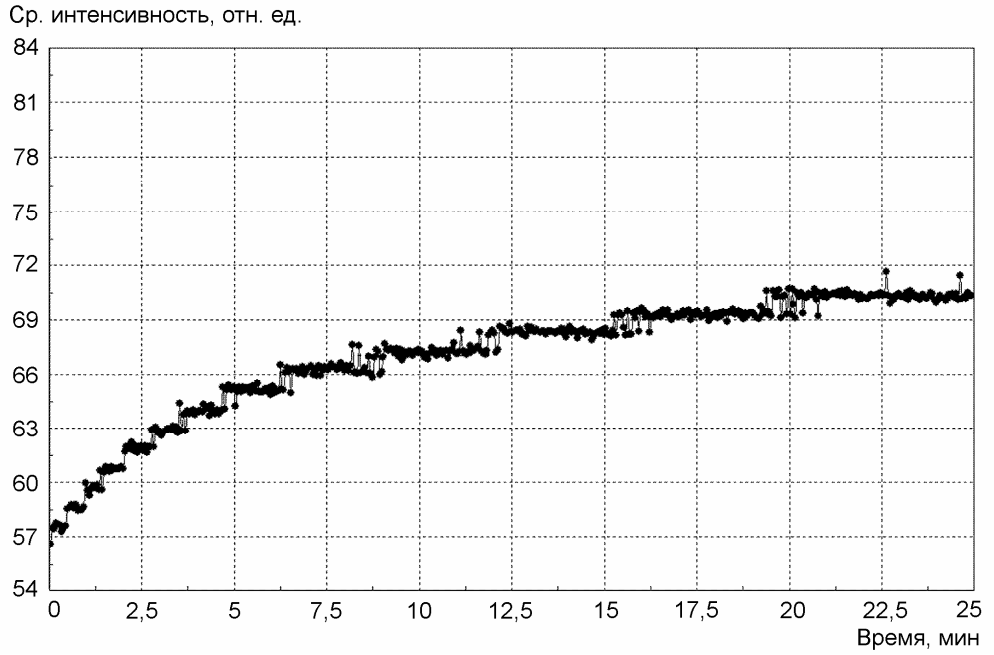


Рис. 4. Явление "разогрева" ГРВ-камеры

Для выхода на стабильный режим по средней интенсивности ГРВ-грамм необходимо произвести разогрев один раз после включения прибора, однако спад площади происходит внутри каждой серии на протяжении первых 40 разрядов.

Смещение тест-объекта

Одним из дестабилизирующих факторов является изменение положения тест-объекта на стеклянном электроде. Подобные действия значительно увеличивают разброс значений параметров ГРВ-грамм между сериями, что снижает стабильность получаемых результатов.

Изменение условий окружающей среды

Условия окружающей среды, например, влажность воздуха, температура, электромагнитный фон, оказывают влияние на развитие газового разряда. Например, включение какого-либо электрического прибора в помещении, в котором производятся измерения на приборе ГРВ, может привести к изменению электромагнитного фона, что, в свою очередь, скажется на получаемых ГРВ-граммах.

Одинаковыми условиями проведения измерений на приборах ГРВ считаются такие, при которых средние значения площади и средней интенсивности серий ГРВ-грамм лежат в пределах ±1,9 % по площади и ±1,5% по средней интенсивности.

Интервал между разрядами

Эксперименты показали, что при временном интервале 3 с между разрядами разброс значений параметров площади и средней интенсивности значительно больше, чем при интервале, равном 5 с.

Общие рекомендации

Исходя из перечисленных дестабилизирующих факторов, были сформулированы общие рекомендации проведения прецизионных измерений на приборах ГРВ:

1. Обеспечить заземление прибора ГРВ и компьютера.
2. Во время проведения длительных непрерывных измерений (десятки минут и более) необходимо обеспечивать постоянное вентилирование, например, при помощи установленного рядом с прибором ГРВ (не ближе 0,2 метра) вентилятора.
3. Перед началом измерений необходимо производить "разогревочную" серию длительностью 600 разрядов с интервалом 3 секунды при замыкании тест-объекта на "землю" прибора.
4. Разогрев нужно производить при интервале 3 с, измерения проводить при временном промежутке между разрядами 5 с.
5. Тест-объект следует аккуратно устанавливать перед началом эксперимента и не передвигать, пока эксперимент не будет закончен и все нужные серии отсняты.
6. Необходимо следить за условиями окружающей среды.
   - Перепады влажности воздуха не должны превышать 5%.
   - Перепады температуры воздуха не должны превышать 5 ºС.
   - Не включать/выключать электрические приборы во время проведения экспериментов в комнате, в которой стоит ГРВ прибор.
   - Не разговаривать по сотовому телефону вблизи ГРВ прибора.
   - Количество людей находящихся рядом с прибором должно быть постоянным.
   - Избегать резких перепадов атмосферного давления.
   - Следить за изменением геомагнитного фона (заход/восход Солнца и Луны и пр.).
7. Длительность каждой серии измерений должна быть не менее 140 ГРВ-грамм.
8. При обработке результатов исключать первые 40 снимков из расчета.
9. После каждого изменения условий окружающей среды следует производить калибровку. Для этого можно использовать последние 10 снимков из "разогревочной" серии.

Стандартная процедура

В каждом конкретном эксперименте необходимо тщательно продумывать процедуру проведения измерений. Необходимо соблюдать перечисленные выше требования.

Любой эксперимент по исследованию определенного воздействия можно разбить на три этапа: 1 – до воздействия (фон), 2 – воздействие, 3 – после воздействия (последействие).

Эксперимент должен в итоге отвечать следующим параметрам:

– любой эксперимент необходимо повторять при одинаковых условиях как минимум четыре раза подряд (минимальное количество экспериментов обусловлено статистическим критерием, который используется для определения статистического различия между сериями «до» и «после»;

– из полученных серий будут выделяться две группы: 1-ая, состоящая из всех серий первого этапа, и 2-ая, состоящая из всех серий третьего этапа.

Перед началом непосредственного исследования воздействия следует проверить саму процедуру измерений на стабильность. Для чего надо выполнить следующие шаги, исключив второй этап эксперимента, то есть само воздействие:

1. Повторить эксперимент как минимум 4 раза.

2. Проверить каждую серию на разброс значений площади и средней интенсивности ГРВ-грамм, чтобы удостовериться в том, что условия проведения измерений оставались стабильными в течение каждой из серий. Воспользовавшись формулой: $\Delta_{вн} = \frac{\sigma}{\overline{A}} \cdot 100$, где $\Delta_{вн}$ – разброс значений параметра ГРВ-грамм внутри серии, %; σ – среднеквадратическое отклонение (СКО); $\overline{A}$ – среднее значение параметра ГРВ-граммы в серии; вычислить разбросы площади и средней

интенсивности ГРВ-грамм. Значения σ и $\overline{A}$ можно рассчитать в программе "GDV Scientific Laboratory". Рассчитанные значения не должны превышать следующих пороговых значений: 2,95% для площади и 1,35% для средней интенсивности. Если рассчитанные значения для какой-либо серии превышают порог, такую серию следует переснять.

3. Проверить являются ли условия проведения экспериментов одинаковыми для каждой из двух полученных групп в отдельности. Вычислить среднее значение средних значений параметров ГРВ-грамм внутри каждой группы по формуле: $\overline{A}_{меж} = \frac{\sum_{i=1}^{n} \overline{A_i}}{n}$, где $\overline{A}_{меж}$ – среднее средних значений параметра группы; $\overline{A_i}$ – среднее значение параметра i-той серии; *n* – количество серий. Если среднее значение $\overline{A_i}$ какой-либо серии отличается на ±1,9% по площади или на ±1,5% по средней интенсивности от $\overline{A}_{меж}$, то эту серию следует переснять.

4. При помощи статистического непараметрического метода Манна-Уитни [6, 7] выявить имеют ли группы серий «до воздействия» и «после воздействия» статистически достоверное различие.

5. Если различие есть, необходимо рассчитать для каждого эксперимента по отдельности разницу значений параметров ГРВ-грамм (площади и средней интенсивности) и найти среднее значение этой разницы.

В случае правильно поставленного эксперимента статистически значимой разницы между значениями параметров ГРВ-грамм не должно быть. Если же разница есть, то следует еще раз перепроверить правильность постановки эксперимента и повторить все шаги с 1-го по 5-ый.

Как только процедура измерений налажена, проверена и не оказывает значимого влияния на объект исследования, то можно переходить к непосредственным измерениям исследуемого воздействия.

Следует выполнить все шаги (пп. 1–5), но включив в эксперимент второй этап – само воздействие. Если различие не обнаруживается, то следует еще раз проверить стабильность условий проведения измерений, и если повторная проверка ничего не даст, то это означает, что данный метод не позволяет статистически достоверно зарегистрировать оказанное воздействие.

Заключение

В результате проведенной работы были разработаны общие рекомендации и стандартная процедура проведения измерений объектов окружающей среды на базе метода ГРВ. Четко следуя этим рекомендациям и процедуре исследований можно получать статистически достоверные результаты. А благодаря предложенному алгоритму обработки получаемых результатов можно легко обрабатывать и интерпретировать данные.

Литература

1. Коротков К.Г. Основы ГРВ биоэлектрографии. – СПб.: ИТМО (ТУ), 2001. – 356 с.
2. Коротков К.Г. Эффект Кирлиан. – СПб: Ольга, 1995. – 218 с.
3. Коротков К.Г. От эффекта Кирлиан к биоэлектрографии. – СПб: Ольга, 1998. – 341 с.

4. Коротков К.Г. Разработка научных основ и практическая реализация биотехнических измерительно-вычислительных систем анализа газоразрядного свечения, индуцированного объектами биологической природы: дис. док. техн. наук. – СПб: СПбГИТМО (ТУ), 1999. – 93 с.
5. Орлов Д.В., Петрова Е.Н., Чайкун К.Е. Параметрические зависимости частотно-резонансных оптоэлектронных контуров. – Матер. V ВМК молодых ученых СПбГУ ИТМО, 2008.
6. Вуколов Э.А. Основы статистического анализа. Практикум по статистическим методам и исследованию операций с использованием пакетов STATISTICA и EXCEL: Учебное пособие. – М.: ФОРУМ: ИНФРА-М, 2004. – 464 с.
7. Гланц С. Медико-биологическая статистика. Пер. с англ. – М.: Практика, 1998. – 459 с.

УДК 681.78: 616.71

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ КОНТРОЛЯ МЕДИКО-БИОЛОГИЧЕСКИХ ПАРАМЕТРОВ И ОКРУЖАЮЩЕЙ СРЕДЫ

Е.Н. Петрова, Д.В. Орлов
Научный руководитель – д.т.н., профессор К.Г. Коротков

Разработан новый программно-аппаратный комплекс для исследования состояния основных систем организма и контроля состояния окружающей среды. Комплекс позволяет проводить диагностику основных функциональных систем организма путем анализа ряда медико-биологических параметров экспресс-методами диагностики. Контроль состояния окружающей среды реализован посредством измерений объектов окружающей среды методом газоразрядной визуализации.

Ключевые слова: программно-аппаратный комплекс, контроль окружающей среды, медико-биологические параметры, диагностика

Введение

Исследование медико-биологических параметров играет важную роль как в медицине – для диагностики состояния организма, так и в экологических исследованиях – для оценки окружающей среды, в частности. В современной медицине существует множество диагностических методов, позволяющих провести обследования различной сложности. Однако создание комплекса превентивной экспресс диагностики состояния человека остается важной и актуальной задачей. В исследованиях окружающей среды важным вопросом контроля также является ее воздействие на состояние человека.

В настоящей статье представлены принцип построения и структура разработанного нового программно-аппаратного комплекса (ПАК) исследования состояния человека и окружающей среды путем регистрации и анализа медико-биологических параметров.

Методы и результаты исследования

Комплекс включает в себя методы экспресс диагностики состояния основных физиологических систем организма и экспресс-метод оценки окружающей среды (ГРВ). ПАК включает в себя следующие методы исследования:

- газоразрядная визуализация (ГРВ);
- анализ вариабельности сердечного ритма (ВСР);
- электросоматография (ЭСГ);
- эргоспирометрия (ЭСМ).

Выбор методик был обусловлен комплексностью и быстротой проведения обследования, направленного на превентивный анализ состояния основных органов и систем организма человека. Кроме того, перечисленные методы экспресс диагностики позволяют проводить исследования и анализировать влияние на состояние человека различных факторов, в том числе, воздействия окружающей среды.

Метод ГРВ, разработанный под руководством профессора К.Г. Короткова, основан на регистрации и последующем анализе цифровых газоразрядных изображений [1–4]. Одними из наиболее широко применяемых на практике направлений исследований, проводимых методом ГРВ, являются экспресс-диагностика состояния здоровья людей и исследование объектов природной среды [1, 2].

В методе ГРВ производится анализ газоразрядного свечения 10 пальцев рук человека [1]. При этом ГРВ программный комплекс позволяет анализировать такие параметры, как площадь свечения, интенсивность, симметрия свечения пальцев на правой и

левой руках, в результате чего осуществляется проведение секторной диагностики по различным органам и системам.

Анализ вариабельности сердечного ритма позволяет провести диагностику сердечно-сосудистой системы и определить степень напряжения регуляторных систем организма [5]. При анализе ВСР производится регистрация электрокардиографического сигнала в течение пяти минут. Метод ВСР использует связь вариабельности ритма сердца с функциональным состоянием вегетативной нервной системы. Система обеспечивает вычисление более 30 различных показателей ВСР, определяет показатели работы сердечно-сосудистой и вегетативной нервной системы, такие как индекс вегетативного равновесия (ИВР), вегетативный показатель ритма (ВПР), показатель активности процессов регуляции (ПАПР), индекс напряженности (ИН). Анализ вариабельности ритма сердца проводится в реальном масштабе времени с отображением на экране текущей электрокардиограммы, процесса распознавания R-зубцов и динамического ряда R-R-интервалов.

Существует система экспресс диагностики состояния основных систем организма по анализу объемной электропроводности внутренних сред организма (электросоматография) [6]. В методе ЭСГ диагностика осуществляется путём измерения биоэлектрического импеданса человеческого организма. Наложение 6 электродов для перекрестного сканирования позволяет снять показания практически со всех участков тела (каждый электрод попеременно служит катодом и анодом). Для моделирования биохимических показателей используется метод электрохимического анализа.

Эргоспирометрические показатели позволяют оценить состояние респираторной системы, определить функциональное состояние легких и характеризовать функции внешнего дыхания.

Таким образом, комплекс экспресс методик, входящих в состав ПАК позволяет провести диагностику основных функциональных систем организма. При этом производится регистрация перечисленных выше медико-биологических параметров с последующей компьютерной обработкой и анализом результатов. ПАК позволяет провести экспресс обследование состояния организма человека и основных функциональных систем за 20– 25 минут.

Структурная схема разработанного ПАК представлена на рис. 1.

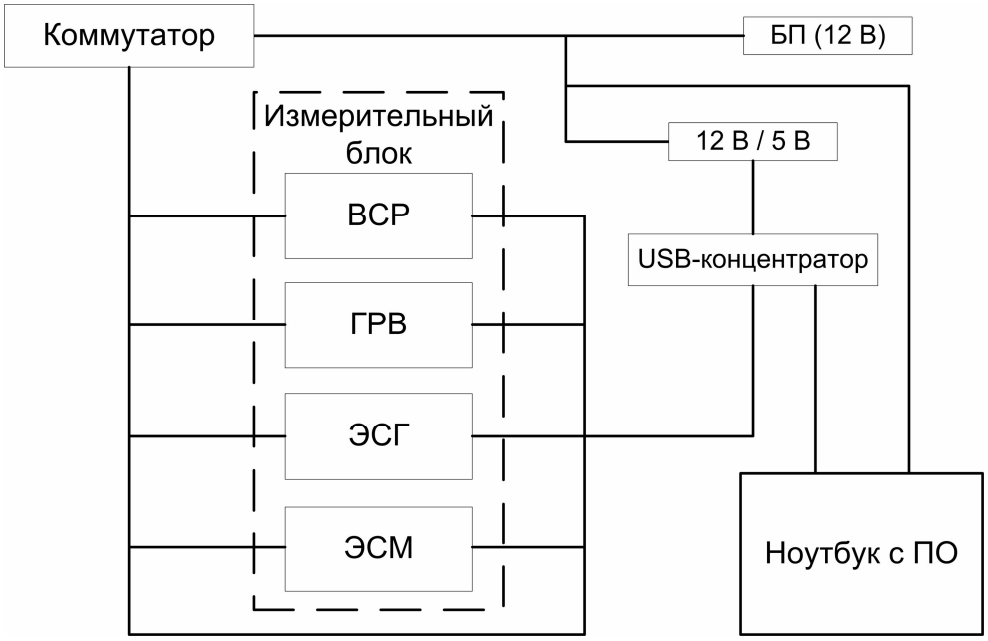


Рис. 1. Структурная схема прграммно-аппаратного комплекса

Относительно новым направлением исследований является не просто экологическое исследование различных мест и объектов, но исследование влияния нахождения в исследуемых местах на состояние человека. Поэтому в разработанном ПАК предусмотрена возможность контроля состояния окружающей среды посредством двух вариантов исследований:

1. Исследование параметров объектов окружающей среды (вода, воздух и др. материалы) методом ГРВ [1, 2].
2. Комплексное экспресс исследование состояния человека до и после нахождения в определенной окружающей среде (методы ГРВ, ВСР, ЭСГ);

Важным достоинством комплекса является его разработка на принципе расширяемости, что позволяет дополнять или заменять входящие в состав комплекса методы новыми перспективными методами исследований или подключать дополнительные методы, необходимые для определенных исследований.

Заключение

Разработанный программно-аппаратный комплекс контроля медико-биологических параметров и окружающей среды позволяет быстро произвести диагностику основных физиологических систем организма и оценить состояние окружающей среды и характер ее воздействия на человека.

Литература

1. Коротков К.Г. Основы ГРВ биоэлектрографии. – СПб.: ИТМО (ТУ), 2001. – 356 с.
2. Коротков К.Г. Принципы анализа ГРВ биоэлектрографии. – СПб.: Изд-во «Реноме», 2007. – 286 с.
3. Коротков К.Г., Матраверс П., Орлов Д.В., Вильямс Б.О. Обзор публикаций по применению метода газоразрядной визуализации (ГРВ) в медицине // Тезисы XII Международного Научного Конгресса по Биоэлектрографии. – СПб, 2008. – С. 6–9.
4. Коротков К.Г., Короткова А.К. Инновационные технологии в спорте: исследование психофизиологического состояния спортсменов методом газоразрядной визуализации. – М: Советский спорт, 2008. – 280 с.
5. Машин В.А., Машина М.Н. Классификация функциональных состояний и диагностика психоэмоциональной устойчивости на основе факторной структуры показателей вариабельности сердечного ритма // Российский физиологический журнал им. И.М. Сеченова. – М. – 2004. – Т. 90. – N 12. – С. 1508–1521.
6. http://www.ddfao.ru

УДК 004.047

ЛОГИЧЕСКАЯ СТРУКТУРА ОРГАНИЗАЦИИ МОДУЛЬНОГО СЕРВЕРНОГО ПРИЛОЖЕНИЯ НА ЯЗЫКЕ PHP

А.Ю. Гришенцев, Е.Н. Петрова
Научный руководитель – д.т.н., профессор К.Г. Коротков

Рассмотрены вопросы разделения интернет приложения на взаимодействующие модули, с целью улучшения бизнес логики приложения и повышения безопасности на базе объектно-ориентированного языка программирования PHP 5.

Ключевые слова: программирование, интернет, PHP

Введение

Разделение интернет приложения на отдельные целевые модули, называемое так же бизнес логикой, необходимо с точки зрения отделения XHTML (HTML, xml) кода определяющего дизайн сайта от скриптовой Perl или PHP программной части, такой подход позволяет максимально разделить труд дизайнера и программиста, повысить читаемость, изменение и (или) редактирование кода.

Задачи разработки логической структуры

Задачей разработки является получение логической структуры серверного приложения разделенной на максимально независимые модули, позволяющие облегчить процессы расширения приложения, изменения дизайна, в то же время обеспечивающие безопасность приложения с точки зрения URL атак.

Модульная организация серверного приложения

Для решения задачи рассматриваемой в данной статье, часто применяют систему активных шаблонов [1] подобных Smarty. Smarty это достаточно мощная и гибкая система целиком реализованная на PHP. Но PHP является сам по себе мощным инструментом [2] и позволяет решать подобные задачи достаточно лаконично, не привлекая сторонних библиотек. Применение системы активных шаблонов хорошее решение вопроса в том случае если разработкой интернет приложения занимается только дизайнер не привлекая программиста. Определенные стандарты характерные сторонним библиотекам во многом определяют логическую организацию приложения, причем влияние оказывается на концептуальном уровне. Для некоторых приложений такое влияние не всегда полезно. Рассмотрим пример реализации бизнес логики интернет приложения только силами стандартного PHP (рис. 1).

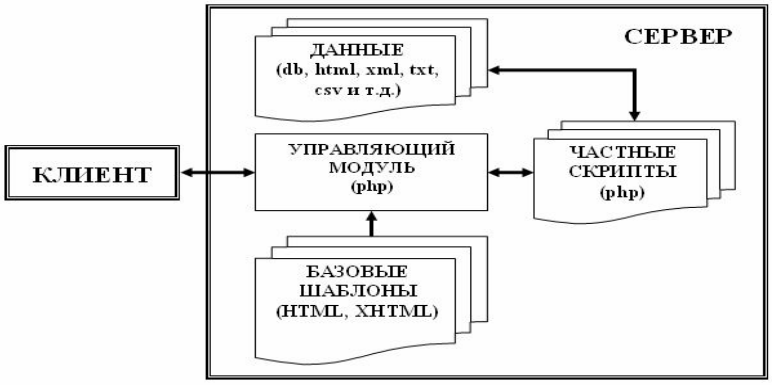


Рис. 1. Блок-схема модульной организации серверного приложения

При передаче управления на сервере «управляющему модулю» происходит анализ URL адреса на основании которого выбирается PHP скрипит (или набор скриптов) из коллекции «частные скрипты», выбранные скрипты производят обмен данными с модулем «данные», далее данные сформированные работающими скриптами возвращаться «управляющему модулю», где происходит выбор шаблона из набора «базовые шаблоны» на основании полученных данных от скриптов. Набор «базовые шаблоны» представляют собой набор готовых HTML файлов содержащих код представления внешнего вида страниц.

Уточним некоторые особенности предлагаемой модульной структуры (рис.1). Анализ URL адреса происходит в управляющем модуле один раз, в результате анализа некоторым переменным, а возможно свойствам объектов некоторого класса, присваиваться определенные значения. Далее все решения принимаются на основании присвоенных значений, и не связанных с URL. Таким образом происходит централизованный анализ URL и отделение внутренней логики работы приложения от внешних данных. Анализ URL позволяет исключить возможность внешних URL атак. Очевидно, что при использовании данной схемы, внутренние данные сервера доступные из PHP отделены от управляющего модуля набором частных скриптов, что является положительным фактором для безопасности, в рамках PHP. Также отделены данные ответственные за внешний вид страницы, при таком подходе их замена, редактирование не представляет сложностей для дизайнера.

Анализ URL лучше всего производить с помощью специального класса, этот класс можно дополнить методом формирующим URL и везде где на странице сайта сформированного приложением будут встречаться внутренние ссылки формировать эти ссылки с помощью данного метода. Такой подход особенно актуален при использовании сервера Apache, т.к. это позволит производить переадресацию при помощи управляющего файла .htaccess [3] в результате которой происходит замена URL на сервере. Например, адрес представленный в браузере клиента http://www.example.com/test/one, в php может быть передан как http://www.example.com/index.php?test=one, соответственно управление будет передано файлу index.php. Такой подход позволяет скрыть структуру сайта от клиента, оптимизировать сайт для работы некоторых поисковых систем чувствительных к URL.

Шаблон HTML кода содержит минимальные вставки PHP, например: <? echo $content ?>, где $content – переменная содержащая требуемый для вставки на данную страницу HTML код.

Обсуждение

В литературе посвященной вопросам программной организации достаточно хорошо рассмотрены универсальные методы разделения PHP и HTML, но имея универсальность такие методы обычно имеют приличный объем кода, что делает их на взгляд автора не очень удобными. Предложенная в статье методика позволяет сделать решение проблемы модульной организации при минимальном количестве кода, при этом если возникает необходимость поменять доменное имя или всю логическую структуру сайта редактировать необходимо лишь несколько строк в объекте одного класса. Анализ URL на самых ранних этапах работы скрипта позволяет максимально защитится от внешних URL атак, таких например, как запуск скрипта на сервере злоумышленника. Дополнительным достоинством предложенного метода является отделение частных скриптов формирования отдельных страниц и работы с данными от управляющего модуля, это позволяет сократить объем исполняемых файлов, а значит освободить дополнительные вычислительные ресурсы и увеличить скорость работы скрипта.

Заключение

В статье предложен метод отделения программной части PHP кода от части HTML отвечающей за дизайн. Достаточно высокая универсальность метода, при простоте реализации позволяет легко использовать его для организации бизнес логики серверного (или серверной части клиент-серверного) приложения. Предложенный метод позволяет обеспечить гарантированную безопасность приложения с точки зрения URL атак.

Литература

1. Скляр Д., Трахтенберг А. PHP. Рецепты программирования, 2-е изд.: Пер., с англ. – М.: изд-во «Русская Редакция»; СПб.: «БХВ-Петербург», 2007. – 736 с.: ил.
2. Веллинг Л., Томсон Л. Разработка WEB-приложений с помощью PHP и MySQL, 3-е изд.: Пер., с англ. – М издательский дом «Вильямс», 2008. – 800 с.: ил.
3. Таймен Б. FreeBSD 6 полное руководство, Пер., с англ. – М издательский дом «Вильямс», 2008. – 1056 с.: ил.

УДК 003.26.09

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ СТЕГАНОГРАФИИ ПРИ ПРОВЕДЕНИИ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

А.В. Кущ
Научный руководитель – д.т.н., профессор А.Г. Коробейников

В работе приводятся наиболее эффективные алгоритмы стегоанализа, позволяющие не только сделать вывод о наличии или отсутствии в контейнере внедренной информации, но и определить примерную длину внедренного сообщения, а так, же приведены результаты экспериментальных исследований подсистемы стегоанализа изображений, применяемой при компьютерно-технической экспертизе.
Ключевые слова: стеганографический анализ, стеганографический алгоритм, атака хи-квадрат, метод RS-анализа, атака «Анализ пар»

Введение

Глобальная компьютеризация, стремительное развитие сферы высоких технологий, компьютерная эра мирового сообщества наряду с положительными тенденциями развития мирового сообщества открывает также новые возможности для развития и совершенствования преступного мира, криминализирует общественно-правовые отношения в данной сфере. А потому значение компьютерной криминалистической информации для раскрытия и расследования преступлений против собственности и в сфере хозяйственной деятельности трудно переоценить.

В последнее время особую популярность приобретают программные средства защиты информации, включающие в себя не только обычную криптографию, но и стеганографические средства скрытия информации. Суть последних заключается в том, что они не только делают информацию недоступной для прочтения без знания пароля, но и скрывают сам факт существования секретной информации, внедряя ее в какой-либо файл-контейнер (html – страницу, изображение, аудиофайл, исполняемый модуль и др.). Таким образом, особой задачей компьютерно-технического эксперта является задача поиска и анализа скрытой и зашифрованной информации подозреваемого, так как она может быть наиболее важной для следствия [1].

Задача пассивного стегоанализа, рассматриваемого в этой работе, состоит в обнаружении факта наличия скрытой информации в файле – контейнере без разрушения этой информации. В этом случае эксперт обычно имеет изображение, которое нужно отнести его к одному из двух классов: содержащих или не содержащих скрытое сообщение. Дополнительно к этому может ставиться задача оценки длины внедренного сообщения. Рассмотрим статистические атаки на стеганографические системы.

Атака Хи-квадрат

Для выявления факта существования скрытого канала передачи информации одним из наиболее перспективных является подход, представляющий введение в файл скрываемой информации как нарушение статистических закономерностей естественных контейнеров.

При таком подходе анализируются статистические характеристики исследуемой последовательности и устанавливается, похожи ли они на характеристики естественных контейнеров (если да, то скрытой передачи информации нет), или они похожи на характеристики стего (если да, то выявлен факт существования скрытого канала передачи информации).

Исследуем закономерности в вероятностях появления значений яркостной компоненты в естественных контейнерах и сформированных программой Steganos стего.

Степень различия между вероятностными распределениями элементов естественных контейнеров и полученных из них стего также может быть использована для оценки вероятности существования стегоканала.

Данную вероятность удобно определить с использованием критерия согласия Хи-квадрат [2].

Зная общее число n появления всех элементов исследуемой последовательности, легко подсчитать ожидаемую вероятность появления этих элементов в стего по правилу: $p_i = n_i / n$. Соответственно, для исследуемой последовательности вероятности равны: $p_i^* = n_i^* / n$.

Величина Хи-квадрат для сравниваемого распределения исследуемой последовательности и ожидаемого распределения стего равна:

$$\chi^2 = \sum_{i=1}^{\nu} \frac{(n_i - np_i)^2}{np_i}, \quad (1)$$

где k – число элементов последовательности; n_i – число совпадений рассматриваемого значения со значением элемента x_i; ν – число степеней свободы. Число степеней свободы равно числу k минус число независимых условий, наложенных на вероятности p_i^*. Наложим одно условие вида:

$$\sum_{i=1}^{k} p_i^* = 1. \quad (2)$$

Вероятность p того, что два распределения одинаковы, определяется как:

$$p = 1 - \int_0^{\chi^2} \frac{t^{(\nu-2)/2} e^{-t/2}}{2^{\nu/2}\Gamma^{\nu/2}}, \quad (3)$$

где Γ – гамма-функция Эйлера

Чем больше значение p, тем выше вероятность встраивания скрываемой информации в исследуемую последовательность.

Метод RS-анализа

Одним из оригинальных методов статистического стегоанализа является метод RS, впервые опубликованным в 2001 г. коллективом ученых под руководством Дж. Фридрих [2, 3]. Сокращение в названии расшифровывается как Regular-Singular, то есть «регулярно-сингулярный».

Суть метода состоит в следующем. Все изображение разбивается на группы по n пикселов $G(x_1, x_2, ..., x_n)$ где n четно, например по 2 пиксела, находящихся рядом по горизонтали. Для группы пикселов определяется функция регулярности или «гладкости» $f(G)$, в качестве такой функции можно выбрать, например, дисперсию значений внутри группы, либо просто сумму перепадов значений смежных пикселов. Под значением пиксела понимаем целое число от 0 до 255.

$$f(x_1, x_2, ..., x_n) = \sum_{i=1}^{n-1} |x_{i+1} - x_i|. \quad (4)$$

Функция F(x) называется флиппингом и имеет свойство F(F(x))=x. Определим две функции флиппинга – F_1, соответствует инверсии младшего бита пиксела, и F_2, представляющая собой инверсию с переносом в старший бит (прибавление единицы).

F_1: 0 ↔ 1, 2 ↔ 3, …, 254 ↔ 255

F_{-1}: 255 ↔ 0, 1 ↔ 2, 3 ↔ 4,…,253 ↔ 254, 255 ↔ 0

При применении флиппинга к группе получаем преобразованную группу пикселов. Далее, поделим все группы пикселов на классы следующим образом:

(1) Регулярные группы: $G \in R \Leftrightarrow f(F(G)) > f(G)$,

(2) Сингулярные группы: $G \in S \Leftrightarrow f(F(G)) < f(G)$,

(3) Неиспользуемые группы: $G \in U \Leftrightarrow f(F(G)) = f(G)$.

Метод основывается на статистическом предположении, что для естественного изображения, другими словами, незаполненного контейнера, характерно следующее:

$R_M \cong R_{-M}$ и $S_M \cong S_{-M}$. (5)

Предположение основано на том, что применение F_{-1} даст то же распределение, что и F_1 на изображении, значения пикселов которого сдвинуты на единицу. Для обыкновенного изображения соотношение между группами не должно существенно меняться. Значительное расхождение между значениями свидетельствует о применении LSB-стеганографии для младших бит изображения.

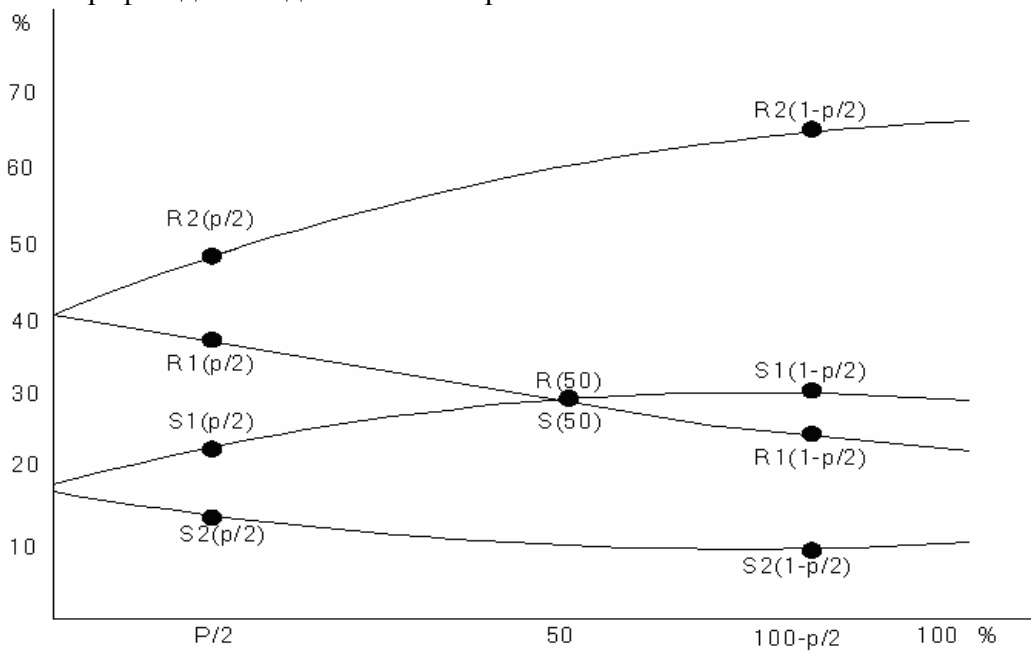


Рис. 1. RS-диаграмма типичного изображения

Рассмотрим изменения младших бит изображения при 100% перезаписи их битами сообщения. Внедрение случайного сообщения длиной, равной размеру изображения, приведет к тому, что 50% младших бит будут инвертированы. Это, в свою очередь сведет к нулю разность между значениями R_M и S_M. Однако на R_{-M} и S_{-M} внедрение сообщения будет влиять прямо противоположно, и разность этих величин будет пропорциональна степени заполненности контейнера, иными словами длине сообщения. На рис. 1 приведена RS – диаграмма для типичного изображения. На оси абсцисс расположено количество инвертированных бит x, искомая длина сообщения p, на оси ординат – относительные значения регулярных и сингулярных групп по отношению к общему числу групп изображения.

Предполагая, что в изображение внесено сообщение длиной p бит, и при этом 50 % младших бит, использованных для записи, будут инвертированы, мы получаем значения статистик в точке p/2. Затем, если инвертировать все младшие биты изображения и пересчитать статистики, на диаграмме они будут соответствовать точкам кривых при x=100-p/2. Полной рандомизации младшей битовой плоскости соответствует точка ½. Теперь, если принять p/2 за ноль, а 100-p/2 за единицу, а также использовать аппроксимацию кривых R_{-M} и S_{-M} прямыми а R_M и S_M параболами, можно вывести квадратное уравнение для нахождения координаты точки пересечения кривых R_M и S_M:

$$2(d_1 + d_0)x^2 + (d_{-0} - d_{-1} - d_1 - 3d_0)x + d_0 - d_{-0} = 0.$$

Затем, длина сообщения p вычисляется как p = x/(x−1/2). Таким образом, выходное значение длины является ответом для данного метода.

Атака «Анализ пар»

Для изображений с палитрой, в которые сообщение вкладывается по алгоритму *EzStego*, можно использовать атаку, которую назвали анализом пар.

Метод основан на поиске закономерности в вероятностях появления значений яркости в естественных изображениях и изображениях со встроенным ЦВЗ. При замене младшего бита цветовой компоненты очередного пиксела изображения на очередной бит предварительно зашифрованного или сжатого ЦВЗ, значение яркости пиксела модифицированного изображения либо равно значению яркости пиксела контейнера, либо изменяется на единицу с вероятностью ~1/2. Для поиска следов встраивания был предложен метод анализа закономерностей в частотах появления «соседних» значений яркости. Такие пары значений («Pair of Values») различаются только значением наименее значащего бита. Значение яркости, двоичное представление которого заканчивается нулевым битом l, назовем «левым» (L), а соседнее с ним значение яркости, двоичное представление которого заканчивается единичным битом – «правым» (R). Пусть цветовая гамма исходного контейнера включает 8 цветов. Следовательно, при встраивании сообщения в НЗБ цветовой компоненты пикселов необходимо исследовать статистические характеристики в 4 парах номеров цвета. При замещении битами внедряемого сообщения младших битов яркостной компоненты пикселов контейнера-изображения проявляются аналогичные статистические различия [4].

Экспериментальное исследование подсистемы стегоанализа изображений

Поскольку алгоритмы, реализованные в подсистеме стегоанализа изображений, дают эксперту возможность оценить примерную длину внедренного сообщения, то и успешность работы этих алгоритмов нужно оценивать по той точности, с которой они определяют длину вложенного сообщения. Для тестирования были отобраны 50 изображений формата BMP (изображения с палитрой), конвертированные из формата JPEG с устранением артефактов JPEG-преобразования и удалением шума. Для тестирования RS-анализа и анализа пар, приведенного на рис. 4, в изображение по случайному пути внедрялась псевдослучайная последовательность битов, модифицирующая 0, 25, 50, 75 и 100% пикселей. На рис. 3 приведены результаты RS-анализа палитрой.

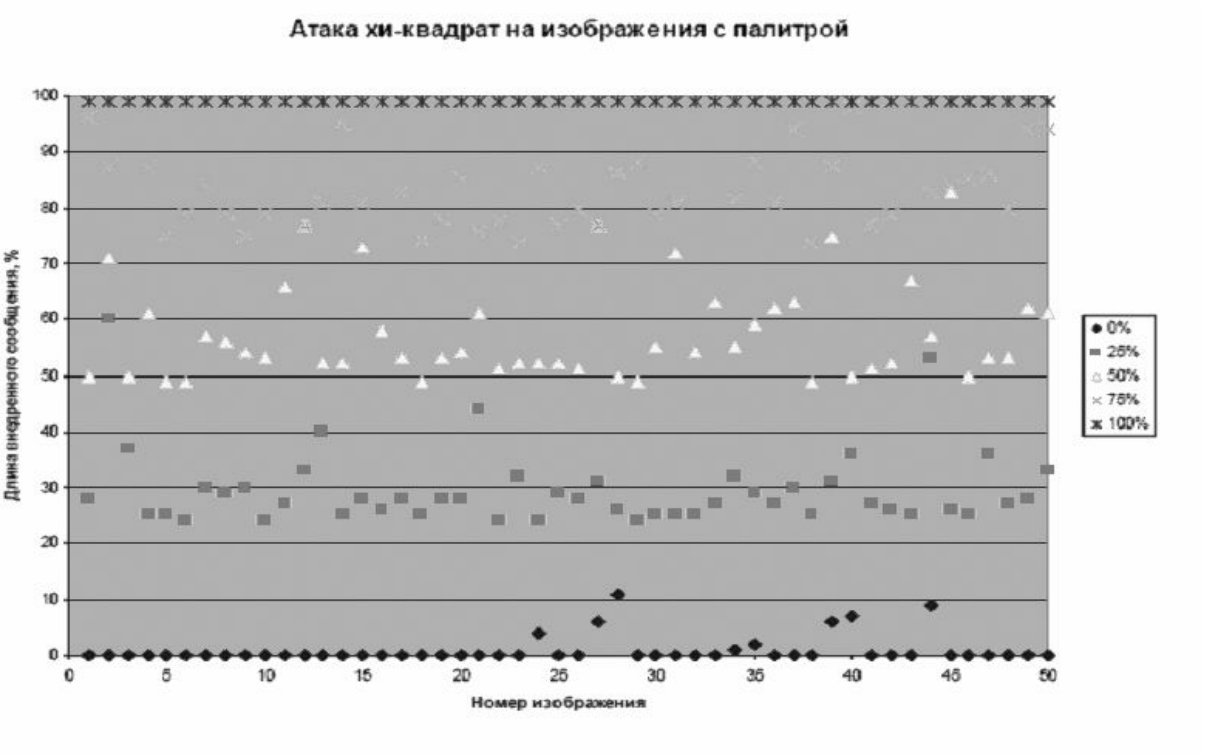


Рис. 2. Результаты атаки хи-квадрат для изображений с палитрой

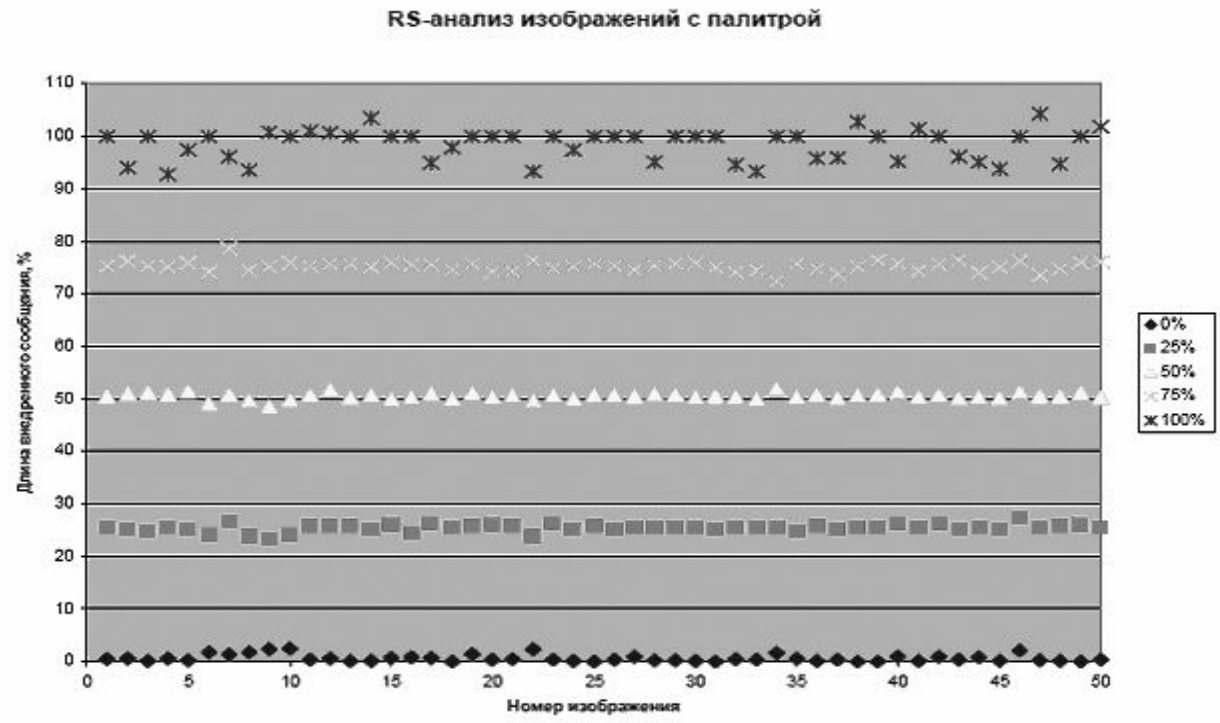


Рис. 3. Результаты RS-анализа изображений с палитрой

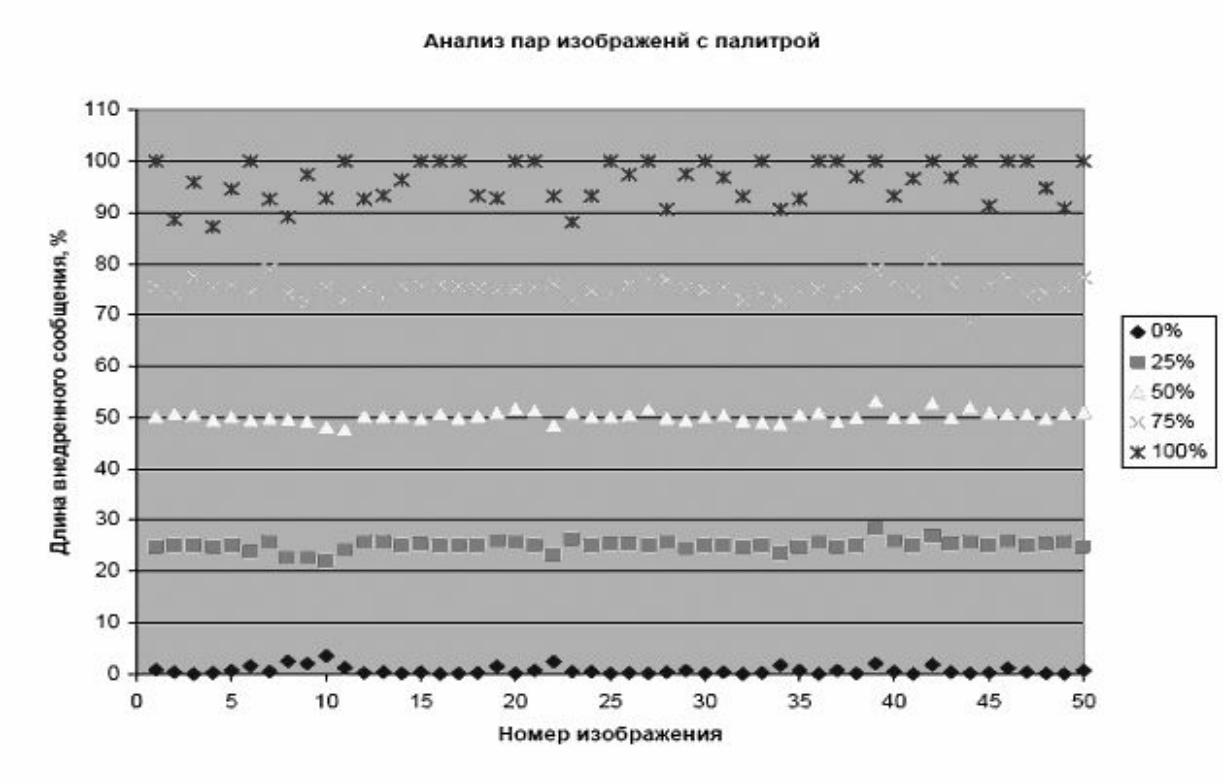


Рис. 4. Результаты анализа пар для изображений с палитрой

Заключение

Таким образом, можно видеть, что из трех реализованных методов стегоанализа наиболее точными являются RS-анализ и анализ пар. Однако, анализ хи-квадрат все же позволяет в большинстве случаев правильно определить факт наличия вложенного сообщения, показывая при этом ошибочную длину внедренного сообщения. Но, учитывая то, что метод последовательного внедрения сообщения в изображение редко применяется в стеганографических программах и, следовательно, компьютерному эксперту редко придется использовать анализ хи-квадрат, можно считать, что подсистема стегоанализа изображений работает вполне успешно.

Литература

1. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая экспертиза. – М.: Право и закон, 2001.
2. Fridrich J., Goljan M. Practical steganalysis of digital images: State of the art. // Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21–24, 2002, pp. 1–13.
3. Provos N. Defending Against on Statistical Steganalysis // Proceeding of the 10 USENIX Security Symposium. 2001, pp. 323–335.
4. Westfeld A., Pfitzmann A. Attacks on Steganographic Systems. Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools – and Some Leassons Learned // Proceeding of the Workshop on Information Hiding. 1999.
5. Грибунин В.Г. Цифровая стеганография. Справочное пособие. – СПб: Солон-Пресс 2002.

УДК 004.932

ОСОБЕННОСТИ ПОВЕДЕНИЯ МЕР КОЛИЧЕСТВЕННОГО РЕКУРРЕНТНОГО АНАЛИЗА

В.Б. Киселев
Научный руководитель – к.т.н., доцент Б.А. Крылов

Рассматривается поведение мер количественного анализа рекуррентных диаграмм (recurrence plots) при вычислении их в сдвигающемся вдоль главной диагонали окне. Динамика меры оценивается как зависимость стандартного отклонения от размера окна. Показывается связь между периодичностью изучаемого временного ряда и размером используемого окна. Приведены графики динамики мер для модельных и естественных временных рядов.

Ключевые слова: нелинейный анализ, динамические системы, рекуррентные диаграммы, количественный анализ рекуррентных диаграмм

1. Введение

В последние десятилетия набор традиционных (линейных) методов исследования был существенно расширен нелинейными методами, полученными из теории нелинейной динамики и хаоса; многие исследования были посвящены оценке нелинейных характеристик и свойств (например, фрактальной размерности) естественных и искусственных (в том числе модельных) процессов. Однако, большинство методов нелинейного анализа [1] требуют либо достаточно длинных, либо стационарных рядов данных, которые далеко не всегда возможно получить при исследовании реальных систем. Более того, было показано [2], что данные методы дают удовлетворительные результаты как правило для идеализированных моделей реальных систем

Рекуррентный анализ [3–5] – динамично развивающийся подход к анализу сложных динамических систем, не требующий длинных или стационарных временных рядов. Рекуррентные диаграммы позволяют судить о характере протекающих в системе процессов, наличии и влиянии шума, дрейфа, наличии состояний повторения и замирания (ламинарность), совершении экстремальных событий, наличии скрытой периодичности и цикличности. Количественный анализ рекуррентных диаграмм позволяет сопоставить диаграмме некоторые численные меры, основанные на плотности рекуррентных точек, распределениях длин диагональных и горизонтальных (вертикальных) линий.

Вычисление мер в окне, смещаемом вдоль главной диагонали рекуррентной диаграммы, позволяет рассмотреть эволюцию изучаемого процесса через эволюцию изменения выбранных мер рекуррентной диаграммы. Целый ряд работ посвящен рассмотрению поиска фазовых переходов при помощи исследований динамики мер при изучении физиологических и гелиогеофизических данных, напр. [6–12].

Как правило, размер окна (в некоторых публикациях – размер эпохи, epoch size) выбирался априорно, при этом не рассматривалось, каким образом размер окна влияет на получаемый результат. В этой работе будет показано поведение мер количественного рекуррентного анализа в зависимости от размера окна при оконных вычислениях.

2. Рекуррентные диаграммы и их количественный анализ

Рекуррентные диаграммы были предложены [3] для иллюстрации поведения динамической системы во времени при помощи визуализации ее рекуррентных состояний матрицей $\mathbf{R}_{i,j}^{m,\varepsilon_i} = \Theta\left(\varepsilon_i - \left\|\vec{x}_i - \vec{x}_j\right\|\right), \quad \vec{x} \in \Re^m, \quad i,j = 1 \ldots N$, где N – количество рассматриваемых состояний x_i; ε_i – размер окрестности точки $\vec{x}$ в момент i; $\|\cdot\|$ – норма (расстояние) и $\Theta(\cdot)$ – функция Хэвисайда. Форма окрестности, характеризуемой парамет-

ром ε_i, определяется в зависимости от типа выбранной нормы и центрирована относительно точки $\vec{x}_i$. В данной работе используются фиксированное значение $\varepsilon_i = \varepsilon = 0.1$, что дает симметричную относительно главной диагонали $\mathbf{R}_{i=j} = 1$ (LOI, line of identity, линия идентичности) диаграмму, и максимальная норма L_∞.

Рекуррентные диаграммы описывают динамику системы при помощи крупномасштабных и мелкомасштабных структур – отдельные точки, диагональные (подобная эволюция двух участков траектории) и горизонтальные (вертикальные) линии (состояние системы не изменяется в пределах окрестности ε).

Меры количественного анализа, предложенные Збилутом и Уэббером [13], основаны на плотности рекуррентных точек и частотном распределении длин диагональных линий: RR (recurrence rate, уровень рекуррентности), DET (determinism, детерминизм), L (средняя длина диагональных линий), L_{max} или DIV (максимальная длина диагональных линий), ENTR (энтропия), TREND (тренд).

Марван [8, 10] предложил меры, основанные на частотном распределении длин горизонтальных (вертикальных) линий: LAM (laminarity, ламинарность) и TT (trapping time, среднее время задержки).

Автором была также предложена [12] мера чистоты траектории CLEAN, показывающая уровень стохастической составляющей процесса.

3. Зависимость эволюции мер от размера окна

На рис. 1 представлены фрагменты рекуррентных диаграмм для синусоиды с периодом 360 точек (1 точка = 1º) и такой же синусоиды, разрушенной равномерным шумом (длины обоих рядов – 5000 точек, $\varepsilon = 0.1$).

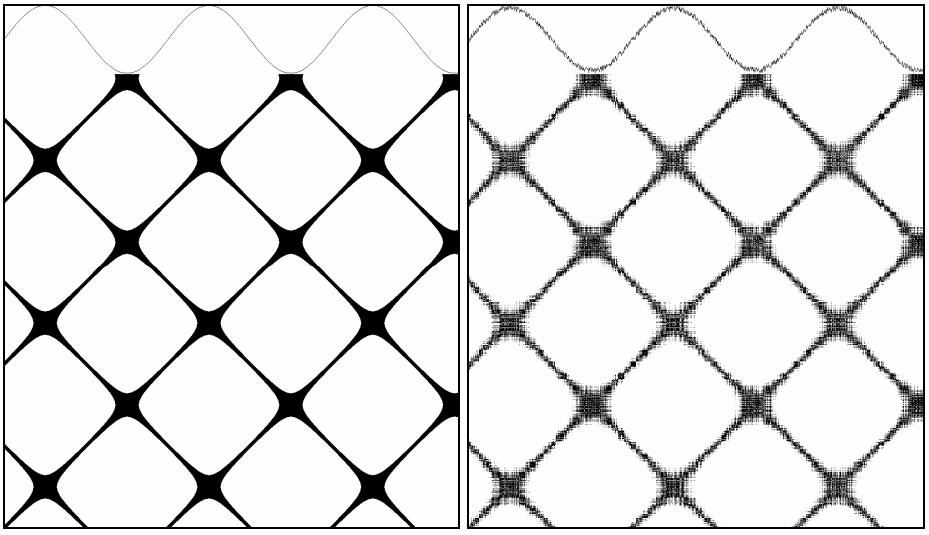


Рис. 1. Фрагменты рекуррентных диаграмм: слева – идеальная синусоида, справа – синусоида, разрушенная равномерным шумом

Проведем вычисление эволюций трех мер – RR, L и TT для размеров окон в 360, 400 и 600 точек (рис. 2, 3). Графики построены таким образом, чтобы для каждой меры соблюдался один и тот же масштаб значений при разных размерах окна.

Данные меры выбраны потому, что их значения зависят только от количества трех базовых элементов текстуры – точек, диагональных и горизонтальных линий соответственно: $RR = \frac{1}{N^2}\sum_{i,j=1}^{N}\mathbf{R}_{i,j}^{m,\varepsilon}$, $L = \frac{\sum_{l=l_{\min}}^{N} lP^{\varepsilon}(l)}{\sum_{l=l_{\min}}^{N} P^{\varepsilon}(l)}$ и $TT = \frac{\sum_{v=v_{\min}}^{N} vP^{\varepsilon}(v)}{\sum_{v=v_{\min}}^{N} P^{\varepsilon}(v)}$. Частотные распре-

деления длин линий определяются как $P^{\varepsilon}(l)=\bigcup_{i=1}^{N}P_i(l)$ для диагональных и $P^{\varepsilon}(v)=\bigcup_{i=1}^{N}P_i(v)$ для горизонтальных линий.

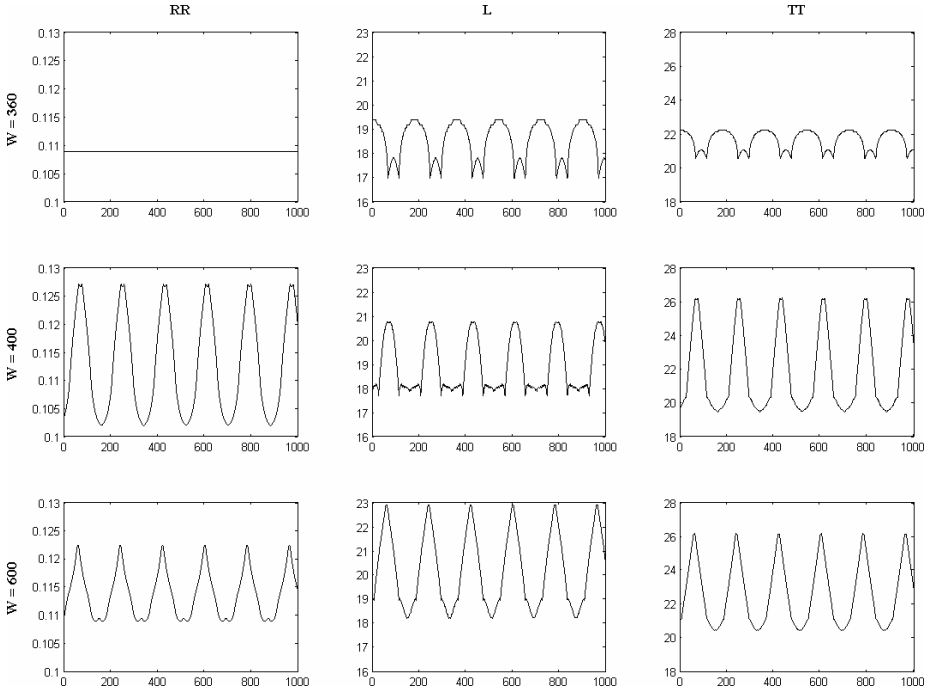


Рис. 2. Динамика мер RR, L, TT при размере окна в 360, 400 и 600 точек (номера эпох с 0 по 1000) для идеальной синусоиды

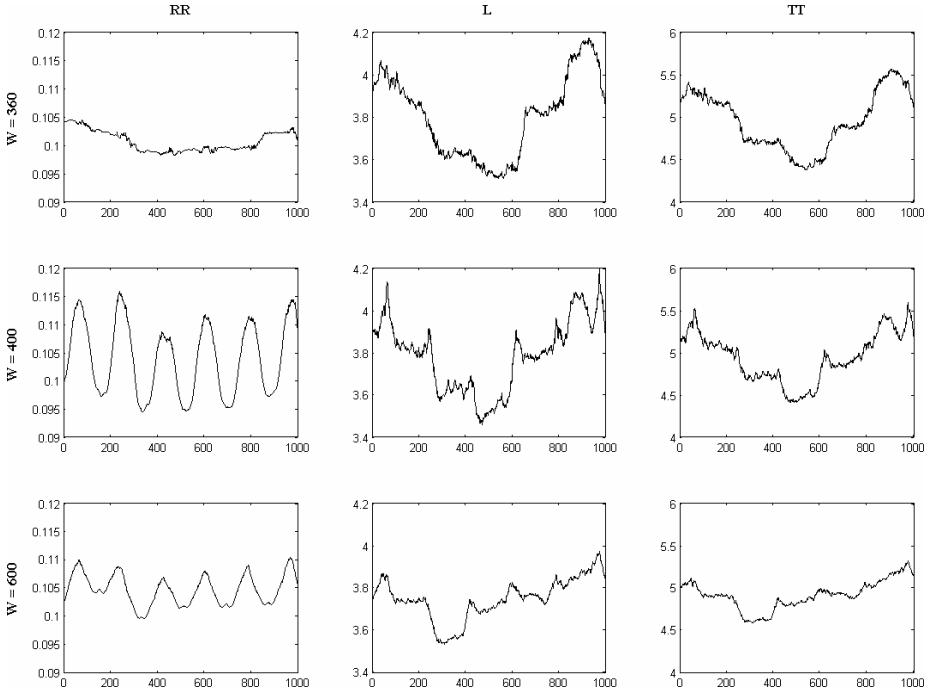


Рис. 3. Динамика мер RR, L, TT при размере окна в 360, 400 и 600 точек (номера эпох с 0 по 1000) для синусоиды, разрушенной равномерным шумом

Из представленных графиков можно сформулировать следующую гипотезу зависимости динамики мер от размера окна:

1. Для сигнала с периодической несущей ее влияние на динамику мер снижается в случае, когда размер окна пропорционален периоду.

2. При увеличении размера окна снижается чувствительность мер к короткопериодным колебаниям.

4. Проверка гипотезы

Для проверки сформулированной гипотезы был выполнен расчет стандартного отклонения значений мер как функции от размера окна (рис. 4)

$$\mathrm{std}_{\mathrm{M}}(W)=\left(\frac{1}{n^W-1}\sum_{i=1}^{n^W}\left(\mu_i^W-\overline{\mu}^W\right)^2\right)^{\frac{1}{2}}, \qquad (1)$$

где количество значений меры $n^W = N - W$, и соответственно $\mu_i^W \in \mathrm{M}^W = \{\mu\}_1^{n^W}$.

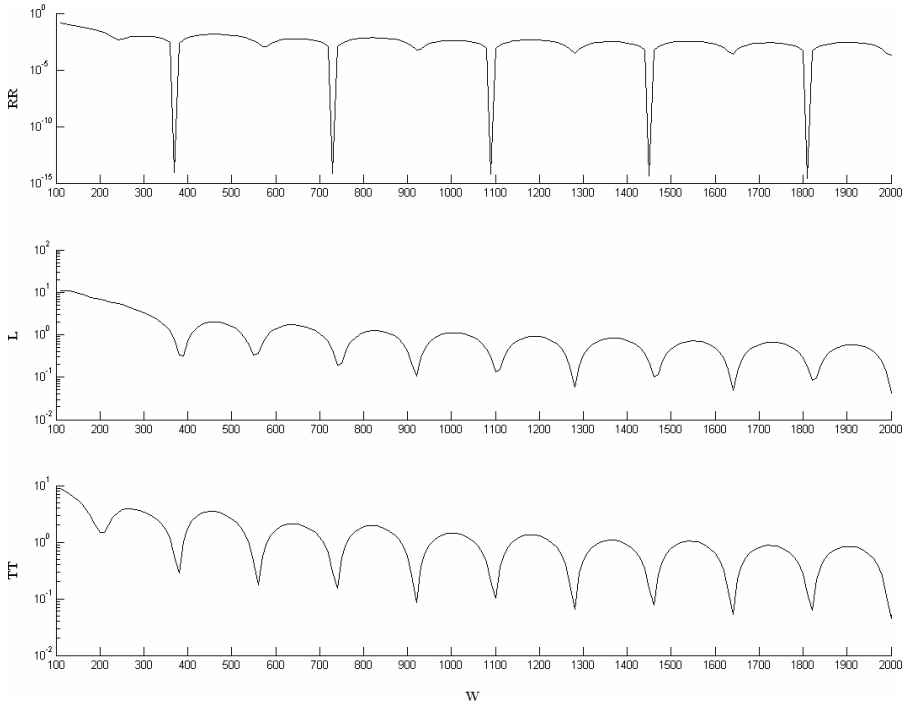


Рис. 4. Стандартное отклонение для мер RR, L, TT рекуррентной диаграммы идеальной синусоиды в диапазоне размеров окна от 100 до 2000 с шагом 10

В целом, графики на рис. 4 подтверждают первое положение сформулированной в параграфе 3 гипотезы. На графике RR четко видны глубокие локальные минимумы в точках, пропорциональных полному периоду исходного сигнала (360 точек). Небольшие локальные минимумы также наблюдаются в точках, пропорциональных полупериоду (180 точек). Графики мер L и TT также демонстрируют локальные минимумы в упомянутых точках, при этом их разница находится в пределах величин одного порядка; тем не менее, значения в точках, пропорциональных полному периоду, несколько больше значений в точках полупериодов. Общий, визуально заметный тренд – понижение с увеличением размера окна.

Таким образом, динамику поведения мер идеальной синусоиды можно записать как $\mathrm{std}_{\mathrm{M}} \underset{W\to\max}{\overset{W\propto\pi}{\to}} \min$, где π – полупериод сигнала. Следует отметить, что в общем масштабе меры DET и LAM достаточно инвариантны размеру окна.

Система Лоренца [14] представляет собой модель нелинейной динамической системы с хаотическим, квазипериодическим поведением (рис. 5).

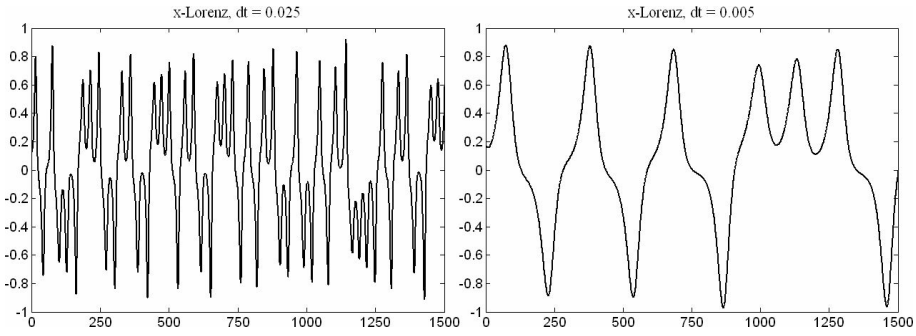


Рис. 5. Фрагменты графиков x-компоненты системы Лоренца при стандартных управляющих параметрах для разных временных масштабов

На рис. 6 представлены графики стандартного отклонения мер L и TT по рекуррентной диаграмме из трехкомпонентных временных рядов системы Лоренца (стандартные параметры) разных временных масштабов длиной 5000 точек.

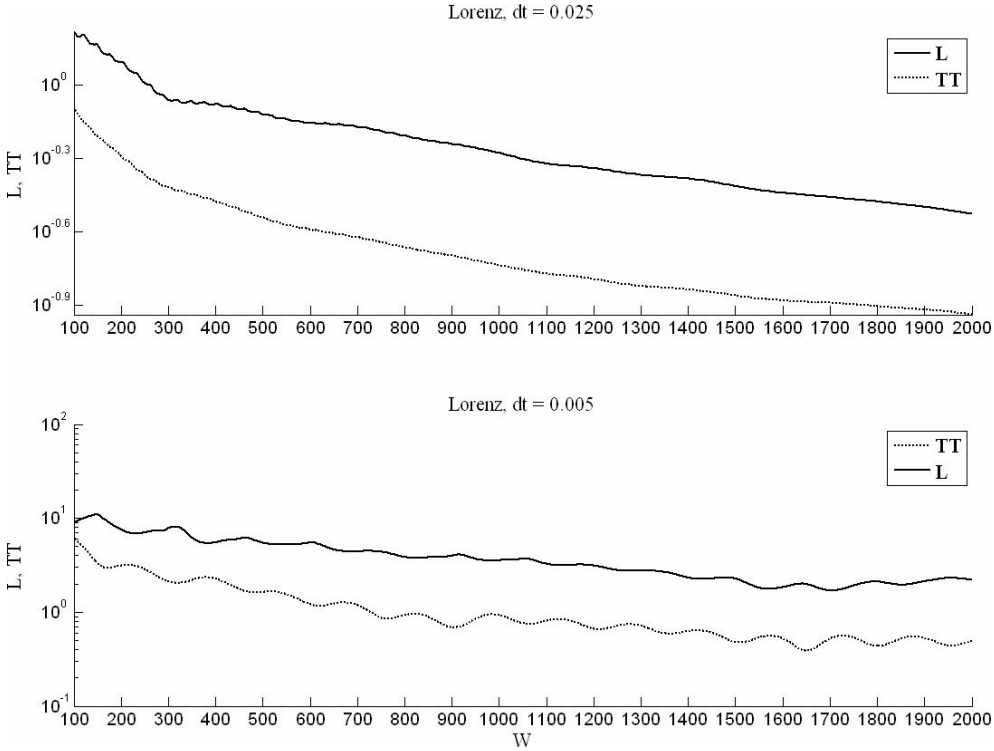


Рис. 6. Стандартное отклонение мер L и TT рекуррентной диаграммы системы Лоренца (стандартные управляющие параметры) на разных временных масштабах

Из графиков для крупномасштабного временного ряда ($dt = 0.025$) на рис. 6 видно, как с увеличением размера окна исчезает чувствительность к короткопериодным колебаниям. Графики для маломасштабного временного ряда, напротив, показывают достаточно высокую чувствительность к квазипериодичности.

Любопытную динамику также показывают меры, вычисленные по диаграммам [12] чисел Вольфа и аа-индекса (рис. 7). В левой части графиков чисел Вольфа можно видеть постепенно затухающие изменения пологости, по мере увеличения размера окна практически исчезающие и пропорциональные одиннадцатилетнему циклу солнечной активности. На графике для аа-индекса (геомагнитной активности), который в целом коррелирует с уровнем солнечной активности, явно выделяется несколько участков, которые прямо не идентифицируются по диаграмме.

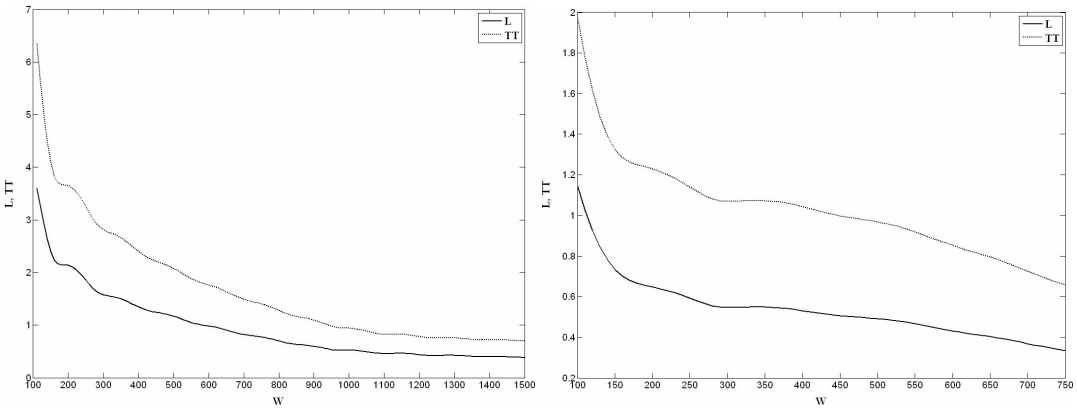


Рис. 7. Стандартное отклонение мер L и TT рекуррентных диаграмм месячных значений: слева – чисел Вольфа за период с 01.1749 по 12.2002, справа – аа-индекса за период с 01.1868 по 12.2000

5. Заключение

Понимание зависимости эволюции мер количественного анализа от размера окна у конкретного типа сигнала необходимо при выявлении фазовых переходов, так как позволит избежать нахождения ложных границ переходов, появляющихся за счет цикличности системы. К сожалению, объем статьи не позволяет привести данные по всем системам, для которых выполнялись исследования динамики мер.

Таким образом:

1. При изучении систем с ярко выраженной несущей частотой целесообразно выбирать размер окна, пропорциональный периоду колебаний;

2. Увеличение размера окна позволяет сгладить влияние короткопериодных колебаний на эволюцию меры. Т.о., слишком большой размер окна может скрыть фазовые переходы, совершающиеся с меньшей относительно него периодичностью;

3. По возможности целесообразно использовать несколько проходов с разным размером окна для последующей коррекции результатов;

4. У систем с хаотическим поведением динамика стандартного отклонения такова, что может быть использован практически любой размер окна.

Исследования поддержаны грантом Правительства Санкт-Петербурга.

Литература

1. Kantz H., Schreiber T. Nonlinear time series analysis // Cambridge University Press. – 1997.
2. Manuca R., Savit R. Stationarity and nonstationarity in time series analysis // Physica D. – 1996. – #99(2–3). – Pp. 134–161.
3. Eckmann J.-P., Kamphorst S.O., Ruelle D. Recurrence Plots of Dynamical Systems // Europhysics Letters 5. – 1987. – Pp. 973–977.
4. Киселев В.Б. Некоторые методы нелинейного анализа // Научно-технический вестник СПбГУ ИТМО. СПб: СПбГУ ИТМО, 2005. – №20. – С. 172–180.
5. Киселев В.Б. Рекуррентный анализ — теория и практика // Научно-технический вестник СПбГУИТМО. СПб: СПбГУ ИТМО, 2006. – №29. – С. 118–127.
6. Trulla L.L., Giuliani A., Zbilut J.P., Webber Jr.C.L. Recurrence quantification analysis of the logistic equation with transients // Physics Letters A. – 1996. – N. 223. – Pp. 255–260.
7. Thomasson N., Hoeppner T.J., Webber Jr.C.L., Zbilut J.P. Recurrence quantification in epileptic EEGs // Physics Letters A. – 2001. – N. 279. – Pp. 94–101.

8. Marwan N., Wessel N., Kurths J.. Recurrence Plot Based Measures of Complexity and its Application to Heart Rate Variability Data // Physical Review E. – 2002. – 66(2) 026702.
9. Naschitz J.E. et all. Assessment of cardiovascular reactivity by fractal and recurrence quantification analysis of heart rate and pulse transit time // Journal of Human Hypertension. – 2003. – N. 17. – Pp. 111–118.
10. Marwan N., Meinke A. Extended Recurrence Plot Analysis and its Application to ERP Data // International Journal of Bifurcation and Chaos "Cognition and Complex Brain Dynamics". – 2004. – N. 14(2). – Pp. 761–771.
11. Fabretti A., Ausloos M. Recurrence Plot and Recurrence Quantification Analysis Techniques for Detecting a Critical Regime. Examples from Financial Market Indices. – 2005. – N. 16(5). – Pp. 671–706.
12. Киселев В.Б., Крылов Б.А. Исследование динамики процессов методом вычисления мер количественного рекуррентного анализа в окне, смещаемом вдоль главной диагонали рекуррентной диаграммы // Научно-технический вестник СПбГУ ИТМО. – 2008. – №56. – С. 62–72.
13. Zbilut J.P., Webber Jr.C.L. Embeddings and delays as derived from quantification of recurrence plots // Physics Letters A. – 1992. – #171(3–4). – Pp. 199–203.
14. Lorenz E.N. Determenistic Non-Periodic Flow // Journal of the Atmospheric Sciences. – 1963. – N. 20. – Pp. 130–141.

УДК 621.315.21

МЕТОДЫ УМЕНЬШЕНИЯ ПОТЕРЬ В ОПТИЧЕСКИХ РАЗЪЕМАХ

Д.А. Шилкин, В.А. Козак
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

Потеря мощности или затухание оптического сигнала возникает при неточной центровке оптических волокон или световодов. В таком случае оптический сигнал просто не переходит в следующий световод, или входит под углом более критического. При неполном физическом контакте волокон образуется воздушный зазор. В связи с чем возникает эффект возвратных потерь. Часть лучей при прохождении прозрачных сред с разной плотностью отражается в обратном направлении. Достигая резонатора, они усиливаются и вызывают искажения сигналов. В статье рассмотрены способы, позволяющие уменьшить потери в оптических разъемах.

Ключевые слова: оптический разъем, оптическое волокно, потери, многомодовый, одномодовый

Введение

Потери в оптических разъемах (ОР) определяются целым рядом причин, которые в общем виде могут быть классифицированы на следующие группы [1]:

- внутренние факторы, которые определяются допусками на геометрические размеры оптического волокна (ОВ);
- внешние факторы, которые определяются качеством изготовления отдельных элементов разъема и его технологическими допусками;
- отражениями и рассеянием;
- загрязнениями.

К числу основных внутренних факторов, которые вызывают потери в ОР, относятся эксцентриситет и некруглость (эллиптичность) сердцевины, а также разность диаметров, числовых апертур и профилей показателей преломления сращиваемых световодов. Необходимость учета эксцентриситета и некруглости возникала на ранних стадиях развития техники оптической связи. В настоящее время в связи с достигнутым технологическим уровнем изготовления ОВ эти факторы перестали играть первостепенное значение [2]. Так, например, при типичной для современных многомодовых ОВ величине некруглости сердцевины 5% вносимые потери не превышают 0,1 дБ.

Потери за счет разности диаметров сердцевин сращиваемых световодов наиболее часто встречаются на практике в случае применения многомодовой техники, так как стандартами допускается использование в СКС двух типов ОВ со значением данного параметра в 50 и 62,5 мкм. При соединении отдельных световодов такие потери происходят только при переходе из волокна с большим диаметром в ОВ с меньшим диаметром. При сращивании световодов с одинаковыми номинальными диаметрами потери рассматриваемого вида возникают из-за допуска на диаметры сердцевины.

Потери, обусловленные разностью числовых апертур, определяются главным образом производственными допусками на этот параметр.

В перечень составляющих потерь, которые вызываются внешними факторами, входят потери за счет наличия воздушного промежутка между торцами сращиваемых ОВ, радиальных и угловых смещений световодов, а также непараллельности торцевых поверхностей ОВ в разъемах. Потери этого вида обусловлены неизбежными производственными допусками на геометрические размеры отдельных деталей ОР, выполняющих центрирование сращиваемых ОВ.

Потери на загрязнение возникают в процессе эксплуатации кабельной системы главным образом из-за несоблюдения правил подключения и отключения ОР. Для ми-

нимизации этой составляющей потерь стандарты требуют выполнять очистку оптически активных поверхностей соединяемых ОВ перед каждым подключением ОР.

Методы уменьшения потерь в оптических разъемах

Значительная часть отдельных составляющих этих потерь может быть уменьшена до приемлемого для практики уровня выбором конструкции соединителя, совершенствованием технологии монтажа и соблюдением правил эксплуатации. Исключением являются принципиально неустранимые потери, которые определяются наличием смещения осей сердцевины соединяемых ОВ.

Далее для определенности речь пойдет о наиболее распространенных на практике симметричных ОР с асимметричными (в подавляющем большинстве случаев цилиндрическими) юстирующими наконечниками. Все приводимые для них положения могут быть без проблем распространены также на разъемы несимметричной схемы и изделия без центрирующих наконечников.

Юстировка ОВ в разъеме осуществляется косвенно за счет выравнивания наконечников в центраторе розетки. При таком способе соединения смещение осей сращиваемых волокон определяется эксцентриситетом сердцевины и оболочки, а также сердцевины и внешней поверхности наконечника. Свой вклад в возникновение эксцентриситета вносит технологический зазор, обеспечивающий ввод волокна в отверстие.

Конструкции ОР, применяемых в СКС, допускают выполнение юстировки, которая имеет своей целью снижение потерь за счет уменьшения величины эксцентриситета сердцевины ОВ и внешней поверхности наконечника. В настоящее время на практике используется несколько разновидностей реализации этой процедуры, которые отличаются друг от друга областью применения и типом исполнения образцовой вилки.

В процессе юстировки ОР оператор подключает его вилку к специально изготовленному мастер-шнуру. Образцовые вилки этого изделия могут быть выполнены в вариантах тип А и В. Вилка типа А изготавливается таким образом, чтобы ось волокна точно совпадала с осью центрирующего наконечника (рис. 1а). В образцовой вилке типа В ось волокна смещена вдоль радиуса в заранее заданном относительно ключа направлении примерно на половину интервала возможных отклонений (рис. 16).

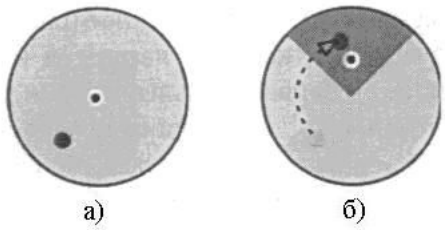


Рис. 1. Области нахождения центров сердцевин соединяемых волокон и волокна мастер-шнура при использовании образцовых вилок типов А и В: а) непозиционный разъем; б) позиционный разъем

При производстве вилок с керамическим наконечником симметричных ОР используются образцовые вилки типов А и В.

Разъемы, которые в процессе изготовления контролируются с помощью вилки типа Л, называются непозиционированными. Основной недостаток ОР данной разновидности состоит в том, что величина потерь зависит не от величины отклонения оси сердцевины каждого световода от оси симметрии, а от абсолютного расстояния между осями сращиваемых волокон пары при вилках, установленных в розетку. Таким образом, в пределе оно достигает удвоенного значения длины интервала возможных отклонений.

При производстве современных разъемов существенно более часто применяется технология юстировки, основанная на использовании образцовой вилки типа В с цен-

тром сердцевины волокна, смещенным примерно на половину радиуса возможных отклонений. Конструкция наконечника юстируемой вилки позволяет установить его в процессе сборки в одном из четырех (шести) угловых положений с угловым смещением 90° (60°). Выбор этого положения осуществляется по критерию минимума потерь, после чего наконечник фиксируют в корпусе вилки. В результате применения данной технологии осевое смещение сердцевин соединяемых ОВ не выходит за пределы определенного квадранта, задаваемого образцовой вилкой (схематически отмечен в виде сектора на рис. 16). Вилки, собранные по такой схеме, иногда называются позиционированными, или калиброванными [3].

В случае использования непозиционированных разъемов величина ожидаемого отклонения осей сердцевин сращиваемых волокон составляет примерно R/2. При переходе на технологию юстировки с помощью образцовой вилки типа В ожидаемая величина расстояния между осями сращиваемых волокон может быть оценена величиной $R / 4\sqrt{1+(tg\pi / 8)^2}$, т.е. сокращается примерно в √2 раз. Таким образом, максимальное значение потерь не превосходит 0,7 дБ при типовом значении этого параметра 0,3–0,4 дБ. Метод юстировки с использованием образцовой вилки типа В рекомендован IEC в качестве стандартного для ОР на основе керамических наконечников.

В отличие от наконечников моноблочной конструкции в композитных наконечниках за счет пластичности материала внутренней вставки возможно применение других механизмов юстировки.

Схема пассивной юстировки

Так называемая пассивная юстировка не требует обязательного применения образцовой вилки, которая используется исключительно для контроля качества готового изделия.

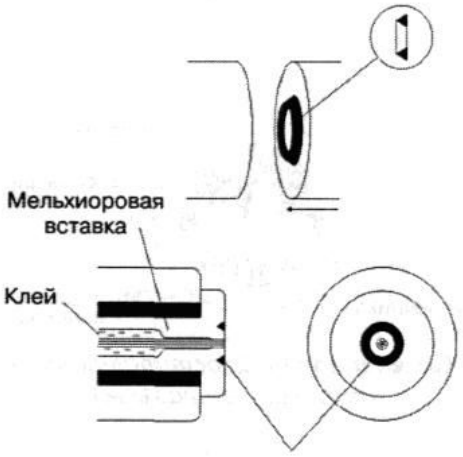


Рис. 2. Схема пассивной юстировки наконечника оптического разъема

Суть этого механизма заключается в том, что после ввода ОВ в канал еще до затвердевания клея на торцевую часть мягкой центральной вставки наконечника воздействуют кольцевым штампом с треугольной в сечении формой рабочего органа. В результате выполнения данной процедуры наконечник плотно охватывает концевой участок волокна, уменьшая остаточный эксцентриситет сердцевины до величины допустимой производственными допусками неконцентричности сердцевины и оболочки (рис. 2). В современных многомодовых волокнах величина этого параметра не превышает 3 мкм. Величина неконцентричности в 0,8 мкм, определяемая геометрическими параметрами одномодовых волокон, не может считаться пренебрежимо малой при их

соединении в разъеме.Поэтому при работе с одномодовыми ОР в дополнение к пассивной юстировке может производиться процедура активной юстировки.

Схема активной юстировки

Она выполняется после затвердевания клея и традиционной для клеевой технологии обработки торцевой поверхности наконечника, и основана на принудительном смещении оси волокна в геометрический центр наконечника, то есть туда, где в неюстированных разъемах обеспечивается минимум потерь. Для реализации процедуры юстировки применяют другой штамп в виде сектора с углом раскрыва 120°. В процессе выполнения подстройки штамп предварительно ориентируют таким образом, чтобы перемещением всей торцевой области наконечника за счет пластической деформации свести к минимуму величину остаточного отклонения осей волокна и наконечника (рис. 3).

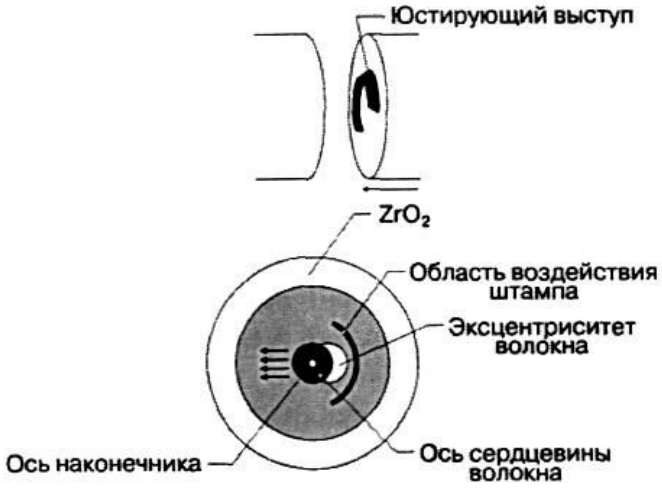


Рис. 3. Схема активной юстировки наконечника оптического разъема

При типовой величине эксцентриситета оболочка – сердцевина современных световодов 0,8 мкм после выполнения процедуры активной юстировки гарантированно обеспечивается величина эксцентриситета сердцевина – наконечник не более 0,5 мкм, что соответствует средним потерям 0,12 дБ [4]. Разъемы данной разновидности называют иногда центрированными, а контроль качества их изготовления осуществляется с помощью шнуров, волокна которых оконцованы образцовыми вилками типа А.

Упомянем также еще одно достаточно эффективное техническое решение, которое пользовалось большой популярностью на ранних этапах развития техники волоконно-оптической связи. Оно основано на том, что для минимизации обратных отражений в область контакта ОВ тем или иным способом вводится прозрачная иммерсионная жидкость, показатель преломления которой выбирался максимально близким к показателю преломления стекла сердцевины. Подобное решение существенно усложняет эксплуатацию ОР и в связи с улучшением технологии обработки наконечников практически вытеснено из широкой инженерной практики. Аналогичный по назначению иммерсионный гель применяется только в некоторых типах, так называемых, механических коннекторов и в механических сплайсах, то есть в тех элементах, где число циклов сращивания и разъединения сведено к минимуму.

Литература

1. Packaging guide: Фирменный материал компании Acome. – 2004.
2. ГОСТ 18690-82 (СТСЭВ 3227-81). Кабели, провода, шнуры и кабельная арматура. Маркировка, упаковка, транспортирование и хранения. Государственный комитет СССР по стандартам. – М.: Издательство стандартов. – 1983.
3. Ларин Ю.Т. Программа разработки нормативно-технической базы оптических волокон и кабелей // Фотон-Экспресс. – 2003. – Сентябрь. – №4(30).
4. Иванов А.Б. Волоконная оптика: компоненты, системы передачи, измерения. – М.: Компания Сайрус Системе. – 1999.
5. Семенов А.Б. Оптические разъемы//Фотон-Экспресс. – 2005. – №4(44).

УДК 004.514

ПРИМЕНЕНИЕ ПРИНЦИПОВ ПОСТРОЕНИЯ ЭФФЕКТИВНЫХ ПОЛЬЗОВАТЕЛЬСКИХ ИНТЕРФЕЙСОВ СИСТЕМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Д.А. Кораблев
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

В работе описываются основные принципы построения эффективного пользовательского интерфейса систем электронного документооборота. Приводятся методики применения принципов. Рассматриваются положительные примеры использования принципов проектирования, в существующих системах электронного документооборота.

Ключевые слова: пользовательский интерфейс, электронный документооборот, принципы построения

Введение

Электронный документооборот – находит все большее применение в различных сферах деятельности бизнеса и государства. Объем рынка систем электронного документооборота в России в 2008 году составил $170 миллионов, при этом отмечается тенденция к его увеличению. В то же время, применение систем документооборота сопряжено с рядом трудностей как организационного, так и технического характера.

Взаимодействие пользователя с системой электронного документооборота, обеспечивает пользовательский интерфейс, от эффективности и качества которого, во многом зависит эффективность и качество результатов работы пользователей с системой.

Проанализировав несколько работ [1–12] посвященных разработке пользовательских интерфейсов, выделил наиболее значимые принципы, предложенные в рассматриваемых работах, в обобщенном виде они представлены ниже.

Основная часть

Золотое сечение – это такое пропорциональное деление отрезка на неравные части, при котором весь отрезок так относится к большей части, как сама большая часть относится к меньшей; или другими словами, меньший отрезок так относится к большему, как больший ко всему.

a : b = b : c или c : b = b : a.

Отрезки золотой пропорции выражаются бесконечной иррациональной дробью 0,618..., если с принять за единицу, a = 0,382. Отношение же отрезков a и b составляет 1,618.

С золотым сечением связано имя итальянского математика Фибоначчи. Ряд чисел 0, 1, 1, 2, 3, 5, 8 и так далее известен как ряд Фибоначчи. Каждый член ряда, начиная с третьего, равен сумме двух предыдущих, а отношение смежных чисел ряда приближается к отношению золотого сечения (21: 34 = 0,617; 34: 55 = 0,618).

Применение принципа

- Всё окна предоставляемые пользователю для работы необходимо проектировать таким образом, что бы соотношение ширины и высоты равнялось золотой пропорции 0,618.
- Если в информационной области окна расположено 2 функционально различных блока, целесообразно разместить их таким образом, что бы их соотношение по ширине равнялось золотой пропорции 0,618.

- Если информационная область содержит в себе разнотипные элементы, такие как кнопки, поля ввода и другие, то необходимо размеры окна и элементов строить в соответствии с рядом Фибоначчи.

Одной из главных задач эффективного дизайна пользовательского интерфейса – это ясность, интуитивность, а также концентрация внимания пользователя на нужных местах страницы [1]. Именно для этого применим принцип золотого сечения. Проиллюстрируем применение принципа золотого сечения в системах автоматизации документооборота. Допустим, макет страницы имеет фиксированную ширину – 960px и содержит два основных блока, таблица документов и список папок (в примере рассмотрен интерфейс системы управления документооборотом компании ЮТК), тогда они будут поделены следующим способом.

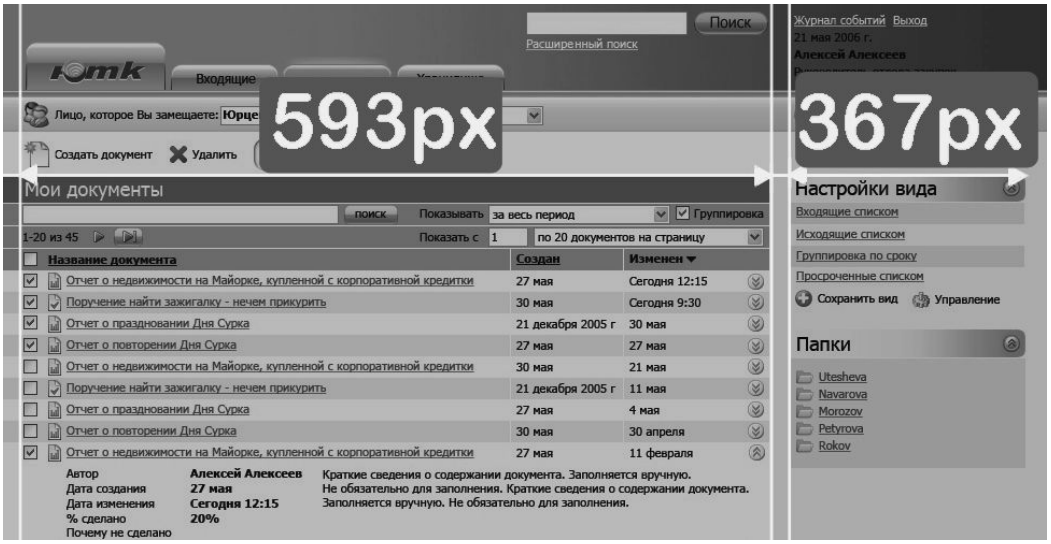


Рис. 1. Интерфейс системы управления документооборотом компании ЮТК

Хотя дизайн и не совсем придерживается принципов Золотого сечения. Пользователи этого не чувствуют, так как они интуитивно разделают макет на два отдельных блока (шириной 593px и 367px), свободное пространство между блоками на экране является пассивным и «отфильтровывается» при просмотре.

Принцип группировки. Согласно этому принципу, экран программы должен быть разбит на ясно очерченные блоки элементов, может быть, даже с заголовком для каждого блока. При этом группировка, должна быть осмысленной, расположение элементов в группах, и расположение самих групп друг от друга должны быть продуманы.

Интерфейс программы в котором, группы элементов разделены, «сканируется» пользователем значительно быстрее обычного, поскольку в таком случае больше «точек привязки» (точно также как и в меню с пиктограммами) [2]. Наконец, в объемных интерфейсах группировка элементов облегчает создание кластеров в кратковременной памяти.

Применение принципа

- Однотипные задачи объединять в отдельные группы, отделенные друг от друга визуальным разделителем.
- Схожие действия, выполняемые программой, объединять в пункты меню.
- Группировать подобные инструменты в соответствующие панели инструментов.

Существует два основных способа разделять группы: между группами можно помещать пустой элемент (разделитель) или же размещать отдельные группы в разных уровнях иерархии. Для разграничения групп традиционно используют полоски.

Хороший пример системы использующей принцип группировки – интерфейс системы документооборота СИБУР. Всё однотипные задачи выполняемые пользователем, сгруппированы, озаглавлены и визуально отделены друг от друга [4].

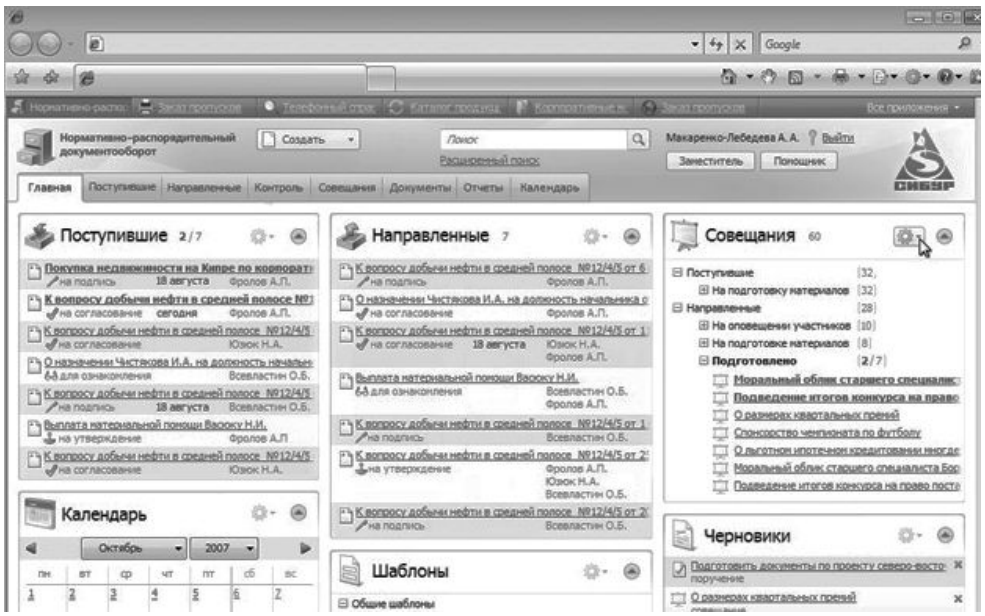


Рис. 2. Интерфейс системы управления документооборотом «СИБУР»

Кошелек Миллера. Этот принцип назван так в честь ученого-психолога Г.А. Миллера, который исследовал кратковременную память, проверяя выводы, сделанные ранее его коллегой, Г. Эббингаузом. Эббингауз пытался выяснить, сколько информации может запомнить человек без каких-либо специальных мнемонических приемов. Оказалось, что емкость памяти ограничена семью элементами.

Применение принципа

- Количество пунктов меню не должно превышать 7–9.
- Количество кнопок на панелях инструментов не должно превышать 7–9.
- Количество опций на каждой закладке также не должно превышать 7–9
- Если количество элементов из 1–3 пунктов превышает 9, необходимо создать дополнительный уровень группировки (смотри принцип группировки).

Хорошим примером данного принципа, служит главное окно системы документооборота «Босс-Референт» (рис. 3): тринадцать кнопок на левой панели, между которыми есть три визуальных разделителя, воспринимаются гораздо лучше, чем, если бы кнопки шли единым блоком [7].

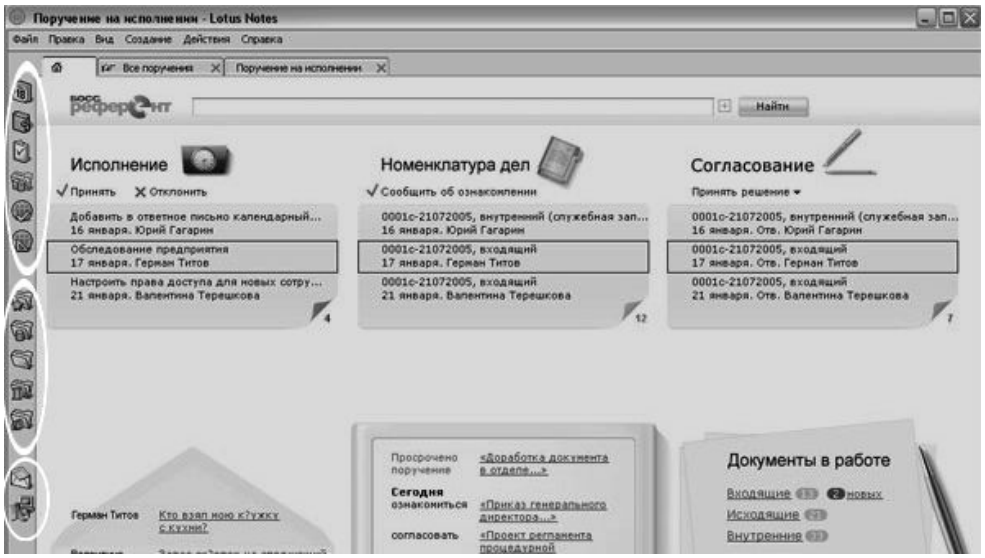


Рис. 3. Интерфейс системы управления документооборотом «Босс-Референт»

Обратная связь. Финальной фазой любого человеческого действия является оценка его результата. Если нажатие на кнопку не дало никакого подтверждения о том, что операция произведена успешно, человек нажмет кнопку еще раз, думая, что он сделал что-то неправильно. Каждое действие пользователя должно получать визуальное, а иногда и звуковое подтверждение того, что система восприняло введенную команду.

Применение принципа

- Необходимо реализовывать обратную связь, как можно ближе к точке последнего взаимодействия пользователя с системой.
- Необходимо предоставить пользователю информацию относительно состояния процесса, особенно если данный процесс выполняется большой промежуток времени. К таким процессам относятся сортировка документов, хранение документов на медленных носителях, печать и т.д.
- Предоставлять пользователю возможность прервать длительный процесс.
- Во время работы с документами, выделять цветом поля ввода которые пользователь не заполнил или заполнил неверно.

Отсутствие достаточного количества обратной связи приводит к фрустрации и является одной из самых опасных ошибок при проектировании интерфейса [11].

Хороший пример, обратной связи – работа системы управления документооборотом компании ЮТК, в случае если пользователь допустил ошибку в заполнении, он сразу получает уведомление об этом.

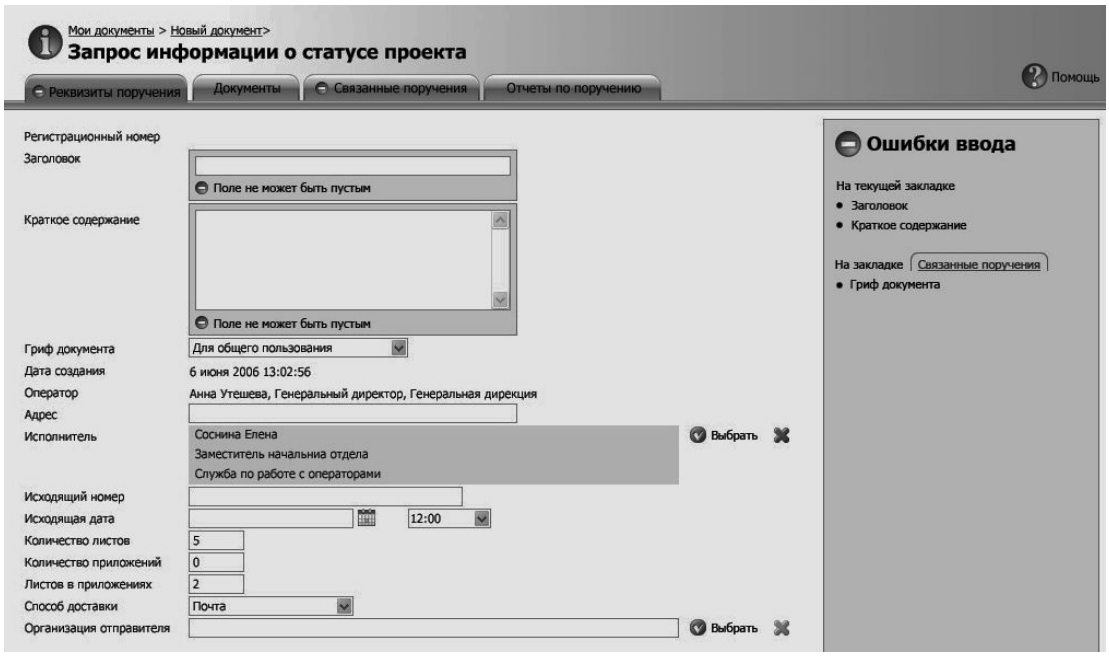


Рис. 4 Интерфейс системы управления документооборотом компании ЮТК

Ограничение количества основных цветов. Предполагает использование ограниченного числа основных цветов в программе – не более трех, исключая оттенки.

При правильном использовании цвета в интерфейсе системы, можно эффективно управлять вниманием пользователя к отдельным частям интерфейса, а так же заметно улучшить внешний вид приложения. С другой стороны, неправильное использование цвета может серьёзно навредить эффективному использованию программного продукта. При разработке следует, ограничится тремя-четырьмя основными цветами.

Применение принципа

- Спроектировать интерфейс системы документооборота, таким образом, что бы основная часть программы была выполнена одним цветом.
- Всё поля ввода должны быть выполнены одним цветом.

- Неизменяемая часть интерфейса должна иметь цвет отличный от цвета полей ввода и основного цвета.
- Поля обязательные для заполнения и необязательные, должны быть выполнены в разных цветах.

Хорошим примером служит интерфейс системы документооборота «Ефрат», в интерфейсе используется не более трех основных цветов.

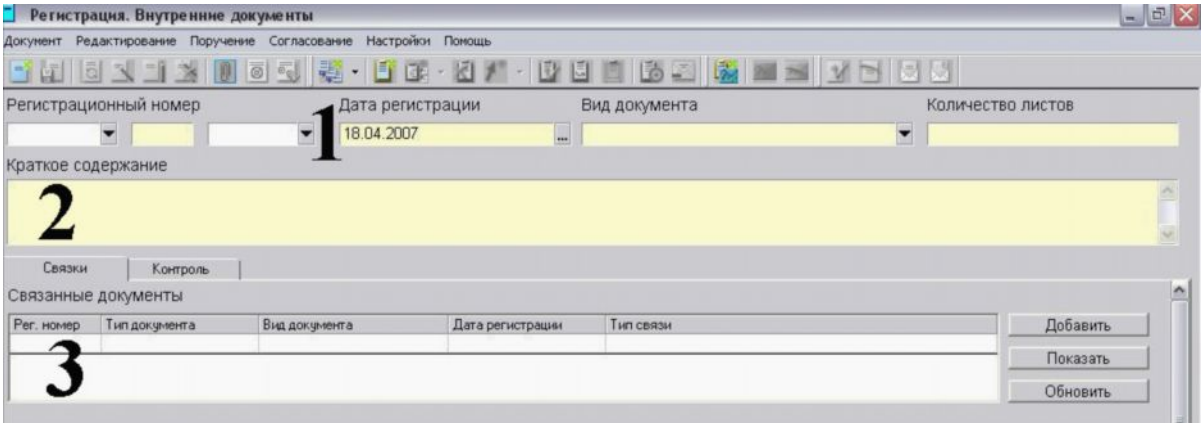


Рис. 5. Интерфейс системы управления документооборотом «Ефрат»

Видимость отражает полезность. Смысл этого принципа состоит в том, чтобы вынести самую важную информацию и элементы управления на первый план и сделать их легкодоступными пользователю, а менее важную – переместить, например, в меню.

Применение принципа

- При выборе различных объектов – текст, графика, пункты меню, действия для работы с ними, должными меняться в соответствии с выбранным объектом.
- Аналогично должны меняться панели инструментов.
- При выделении объекта выводить рядом всплывающее меню с перечнем характерных операций.
- Первоначально на экране должно быть минимальное количество компонентов, а все редко используемые элементы должны быть убраны в пункты меню.

Хорошим примером применения этого принципа, являются контекстные панели инструментов системе «Босс-Референт», которые меняются в зависимости от того, с какой частью программы в данный момент работает пользователь [7].

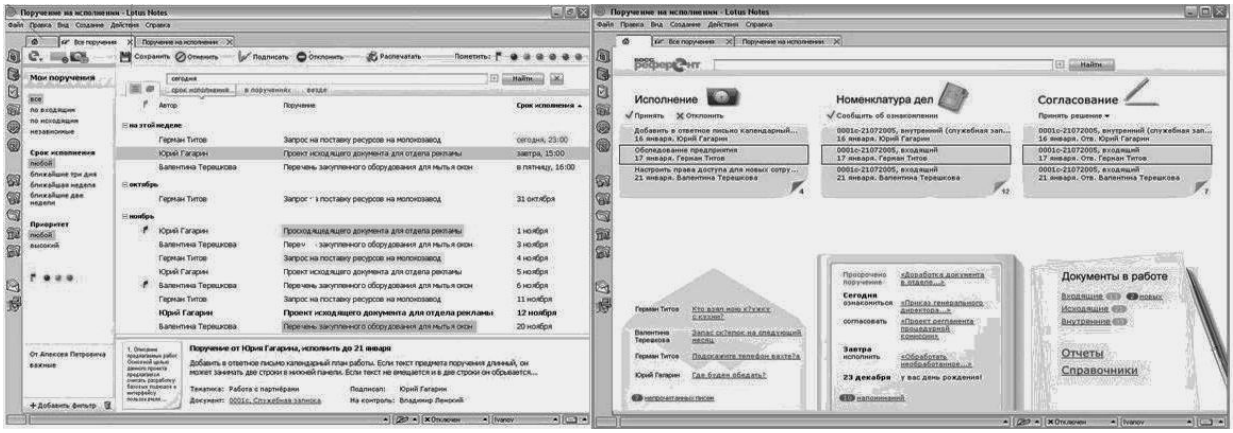


Рис. 6. Интерфейс системы управления документооборотом «Босс-Референт»

Умное заимствование. Если пользователь привык к чему-либо, он быстрее научится работать и будет работать с вашей программой, так как сможет использовать приобретенные навыки. Базовое заимствование – это использование стандартных эле-

ментов, общих для всех программ Windows – меню, списки, кнопки и тому подобное. Так же это позволяет легко добиться последовательности в интерфейсе

Заимствование широко распространенных приемов дизайна интерфейсов и удачных находок авторов конкурирующих программ позволяет резко сократить время обучения и повысить комфорт пользователя. При работе он будет использовать уже приобретенные навыки – этот вопрос затрагивает и принцип равенства между системой и реальным миром.

Применение принципа

- При сохранении документа использовать стандартный диалоговое окно операционной системы или внешне похожее на него.
- При выборе цвета интерфейса, шрифта использовать стандартное диалоговое окно операционной системы.
- Использовать в системе документооборота, стандартную раскладку горячих клавиш операционной системы.
- Кнопки и иконки системы, должны иметь визуальное сходство с аналогичными элементами операционной системы, под которую ведется разработка.

Программы, лидирующие па рынке, часто обладают схожим дизайном, например интерфейс системы «DocsVision» (слева) и интерфейс системы «LanDocs» (справа)

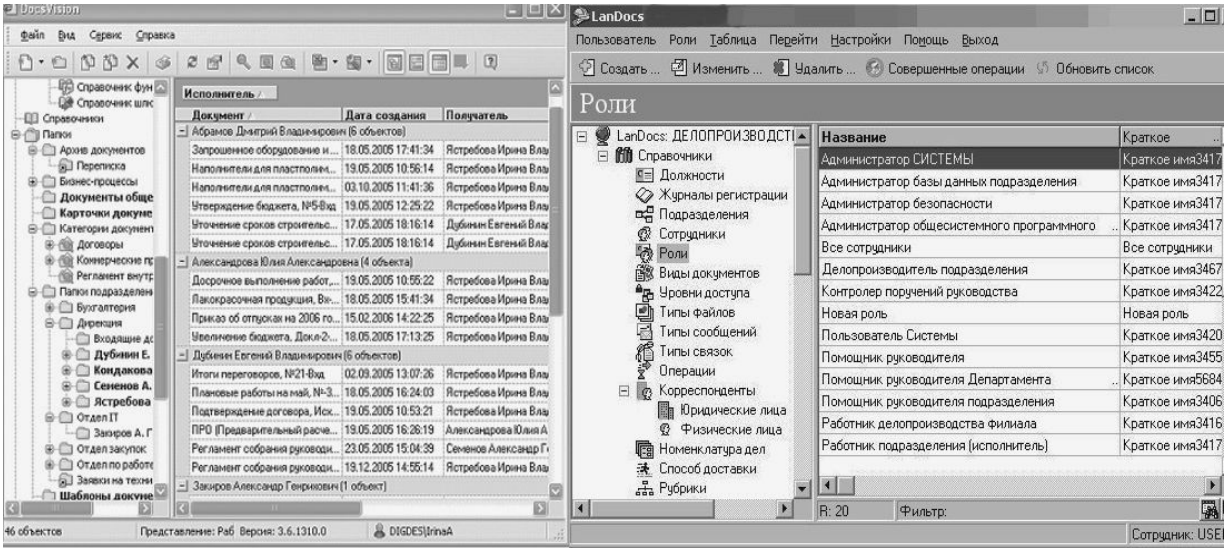


Рис. 7. Интерфейс систем управления документооборотом «DocsVision» и «LanDocs»

Заключение

Рассмотренные принципы построения пользовательских интерфейсов, позволяют разработать высоко эффективный пользовательский интерфейс, систем электронного документооборота. Без использования принципов, есть больший риск получить громоздкий и неудобный для пользователя продукт. Развитие систем электронного документооборота показывает, что конкуренция продуктов из области функциональности перемещается в область удобства и комфортности их для пользователей. В этих условиях, принципы проектирования становятся технологиями, обеспечивающими рыночный успех проекту.

Литература

1. Гультяев А.К., Мишин В.А. Проектирование и дизайн пользовательского интерфейса. С.-Пб.: КОРОНА-принт, 2000. – 280 с.

2. Жарков С.В., Shareware: профессиональная разработка и продвижение программ. С.-Пб.: BHV-СПб, 2002. – 320 с.
3. http://www.stcompany.ru/
4. http://www.visualpharm.ru/sibur.html
5. Тео Мандел. Дизайн интерфейсов. ДМК пресс, 2005. – 416 с.
6. www.evfrat.ru
7. http://www.boss-referent.ru/
8. Дженнифер Тидвел. Разработка пользовательских интерфейсов. Питер, 2008. – 416 с.
9. www.**landocs**.ru
10. http://www.interface.ru/
11. Головач В. В., Дизайн пользовательского интерфейса^2 Искусство мыть слона. 2008. – 97 с.
12. http://usability.ru

УДК 004.056.53

ЗАЩИТА КОНТЕНТА WEB-ПРИЛОЖЕНИЯ ОТ НЕСАНКЦИОНИРОВАННОГО ИСПОЛЬЗОВАНИЯ

С.С. Кувшинов
Научный руководитель – д.т.н., профессор А.Г. Коробейников

В работе предлагаются подходы к реализации защиты контента web-приложения как объекта интеллектуальной собственности от вариантов несанкционированного использования. Рассмотрены решения позволяющие выявить и предотвратить неправомерные действия сторонних web-разработчиков по использованию чужих графических изображений, каскадных таблиц стилей, а также клиентского скриптового кода. Описывается общая схема решения, приводится программная реализация алгоритмов. Также в работе рассмотрен пример использования описываемых подходов на конечном web-приложении.
Ключевые слова: защита интеллектуальной собственности, web-разработка, цифровые водяные знаки, обфускация, кэширование

Введение

Проблема защиты цифрового контента остро стоит в современном интернете. Одни разработчики Web-ресурсов (Web-сайтов, Web-служб) кропотливо и усердно создают начинку приложений, механизмы работы, внешний вид; другие, в свою очередь, имеют возможности без лишних усилий и совершенно безнаказанно использовать объекты интеллектуальной собственности первых. Именно собственности, поскольку мультимедийные файлы, таблицы стилей, клиентские скрипты, серверный код Web-приложения имеют законного владельца – правообладателя. Особенно неприятен тот факт, что в большинстве случаев несанкционированное использование элементов контента Web-ресурса осуществляется автоматически в то время как недобросовестный злоумышленник, единожды автоматизировав процесс получения нужных ресурсов, долговременно извлекает выгоду от реализации чужого труда.

В данной статье предлагаются подходы реализации защиты следующих элементов контента сайта от несанкционированного использования:

1. Клиентские скрипты (JavaScript файлы);
2. Изображения (файлы .jpeg, .png, .gif и другие);
3. Каскадные таблицы стилей (.css файлы);
4. Описания поведений (.htc файлы).

Защита от несанкционированных ссылок

Несанкционированные ссылки на элементы контента сайта – наиболее простой пример неправомерного использования чужой интеллектуальной собственности в интернете. Нерадивые разработчики довольно часто используют (делают ссылки на чужой ресурс) графические изображения со сторонних сайтов. Ниже описан подход, предотвращающий подобные нарушения в отношении сайтов, созданных на основе технологии ASP.Net [1] и развёрнутых на серверах с Internet Information Services [2].

Рассмотрим пример, базирующийся на следующем:

- Существует сайт под названием «Original» содержащий некоторое количество страниц с изображениями;
- Другой сайт, по названием «Consumer», содержит неправомерные ссылки на графические ресурсы с сайта «Original»;
- Требуется исключить получение оригинальной графической информации сайтом «Consumer» с сайта «Original».

Решением является создание особенного HttpHandler'а – серверного обработчика запросов к сайту [3]. Для этого к web-приложению добавляется новый файл с расширением .ashx и в его теле описывается класс «ReferenceController», который реализует интерфейс IHttpHandler и определяет метод обработки запроса – ProcessRequest():

```
using System;
using System.Web;
public class ReferenceController : IHttpHandler {
    public void ProcessRequest (HttpContext context) {
            // Обработка запроса.
    }
    public bool IsReusable {
        get {            return false;        }
    }
}
```

Листинг 1. Реализация интерфейса IHttpHandler средствами языка C#

Для регистрации обработчика необходимо в конфигурационном файле сайта определить HttpHandler в xml-теге «system.web\httpHandlers» на каждое из интересующих нас расширений файлов:

```
<system.web>
  <httpHandlers>
    <add path="*.jpg" verb="GET" type="ReferenceController"/>
    <add path="*.png" verb="GET" type="ReferenceController"/>
    <add path="*.gif" verb="GET" type="ReferenceController"/>
  </httpHandlers>
</system.web>
```

Листинг 2. Регистрация собственного HttpHandler'а в конфигурационном файле web-сайта

Данный обработчик проверяет, кто ссылается на запрашиваемый ресурс, используя свойство Referer у текущего запроса, и по результатам проверки возвращает в качестве ответа (Response) либо ожидаемое графическое изображение в случае оригинальных ссылок; либо, в случае неправомерных ссылок, выполняет один из следующих сценариев:

- генерирует серверную ошибку;
- возвращает картинку-заглушку;
- возвращает ожидаемое графическое изображение с некоторой обработкой.

Алгоритм проверки представлен на рис. 1.

Универсальность данного подхода в том, что конкретные данные, такие как имя ресурса и имя web-приложения в коде не фигурируют,что позволяет применять HttpHandler для всех ASP.Net приложений. Для этого необходимо заранее описать HttpHandler "ReferenceController" в отдельной .Net сборке, сделать её доступной web-приложению и зарегистрировать полное имя типа в конфигурационном сайте. Доступность приложению достигается несколькими способами:

1. Размещение сборки в глобальном кэше сборок (GAC);
2. Размещение сборки в собственном каталоге сборок web-приложения.

В любом случае, регистрация HttpHandler'а для этой цели будет осуществляться по полному имени типа, как показано в листинге 3:

```
<system.web>
  <httpHandlers>
    <add path="*.jpg" verb="GET" type="[FullTypeName]"/>
    <add path="*.png" verb="GET" type="[FullTypeName]"/>
    <add path="*.gif" verb="GET" type="[FullTypeName]"/>
  </httpHandlers>
</system.web>
```

Листинг 3. Регистрация HttpHandler'а в конфигурационном файле web-сайта

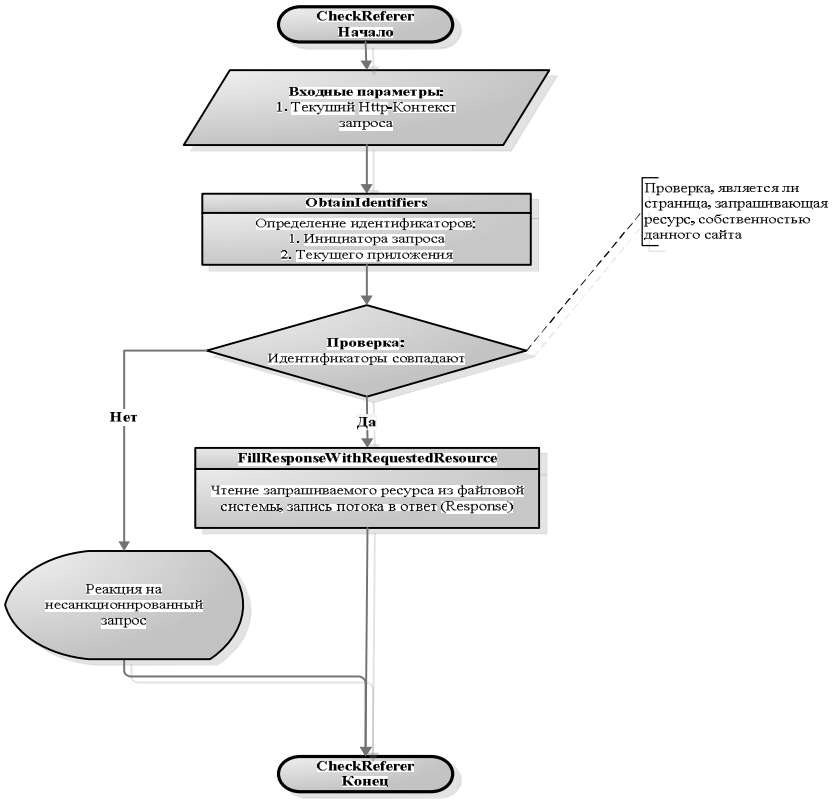


Рис. 1. Общая схема алгоритма проверки инициатора запроса

Таким образом, все запросы графических файлов, приходящие на web-сайт «Original», будут обработаны при помощи класа «ReferenceController». Для других расширений файлов можно применять подобный подход с тем же успехом. Единственное ограничение использования – это вопрос производительности сайта. Дополнительные операции с так называемыми «flat files», которыми являются пассивные с точки зрения серверной обработки изображения, таблицы стилей, клиентские скрипты; нагружают web-сервер и тормозят работу web-приложения. Созданный в таком простейшем виде HttpHandler обуславливает падение производительности обработки запросов.

Влияние на производительность и оптимизация решения

Для оптимизации формирования тела ответа (Response) необходимо реализовать кэширование содержимого Response. При первом запросе отдельного файла его содержимое помещается в коллекцию кэша. Ключом элемента коллекции является пара - имя запрашиваемого файла и флаг, является ли запрос правомерным; значением – содержимое файла или альтернативное содержимое, возвращаемое в ответ на неправомерные запросы. Пример заполненнной коллекции описан в таблице:

№ п/п	Имя файла	Ключ элемента коллекции	Значение элемента коллекции
1	Logo.gif	1. logo.gif_true 2. logo.gif_false	1.  2. 
2	External.js	1. external.js_true 2. external.js_false	1. var a = 15; 2. /* Запрашиваемый скрипт недоступен */

Таблица. Пример заполнения коллекции кэша

Рассмотрим реализацию кэширования JavaScript файлов web-приложения «Original». Алгоритм несложен, его схема представлена на рис. 2.

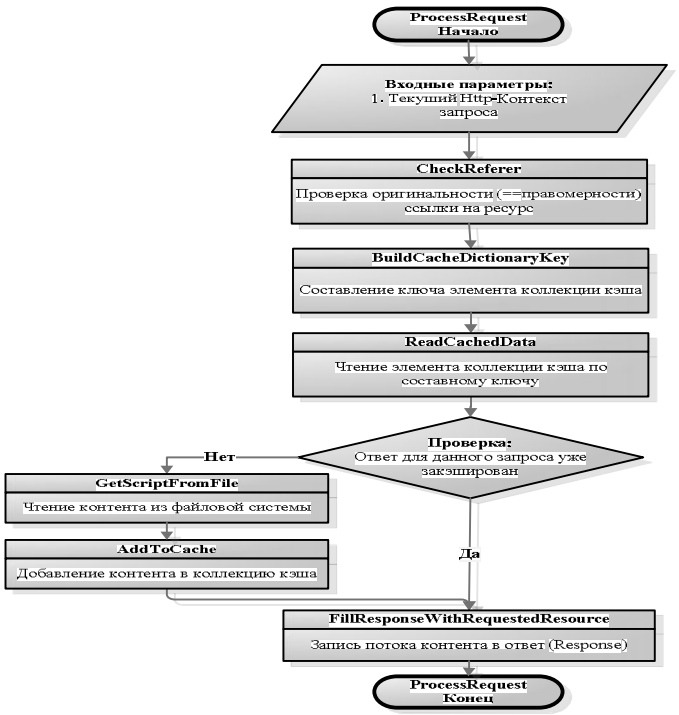


Рис. 2. Общая схема алгоритма кэширования запросов к ресурсам

Подпись изображений и внедрение ЦВЗ

Для графических изображений можно реализовать их автоматическое подписывание с целью опубликования информации об авторе. Это может быть текст или иная графическая информация размещённая в какой-либо (например, нижней) части изображения, однозначно ассоциирующаяся с личностью автора-правообладателя. Такие «метки» служат неопровержимой сылкой на источник, предоставивший конкретный графический файл. Однако более интересен вариант внедрения в изображения цифровых водяных знаков [4] – цифровых меток, скрытых в файле, позволяющих подтвердить и проверить права разработчика на данный файл мультимедиа. Такие метки могут быть различным образом расположены в мультимедийном файле и служить противодействием следующим неправомерным деяниям:

1. Подмена авторства.
2. Отказ от авторства.

Замечателен факт, что и метки, и ЦВЗ довольно легко реализовать в том же самом HttpHandler’е «ReferenceController».

Для внесения в графику видимых изменений (меток), необходимо получить байтовое представление графического потока, сериализовать его в изображение, храня-

щееся в виртуалой памяти и с помощью функций работы с графикой пометить изображение заранее продуманным образом. Далее модифицированное изображение десериализуется в байтовый поток, который впоследствии фигурирует во всех операциях как изображение, предоставляемое конечному пользователю Web-приложения.

Внедрение ЦВЗ происходит иначе, поскольку такое модифицирование файла не должно быть заметно человеческому глазу и, вместе с тем, должно распознаваться программами проверки наличия ЦВЗ. Не углубляясь в конкретику процедуры встраивания отметим её математическую сложность. Для нашей задачи важно следующее:

1. Необходимо наличие внешнего модуля, осуществляющего данное встраивание.
2. Необходимо предоставить входные данные (поток графической информации) для встраивания ЦВЗ.
3. Необходимо обработать полученные данные и записать их в ответ сервера.

Требование наличия внешнего модуля обоснованно и позволяет развязать общий алгоритм решения и конкретику алгоритма встраивания ЦВЗ.

Эффективная защита клиентского кода

На сегодняшний день единственным эффективным способом сохранения исключительного права на использование клиентского скрипта (в статье ограничимся рассмотрением Java Script файлов) является его обфускация (запутывание кода). Это заключение подтверждается многолетним опытом разработки приложений и масштабной исследовательской работой проделанной в данной и смежных областях программной инженирии.

Обфускация кода лишает его смысловой нагрузки, понятной для читателя. Названия переменных, функций, синтаксис – становятся бессмысленной линейной комбинацией символов алфавита.

Существует множество утилит, производящих операцию обфускации. Наиболее интересной предстает продукт под название Jasob[5], который позволяет запутывать код файлов JavaScript, html, aspx и множества других без потери функциональности. Полезно и наличие двух вариантов работы с Jasob:

1. Интерактивный – через графический пользовательский интерфейс.
2. Автоматический – через коммандную строку.

Листинги 4 и 5 показывают разницу между оригинальным и обфусцированным вариантами JavaScript кода:

```
function CalculateSalary(aEmployees)
{
   var nEmpIndex = 0;
   while (nEmpIndex < aEmployees.length)
   {
      var Employee = aEmployees[nEmpIndex];
      Employee.fSalary = CalculateBaseSalary(Employee.nType);
      if (Employee.bBonusAllowed == true)
      {Employee.fB = CalculateBonusSalary(Employee.nType); }
      else
      { Employee.fB = 0;  }
      Employee.sSalaryColor = GetSalaryColor(Employee.fSalary +Employee.fB);
      nEmpIndex++;
   }
}
```

Листинг 4. Пример оригинального кода JavaScript

```
function c(g){var m=0;while(m<g.length){var
r=g[m];r.l=d(r.n,r.o);if(r.j==true){
r.k=e(r.n,r.o,r.l);}else{r.k=0;}r.t=f(r.l+r.k);m++;}}
```

Листинг 5. Пример обфусцированного кода JavaScript

Приведённые примеры кода описывают одну функциональность и нетрудно заметить, насколько мал размер соответствующего обфусцированного кода по отношению к оригиналу. Данный факт показывает ещё одну выгодную сторону применения обфускации – сокращение объёма, необходимого для хранения информации без потери функциональности.

Заключение

Пути нарушения прав собственности на продукты интеллектуального труда, такие как web-приложения, многообразны. Среди прочих – несанкционированное использование элементов контента web-сайта, в том числе в автоматическом режиме. Однако, подходы, позволяющие успешно противодействовать данным проблемам, существуют и в умелых руках находят действенную реализацию. Прежде всего это защита от автоматических сылок, сквозное подписывание графических ресурсов, внедрение ЦВЗ и обфускация клиентского кода. Названные способы просты в реализации и действенны. Каждое предлагаемое в статье решение расширяемое, набор базовой функциональности позволяет улучшать механизмы защиты не забывая о вопросе производительности защищаемого web-приложения.

Литература

1. Microsoft ASP.Net [Электронный ресурс] / Microsoft Corporation, 2008. – Режим доступа: http://www.asp.net/, свободный. – Загл. с экрана. – Яз. англ.
2. Microsoft Internet Information Services [Электронный ресурс] / Microsoft Corporation, 2008. – Режим доступа: http://www.iis.net/, свободный. – Загл. с экрана. – Яз. англ.
3. Microsoft Software Development Network [Электронный ресурс] / Creating HttpHandlers, 2008. – Режим доступа: http://msdn.microsoft.com/en-us/library/f3ff8w4a(VS.71).aspx, свободный. - Загл. с экрана. – Яз. англ.
4. Грибунин В.Г. Цифровая стеганография. Справочное пособие – СПб.: Солон-Пресс 2002. – 272с.
5. Jasob Obfuscator [Электронный ресурс] / JavaScript Obfuscation Fascination, 2008. – Режим доступа: http://www.jasob.com/, свободный. – Загл. с экрана. - Яз. англ.

УДК 681.4

ИСПОЛЬЗОВАНИЕ МАТРИЦ ДИСКРЕТНО-КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ В МЕТОДИКЕ ОЦЕНКИ ВНЕСЕННЫХ ИСКАЖЕНИЙ В НЕПОДВИЖНЫЕ ЦИФРОВЫЕ ИЗОБРАЖЕНИЯ

Н.Н. Прохожев, О.В. Михайличенко
Научный руководитель – д.т.н., профессор А.Г. Коробейников

В статье рассматриваются существующие методы оценки искажений для неподвижных цифровых изображений. Проводится анализ методик при практическом их применении. Предлагается новый метод оценки искажений, основанный на дискретно-косинусном преобразовании и матрицах квантования стандарта JPEG. Приводятся результаты практического применения нового метода, а также даются рекомендации по его применению.

Ключевые слова: методы оценки искажений, матрица квантования, стеганография

Введение

Наличие объективного инструментария для определения уровня искажений в цифровых изображениях является необходимым условием для проведения успешных разработок и исследований в целом ряде направлений связанных с информационными технологиями.

Прежде всего, это актуально для разработчиков различного рода видеокодеков и стеганографических систем. В данных направлениях искажение изображения-оригинала является, хоть и нежелательным, но неотъемлемым атрибутом. Мировым сообществом прилагаются усилия по разработке эффективных объективных метрик оценок уровня искажений и определения качества изображения.

Современные метрики оценки уровня искажений в цифровых изображениях

Существующие на данный момент метрики можно разделить на две большие подгруппы. Это метрики учитывающие систему человеческого зрения и без учета таковой.

Метрики, не учитывающие систему человеческого зрения, как правило, заимствованы из других областей, имеющих дело с сигналами. К таким метрикам можно отнести соотношение сигнал/шум, корреляцию, метрики спектральной области. Несмотря на то, что эти метрики хорошо себя зарекомендовали для оценки искажений в сигналах самой разной природы, для цифровых изображений это не лучший способ оценки. В первую очередь, это относиться к группе, так называемых, пиксельных метрик. Оценка искажений в пиксельных метриках возможна только по всему изображению целиком, соответственно, и результат получается для всего изображения в целом, без какого либо учета локализации искажающего воздействия. Таким образом, невозможно сделать различия между равномерно искаженным изображением, скажем при гаусовском зашумлении, и с искажением малой локализации, но с большой интенсивностью. На рис. 1 проиллюстрирован описанный выше основной недостаток такого подхода к оценке искажения для цифровых изображений.

Для обоих искаженных изображений параметры, как PSNR (Peak Signal Noise Rate) или корреляция, будут одинаковы, в то время как визуальные артефакты искажений значительно различаются системой восприятия человеческого зрения (СЧЗ). Единственной сферой применения пиксельных метрик может быть оценка искажений слабого уровня, не приводящих к их визуализации. То есть, если СЧЗ не фиксирует искажения, то вполне можно оценить их уровень и без учета ее особенностей. Хотя, такое применение возможно только в очень узком круге задач.

Метрики учитывающие СЧЗ основываются, прежде всего, на ее основных особенностях, таких как, чувствительность к изменению яркости изображения, частотная чувствительность, эффект маскирования в пространственной области и т.д. Одной из возможностей построения метрик данного класса является предварительная фильтрация изображения полосовыми фильтрами, имитирующими их восприятие человеком.

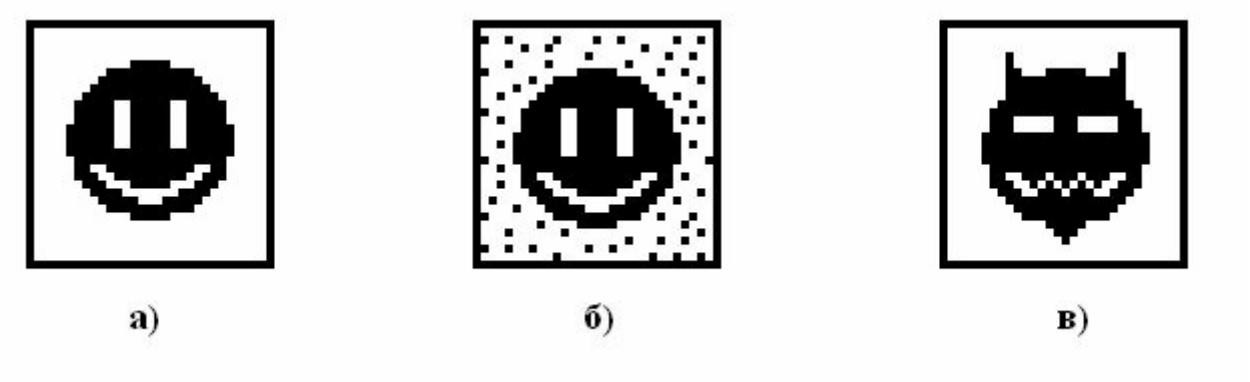


Рис. 1. Отличия восприятия равномерного и локализованного искажений изображений: а) оригинал изображения; б) равномерно искаженное изображение; в) локализованное искаженное изображение

Другой возможностью построения метрик, учитывающих свойства зрения, является выполнение вейвлет-преобразования исходного и искаженного изображения, в результате чего изображение будет представлено на нескольких масштабах. Далее, для каждой субполосы вейвлет-области надо выбрать масштабный вес, на который будет умножаться та или иная метрика, вычисленная локально для этой области. В зависимости от задачи, эти веса могут варьироваться. Например, если важен учет высокочастотных составляющих (четкость линий и т.д.), то веса для высокочастотных областей могут быть увеличены [1]. К недостаткам метрик данной группы можно отнести, как значительную вычислительную емкость, так и сложность настройки метрики. Необходимо подобрать множество коэффициентов, размеров окон и видов фильтров. Такой подход приводит к тому, что хорошо настроенная метрика дает неплохие оценки, но, только для определенного искажающего воздействия. Что и подтверждается на практике. Довольно удачная метрика SSIM (Structural Similarity Image Measure) хорошо зарекомендовала себя при сравнительном тестировании видеокодеков. Однако ее непросто применить для сравнения искажений различной природы, скажем зашумленного изображения и изображения, к которому был применен усредняющий фильтр или JPEG сжатие с потерями. Не лучшим образом данная метрика показала себя и при сравнении различных стеганоалгоритмов частотной области встраивания.

Разработанная метрика на основе ДКП

В силу всего вышесказанного авторами статьи была разработана метрика на основе ДКП преобразования. Алгоритм метрики представлен на рис. 2.

Оригинальное и искаженное изображения делятся на блоки, размером 8x8 пикселей. Каждый блок подвергается ДКП и вычисляется разность коэффициентов между соответствующими матрицами коэффициентов оригинального и искаженного изображения. Различные области коэффициентов матрицы ДКП отвечают за разные частотные компоненты изображения и СЧЗ, которая так же по-разному восприимчива к различным деталям изображения.

Математическое описание такой избирательности СЧЗ задача сложная, поэтому предлагается воспользоваться результатами, полученными при субъективной оценке в лаборатории JPEG (Joint Photographic Experts Group). В рамках работы над одноименным алгоритмом и решая задачу сжатия изображений с наименьшими искажениями,

специалистами лаборатории JPEG была определена матрица квантования, см. рис. 3, которая отражает значимость коэффициентов матрицы ДКП для СЧЗ.

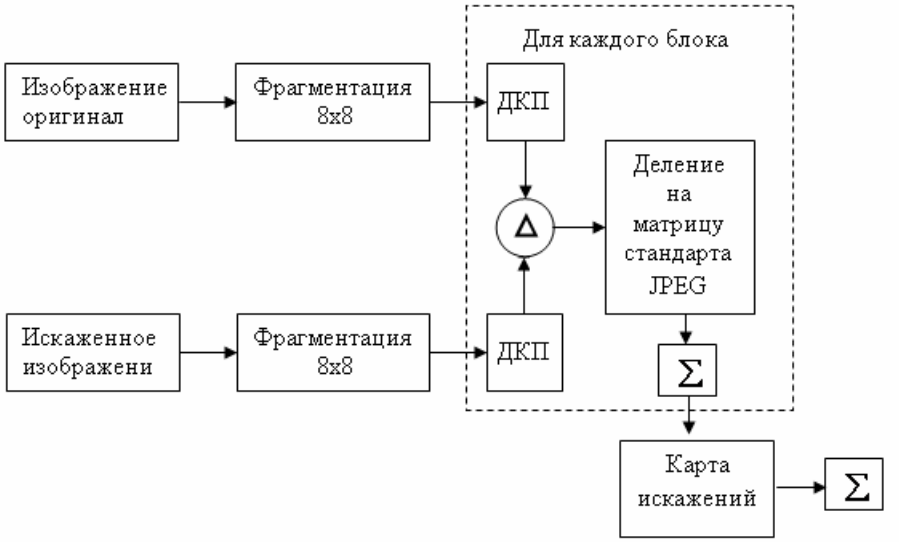


Рис. 2. Алгоритм вычисления уровня искажений на основе ДКП

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	102	121	120	101
72	92	95	98	112	100	103	99

Рис. 3. Коэффициенты матрицы квантования стандарта JPEG

Поэтому после получения разностной матрицы коэффициентов ДКП, выполним ее деление на матрицу квантования стандарта JPEG.

Полученную результирующую матрицу просуммируем без учета знака коэффициентов матрицы. Результатом будет являться уровень искажений для конкретного блока. Таким образом, вычислив искажения для каждого из блоков изображения, мы получим соответствующую карту искажений. Для получения общей величины искажений для изображения в целом, усредним значения по всей карте искажений. Если необходимо увеличить или загрубить «чувствительность» оценки, можно использовать матрицу квантования с некоторым коэффициентом, как это делается в стандарте JPEG для различных значений коэффициента качества.

Вывод

В работе предложен достаточно простой метод оценки искажений, учитывающий особенности человеческого зрения. Метрика не требует тонкой настройки и большой вычислительной мощности. Наилучшие результаты данная метрика будет демонстрировать для искажений частотного характера, которые, в первую очередь, воздействуют на матрицу ДКП коэффициентов. Метрика расширяема и для цветных изображений, для чего необходимо воспользоваться матрицами квантования JPEG для плоскостей интенсивности, хроматического красного и хроматического синего. Для последних

двух следует, также, использовать коэффициенты, величина которых может быть пропорциональна схожим коэффициентам при семплировании цветовых плоскостей в стандарте JPEG.

Литература

1. Грибунин В.Г. Объективные метрики для оценки качества видеокодеков //Технология защиты. – 2008. – № 2.
2. Wang Z., Bovik A., Sheikh H., Simoncelli E. Image Quality Assessment: From Error Visibility to Structural Similarity //IEEE Trans. On Image Proc. – 2004. – № 4. – Vol. 13.

УДК 004.654

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ БАЗ ДАННЫХ ПРИ ПРОЕКТИРОВАНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

П.В. Федосов, А.С. Федотов
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

В статье приводятся краткие сведения о форматах и способах хранения данных в современных САПР. А так же описываются особенности коллективной работы с САПР, сложности, которые это вызывает, и пути их преодоления. Статья будет полезна тем, кто хочет подробнее узнать о создании САПР с возможность коллективной работы и связанных с этим трудностях

Ключевые слова: САПР, хранение данных, форматы файлов, базы данных

Введение

С каждым годом сложность окружающих нас систем и сооружений все возрастает. Улучшаются технологические процессы, внедряются новые материалы, разрабатываются новые технологии. Однако одновременно с этим происходит и усложнение самих проектов, а как следствие увеличиваются трудозатраты на их создание. Именно с этим изначально было связано повсеместное внедрение САПР [1]. Но с дальнейшим ростом сложности проектов даже одновременная работа нескольких инженеров над различными частями одного проекта становится не достаточно эффективной.

В современных САПР эта проблема решается по-разному. Давайте рассмотрим один из способов – параллельное проектирование или параллельный инжиниринг. Изначально этот термин появился в 80-е годы XX века в США. Его целью является повышение качества и сокращение сроков разработки. В настоящее время данный метод претерпел некоторые изменения, но больше частью они коснулись средств проектирования – САПР.

Способы хранения данных

Во многом на выбор способа хранения данных влияет объем и тип хранимых данных. Существует два наиболее распространенных пути хранения данных. В файле – данный метод исторически появился раньше, однако уже тогда у него были серьезные недостатки, главными из которых являются [2]:

- относительная сложность резервного копирования;
- сложность масштабирования системы хранения;
- подверженность отказам оборудования.

Хранение данных во внешней базе не лишено всех вышеперечисленных недостатков, но в данном случае они проявляются гораздо реже в силу того, что обслуживанию специально выделенных серверов уделяется больше внимания, чем отдельным рабочим станциям. Нельзя однозначно заявлять, что какой-то из этих методов плох, именно поэтому они оба гармонично уживаются до наших дней. Так же стоит отметить, что существует промежуточный вариант, который в последнее время становится все более популярным. Он сочетает в себе достоинства выше описанных методов. Это, так называемые, file flat database – встраиваемые базы данных. Отличительной чертой таких баз данных является то, что для их работы не требуется выделенный сервер, доступ к данным и их обработка осуществляется так, как если бы работа шла с обычной базой данных, однако все данные хранятся в файле [3]. Схема такого взаимодействия и его отличия от классических клиент-серверных баз данных показана на рисунке. Это позволяет использовать результаты работы в любом месте, без необходимости постоянно находится в одной сети с сервером базы данных. Однако с таким файлом могут параллельно рабо-

тать несколько пользователей, что во многих случая весьма удобно.

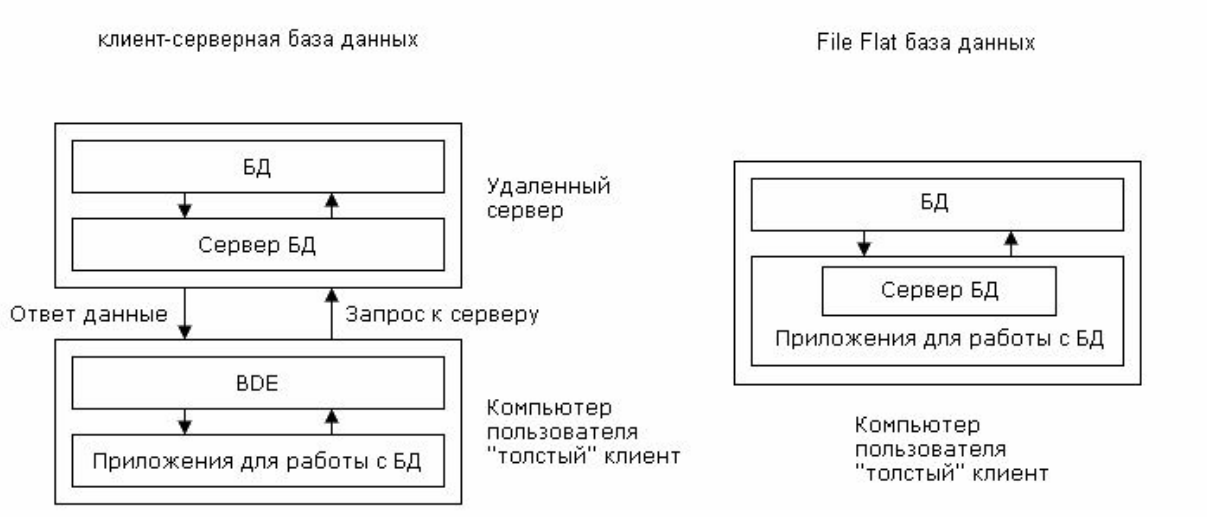


Рисунок. Клиент-серверная и file flat базы данных

Современные форматы файлов САПР

Специфичность задач, выполняемых различными системами автоматизированного проектирования, сказалась и на файлах хранение данных. До недавнего времени фактически у каждой компании был разработаны собственные закрытые форматы, что вызывало множество проблем с совместимостью.

Именно это побудило компанию Autodesk разработать формат DXF, универсальность и открытость которого сделали его на данный момент основным форматом межсистемного обмена. На данный момент практически все современные САПР поддерживают экспорт и импорт в данный формат.

Однако, не смотря на свою открытость, DXF все же является разработкой фирмы Autodesk и нацелен, в первую очередь на ее основную линейку продуктов – AutoCAD. Постоянное развитие этой САПР провоцирует внесение соответствующих изменений и в спецификации DXF. Это неизбежно приводит к проблемам совместимости с уже существующими приложениями.

В более поздних версиях своих продуктов, Autodesk начала использовать двоичный формат файлы – DWG. Он так же является разработкой Autodesk, но это закрытый формат, спецификации которого никогда не публиковались. Для разработки библиотек, которые позволили бы сторонним программным продуктам работать с форматом DWG, был создан консорциум ODA (Open Design Alliance) [4].

Консорциумом была произведена обратная разработка формата DWG и разработаны соответствующие программные библиотеки, разработаны спецификации OpenDWG, доступ к которым открыт всем желающим. ODA осуществляет поддержку OpenDWG в актуальном состоянии. Финансирование разработки программных библиотек производится на членские взносы участников консорциума. В Open Design Alliance состоит 32 участника-учредителя (Founding Members) и свыше 600 коммерческих (Commercial Members) и поддерживающих участников (Sustaining Members) (данные на начало 2008 года). В число поддерживающих участников (Sustaining Members) входят, например, ведущие российские производители САПР, такие как: АСКОН (Компас (САПР)), Топ Системы (T-FLEX CAD) и другие.

Таким образом, на данный момент подавляющее большинство различных САПР поддерживают форматы межсистемного обмена DWG.

Однако этим развитие формата DWG не ограничилось. В последних версиях формата DWG появились нововведения, например специальный механизма запросов, по-

зволяющие организовывать параллельную работу нескольких пользователей с одним файлом данных. Это позволяет сократить затраты на разработку и отказаться от таких инструментов, как, например, системы контроля версий.

Большинство современных форматов файлов САПР уже давно напоминают своей структурой базы дынных, а многие именно ими и являются. Однако сейчас многие форматы являются закрытыми, отсутствует актуальная документация, а разработчики не желают открывать свои форматы. А так же развитие и выход на массовый ранок свободного программного обеспечения, и появление достойных аналогов платных систем автоматизации проектирования, привели к тому, что в качестве файлов данных стали использовать различные разновидности баз данных. Несомненным достоинством такого способа хранения данных является универсальность. Благодаря которой без больших трудозатрат можно обеспечить поддержку большого спектра баз данных, а так же конвертации данных между ними. Однако переносимость и удобство применения такого решения по сравнению с классическим хранением результатов работы в файле не очевидно. В настоящее время встраиваемые базы данных активно развиваются как отдельное направление. Свои разработки имеют многие известные компании и организации, среди них:

- Berkeley DB;
- MySQL Embedded [5];
- SQLLite [5];
- TextDB;
- Mimesis;
- TheIntegrationEngineer.

Применение этих технологий, позволяет значительно упростить работу с файлами данных, как из самого САПР'а [6], так и из сторонних программ, упразднить проблему совместимость форматов, упростить преобразование из одного формата в другой. Так же, отсутствие блокировок, быстрота обращения к файлу позволяют добиться высокой производительности.

Заключение

В статье рассматривались возможности совместной работы современных САПР и связанные с этим сложности организации хранения данных. В настоящее время в виду все возрастающей сложности проектов, совместная разработка становится все более часто встречающимся явлением. Однако ее полноценная реализация сильно зависит от области деятельности проектировщика и специфических ограничений, накладываемых как технологическими, так и экономическими факторами.

Литература

1. Боровский А.Н. Современные средства разработки Borland для Oracle и MS SQL Server. – СПб.: БХВ-Петербург, 2007. – 385 с.
2. Васвани В. Полный справочник по MySQL. – М.: Вильямс, 2006. – 517 с.
3. Гринвальд Р. Oracle: справочник. – М.: Символ, 2005. – 975 с.
4. Ли К. Основы САПР (CAD/CAM/CAE). – СПб.: Питер, 2004. – 560 с.
5. Кузнецов М.В. MySQL 5. – СПб.: БХВ-Петербург, 2006. – 1002 с.
6. Семенова И.И. SQL стандарт в СУБД MS SQL Server, Oracle, VFP и Access. – Омск: СибАДИ, 2008. – 257 с.

УДК 004.942

СИСТЕМА ПОДДЕРЖКИ ПРИНЯТИЯ ПРОЕКТНЫХ РЕШЕНИЙ В СФЕРЕ ИНЖЕНЕРНОГО АНАЛИЗА РАДИОЭЛЕКТРОННЫХ СРЕДСТВ

Д.А. Боголюбов
Научный руководитель − к.т.н., доцент Н.С. Кармановский

Данная работа посвящена системе поддержки принятия решений на этапе конструкторского проектирования, разработанной в рамках специализированного проекта в Российском Институте Радионавигации и Времени в 2005–2008 гг. Система призвана сопровождать процесс проектирования радиоэлектронного устройства от создания трёхмерной модели до проведения инженерных расчётов и конструирования самого устройства. Приводится общий алгоритм системы, описаны принципы функционирования.

Ключевые слова: САПР, системы принятия решений, инженерные расчёты

Введение

В настоящее время системы принятия решений различного уровня разрабатываются повсеместно для различных отраслей человеческой деятельности [1]. Как известно, такая система – это компьютерный автоматизированный программно-аппаратный комплекс, целью которой является помощь людям, принимающим решение в сложных условиях для полного и объективного анализа предметной деятельности. Системы поддержки принятия решений (СППР) возникли в результате слияния управленческих информационных систем и систем управления базами данных. Такая система призвана автоматизировать процесс проектирования либо разработки и обеспечить возможность наблюдения над ходом работы и контроль в режиме реального времени.

Система была в рамках проекта внедрения методики проведения автоматизированных инженерных расчётов в Российском Институте Радионавигации и Времени при работе над системой глобальной спутниковой навигации ГЛОНАСС. Отдельные составляющие этого проекта были представлены автором данной работы ранее [2, 3].

Целью настоящей работы явилось создание и внедрение системы поддержки принятия решений в сфере систем конечно-элементной дискретизации на этапе проектирования бортовой радиоэлектронной аппаратуры.

Результатом данного проекта является систематизация процессов, составляющих этап конструкторского проектирования радиоэлектронной аппаратуры. В настоящее время система находится в стадии предварительного тестирования.

В течение трёх лет отдельные составляющие данной системы разрабатывались по отдельности как самостоятельные модули. В целях повышения степени адекватности системы новым экономическим условиям было принято решение о создании СППР, сопровождающей весь процесс проектирования.

В основу разрабатываемой системы лежит принцип разделения процесса проектирования на следующие этапы:

1. разработка технического задания, выбор элементной базы и моделирование;
2. разработка принципиальной схемы;
3. программирование микроконтроллеров и проектирование логических интегральных схем;
4. разработка печатной платы;
5. трехмерное твердотельное проектирование;
6. монтаж и отладка;
7. разработка программного обеспечения для ПК, осуществляющего взаимодействие с устройством;

8. испытания и подготовка протокола испытаний;
9. подготовка документации.

Как было показано ранее [2, 4], автоматизация процесса проектирования невозможна без современных CAD/CAE систем, отвечающих требованиям ГОСТ и стандартам предприятия. По ряду критериев [4] была выбрана САПР SolidWorks/COSMOSWorks, предоставляющая возможность автоматизировать большинство процессов, составляющих этап конструкторского проектирования.

Основным новшеством, внесённым данным программным продуктом, явилась автоматизация процесса как моделирования устройства, так и испытаний и сопутствующей корректировки модели. Это позволило повысить экономическую эффективность процесса и снизить время на разработку радиоэлектронного устройства [4].

Рассмотрим применение системы принятия проектных решений на примере процесса создания дискретизации трёхмерной модели.

Используемая САПР SolidWorks/COSMOSWorks предоставляет широкий спектр инструментов для создания конечно-элементной дискретизации. В процессе разработки методики теплового расчёта были исследованы и другие методы подготовки трёхмерной модели к проведению инженерных расчётов[5], в частности, на основе бессеточных методов, методов граничных элементов и т.д. Выбор в пользу САПР SolidWorks был сделан ввиду удовлетворительной точности расчётов, возможности интеграции с системами принятия решений, соответствие российским стандартам и дружественному интерфейсу [4].

Алгоритмы дискретизации, используемые в данной САПР, сводятся к алгоритму Делоне-Вороного и движущегося фронта [6].

Алгоритм Вороного-Делоне [7] основывается на методах триангуляции Делоне и многоугольниках Вороного. Эта часть методов вычислительной геометрии в сравнении с другими требует больших затрат компьютерных мощностей, однако предоставляет требуемую погрешность построения сетки (в соответствии с техническим заданием на данную СППР она составляла 9,5%).

Алгоритм движущегося фронта предполагает работу со сложными для конечно-элементной обработки участками поверхности (тонкостенные элементы, резьбовые отверстия и т.д.) В большинстве расчётов этот алгоритм не используется, так как сложные конструкции, как правило, корректировались с целью упрощения ввиду нехватки вычислительных мощностей.

Пример решения задачи дискретизации

Конечно-элементная дискретизация остаётся одной из самых сложных частей процесса автоматизированного инженерного анализа. На рис. 1 приведён пример построения конечно-элементной сетки для фрагмента трёхмерной модели.

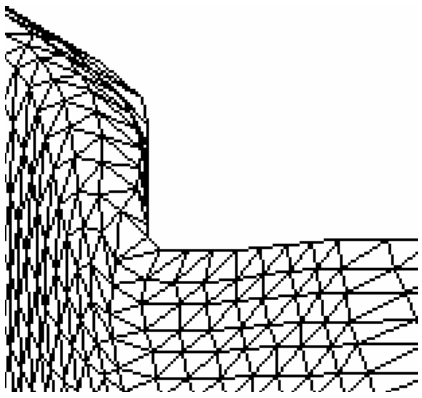


Рис. 1. Пример конечно-элементной дискретизации

В данном случае сетка была построена методом Вороного-Делоне. Можно заметить, что результат конечно-элементной дискретизации следует признать удовлетворительным. Соотношение сторон близко к 1:3–1:1. Применение метода движущегося фронта даёт нежелательный результат – появляется ошибка, проиллюстрированная рис. 2 и 3.

Рис. 2. Фрагмент конечно-элементной дискретизации методом Вороного-Делоне

Рис. 3. Фрагмент конечно-элементной дискретизации методом движущегося фронта

В этой ситуации система выдаст предупреждение пользователю, что не рекомендуется производить дискретизацию методом движущегося фронта. Причины:

1. сетка неоправданно уплотнена;
2. соотношение сторон от 1:1 до 1:10, что не гарантирует допустимой погрешности итогового расчёта.

После серии принятия решений по выбору алгоритма конечно-элементной дискретизации СППР в автоматическом режиме проведёт выбор алгоритма расчёта тепловых режимов, методика которого была разработана ранее [3], а также других инженерных расчётов. На основании выбранных методик будет проведён заданный в техническом задании комплекс расчётов.

Описание алгоритма СППР приведём на примере задачи оптимизации поиска многоугольника Вороного (в нашем случае для n=3), соотношение сторон которого не удовлетворяет условиям (обычно соотношение должно укладываться в интервал 1:1–1:3), и реакции системы на ход решения этой задачи.

1. Проверяются конечные элементы в тех местах, где пользователь потребовал создать более плотную сетку, так как обычно именно в этих местах обнаруживаются дефекты дискретизации.

2. В случае обнаружения такого элемента проверяется возможность создания сетки с помощью альтернативного алгоритма на базе метода движущегося фронта либо путём создания ещё большего уплотнения.

3. Пользователю выдаётся предварительное заключение о возможности построения сетки для данной модели.

Для ускорения работы программы необходимо рассчитать вероятность нахождения дефектного узла Вороного в данном сегменте поверхности с помощью алгоритма поиска узлов, работающего методом частичного перебора конечных элементов.

$$P = 1 - e^{-\frac{P_p}{\omega_p} N_p}. \qquad (1)$$

где P – вероятность нахождения нестандартного узла; P_p – вероятность нахождения такого узла с помощью алгоритма поиска дефектов сетки SolidWorks; ω_P – среднее число прохождений с помощью алгоритма поиска узлов; N_P – константа, зависящая от вычислительных мощностей аппаратного обеспечения СППР и показывающая возможное число прохождений с помощью алгоритма поиска узлов.

Формула (1) выведена в процессе разработки алгоритмов СППР и исследования следствий из закона поражений Колмогорова [8]. Из неё можно вывести выражение для определения вероятности нахождения конечного элемента с неверным соотношением сторон:

$$P_H = 1 - e^{-\alpha m}, \qquad (2)$$

где $P_н$ – вероятность обнаружения элемента; α – удельная эффективность алгоритма (при разработке СППР устанавливалась эмпирически); m – коэффициент вычислительной мощности аппаратных средств.

m и N_p, помноженные на статистические коэффициенты, формируют ресурсный показатель целевой функции.

Если вероятности, рассчитанные по вышеприведённым формулам, не превышает значения, заданного в техническом задании, программа выдаст предупреждение пользователю о несоответствии вычислительных мощностей имеющимся в распоряжении СППР алгоритмам, что может привести к аппаратным сбоям либо росту ошибок в конечно-элементной дискретизации. На данной стадии разработки СППР предполагается, что итоговое решение о выполнении процесса дискретизации и инженерного расчёта производит сам пользователь-инженер, производящий автоматизированный расчёт данного устройства.

Полученные результаты

1. Разработана и внедрена на предприятии единая система поддержки принятия решений.
2. Обеспечена возможность контроля над процессом конструкторского проектирования.
3. Повышена эффективность процесса проектирования, уменьшена трудоёмкость на 16%.
4. Достигнут расчётный уровень погрешности в 8%.

В дальнейшем предполагается провести более глубокий анализ алгоритмов поиска конечного элемента с неудовлетворительным соотношением сторон, а также с помощью постоянно пополняемой базы статистических данных о расчётах выработать более адекватный реальным условиям алгоритм работы всей системы в целом для снижения уровня погрешности результатов инженерных расчётов.

Литература

1. Ларичев О.И., Петровский А.В. Системы поддержки принятия решений. Современное состояние и перспективы их развития. // Итоги науки и техники. Сер. Техническая кибернетика. – Т.21. М.: ВИНИТИ, 1987. – С. 131–164.
2. Боголюбов Д.А., Кармановский Н.С. Интерпретация результатов расчётов тепловых режимов ЭВС в приложении COSMOSWorks. // Научно-технический вестник СПбГУ ИТМО. – Выпуск 32. – СПб. – 2006.
3. Боголюбов Д.А., Кармановский Н.С. Исследование тепловых режимов различных радиоэлектронных конструктивов с помощью системы COSMOSWorks. // Научно-технический вестник СПбГУ ИТМО. Выпуск 44. Современные технологии / Главный редактор д.т.н., проф. В.Н. Васильев. – СПб: СПбГУ ИТМО, 2007. – 300 с.
4. Боголюбов Д.А., Григорьева Н.С., Елисеев О.В., Когай Н.В. Автоматизация тепловых расчётов электронных блоков с помощью САПР SolidWorks/COSMOSWorks на этапе конструкторского проектирования. // Научно-технический вестник СПбГУ ИТМО. Выпуск 40. Научная школа «Информационная безопасность, проектирование, технология элементов и узлов компьютерных

систем». Труды молодых учёных / Главный редактор д.т.н., проф. В.Н. Васильев. – СПб: СПбГУ ИТМО, 2007. – 290 с.
5. Боголюбов Д.А. Применение элементов теории графов в конечно-элементном анализе. // Научно-технический вестник СПбГУ ИТМО. Выпуск 51. Научные школы в СПбГУ ИТМО / Главный редактор д.т.н., проф. В.Н. Васильев. – СПб: СПбГУ ИТМО, 2008. – 408 с.
6. Алямовский А.А. SolidWorks/COSMOSWorks 2006–2007. Инженерный анализ методом конечных элементов. – М.: ДМК, 2007. – 784 с., илл.
7. Скворцов А.В. Триангуляция Делоне и её применение. – Томск: Изд-во Том. ун-та, 2002. – 128 с.
8. Абчук В.А., Матвейчук Ф.А., Томашевский Л.П. Справочник по исследованию операций. – М.: Воениздат, 1979. – 451 с.

УДК 004.738.5

АРХИТЕКТУРА РАСПРЕДЕЛЕННОЙ СЕТИ НАЦИОНАЛЬНЫХ ЛЕКСИКОН-ПРОВАЙДЕРОВ В ИНТЕРНЕТЕ СЛЕДУЮЩЕГО ПОКОЛЕНИЯ

В.В. Власов
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

За последние несколько лет W3C[1] разработал стандарты и технологии для следующего поколения Интернета, т.н. Semantic Web. Несмотря на это, применению и распространению этих стандартов препятствуют различные факторы. В данной статье рассматриваются следующие проблемы: архитектура будущего Интернета на основе распределенной сети лексикон-провайдеров, а также предлагается использование национальных языков для представления знаний и обмена ими независимо от языковой принадлежности пользователей.
Ключевые слова: интернет, семантический веб, RDF, стандарты, лексикон-провайдер

Введение

Впервые о Semantic Web (Семантическом Вебе, далее СВ) заговорили еще в 2001 году [1]. Сейчас уже созданы важные технологии для перехода к этому этапу развития Интернета. Это и расширяемый язык разметки (XML), и технология описания ресурсов (Resource Description Framework, RDF[2]), ставшая стандартом W3C для интероперабельных машиночитаемых данных. Появился язык веб-онтологий (Web Ontology Language, OWL[3], которому 10 февраля 2004 года W3C присвоил статус рекомендованной к реализации технологии. Был также разработан язык запросов SPARQL[4], получивший аналогичный статус в 2008 году. Для практической реализации СВ критично также наличие словарей метаданных общего и, что еще более сложно, тематического назначения, стандартизирующих описания ресурсов в формате RDF и сущностей в формате OWL. Именно практическая реализуемость создания таких библиотек, которые могли бы описать все необходимые разработчикам описания и сущности, часто ставится под сомнение.

Несмотря на это, имеется ряд обнадеживающих примеров. Одним из первых серьёзных и популярных проектов, основанным на принципах семантической паутины, стал проект «Дублинское ядро», реализуемый инициативной организацией Dublin Core Metadata Initiative (DCMI)[5]. Это открытый проект, цель которого – разработать стандарты метаданных, которые были бы независимы от платформ и подходили бы для широкого спектра задач. Однако не все необходимые понятия описываются в нем. Например, создается большое количество стандартов, ориентированных на нужды Web 2.0 [2], такие как словарь Friend-of-a-Friend [FOAF][6], для описания контактов и отношения знакомств между людьми, SIOC[7] и другие. Но самым популярным наследником RDF стал, безусловно, формат распространения новостей RSS 1.0[8].

Однако, уже прошло более 7 лет с момента объявления старта разработок в области СВ, но Интернет все так же полон неструктурированной информации, и разработчики не спешат использовать созданные стандарты. Разработка онтологий остается уделом научных лабораторий, а количество знаний, которые пользователи Интернета выкладывают в Сети, растет катастрофическими размерами. Именно применение СВ для управления коллективными знаниями является одной из наиболее актуальных проблем.

---

[1] http://www.w3.org/
[2] http://www.w3.org/RDF/
[3] http://www.w3.org/2004/OWL/
[4] http://www.w3.org/TR/2008/REC-rdf-sparql-protocol-20080115/
[5] http://dublincore.org
[6] D. Miller, D. Brickley, Friend of a Friend Project, http://www.foafproject.org/ и http://xmlns.com/foaf/0.1/
[7] http://sioc-project.org/
[8] http://web.resource.org/rss/1.0/

Таким образом, назрела необходимость развития архитектуры СВ и развития региональной (национальной) поддержки библиотек RDF и онтологий на родных языках. Если применение исключительно английского языка в языках разметки было верным решением, то в вопросах управления и представления знаний безусловно должны быть использованы родные языки того региона, для которого создается Интернет-ресурс. Это касается не только представления, но и связей и особенностей грамматик языков, будь, то латиница, кириллица, иероглифы, иврит или другие. Это будет также способствовать распространению стандартов СВ, стимулировать людей публиковать свои знания в структурированном виде, и на родном языке.

В связи с этим, в данной статье вводится понятие *лексикон-провайдеров* – интернет-ресурсов, которые и предоставляют в пользование словари и логики, необходимые для поддержки распределенной архитектуры СВ. За разработку и поддержку этих компонентов отвечают либо организации, которые их создают, либо *региональный семантический центр*, который также отвечает за взаимодействие с другими центрами и стандартизацию словарей. В данной статье будет показано, как можно автоматизировать и унифицировать процесс получения и использования онтологий и библиотек и предложена архитектура распределенной сети *национальных* лексикон-провайдеров, что значит использующих *национальные* языки для представления и обработки знаний и информации.

Основная часть

Существующие интернет-ресурсы в основном разрабатывались для использования их людьми. Несмотря на то, что язык разметки HTML позволял определять логическую структуру документа, понятную машине, и включать в страницу различные метаданные, но с точки зрения поисковиков и компьютерных программ веб-страницы все еще оставались набором слов без какого-либо смысла и значения. В то время как человек визуально определяет и понимает значение тех или иных ссылок, графических, текстовых и прочих элементов на странице, машине только с помощью дополнительных указаний можно «объяснить» семантическое значение элементов. Поэтому был разработан стандарт XHTML, который позволял добавлять с помощью дополнительных атрибутов машиночитаемые аннотации. Однако кроме добавления семантики существует проблема использования библиотек, с помощью которых можно было бы описать большинство используемых понятий и терминов, о чем еще будет говориться ниже.

Добавление семантики на страницу (к элементам страницы или элементам формы) позволит машине «понимать» смысл отдельных ее частей. Компьютер не «понимает» в полном смысле этого слова ничего из всей этой информации, но теперь он уже сможет манипулировать терминами гораздо более эффективно с тем, чтобы стать полезным и осмысленным для пользователя-человека.

С другой стороны, в современном Интернете существует проблема доступа поисковых машин и программ к данным, так называемого Глубинного Веба (Deep Web) – базам данных, которые скрыты за интерфейсами запросов и не имеют прямых гиперссылок. Не существует не только единого механизма поиска по базам различных сайтов (интернет-магазины, базы данных различных сущностей, социальные сети и др.), но и единого представления одних и тех же данных. Огромное количество стандартной информации используется на различных сайтах: списки стран, городов, почтовые коды, названия университетов, языков, форматы дат, телефонов, адресов, названия сущностей в различных областях деятельности (путешествий, финансы, медицина и прочее). Создатели сайтов самостоятельно составляют эти списки, либо копируют их из других источников. А гораздо проще было бы унифицировано получать эту информацию. Кроме того, единый источник подобной информации дает такое преимущество, как актуальность и полнота информации, которую не может обеспечить самостоятельно ни одна компания.

Всемирно известный интернет-магазин Amazon[9] имеет форму заказа товаров. Разумеется, форма заказа имеет такую информацию, как реквизиты получателя, в котором пользователь должен указать страну, город, почтовый индекс, домашний адрес. Очевидно, что эти данные кроме адреса вполне стандартны и редко изменяются. Предположим, существует авторизованный *семантический центр* в России. Даже если его не будет, то он должен быть создан, потому что никто, кроме живущих в России, не сможет дать полную и актуальную информацию об российских адресах и прочих локальных стандартах. Если пользователь из России указал неправильно почтовый индекс или индекс не соответствует городу (Amazon самостоятельно не сможет определить это, потому что у него нет доступа к базе всех существующих индексов, если такая база уже есть, и городов России и он не знает где ее искать), то Amazon не сможет ему отправить заказанные товары. А если необходимо пользователям показывать эту информацию на их родном языке? Возникает необходимость, чтобы либо носители языка помогли компании Amazon с переводом, либо компания Amazon будет автоматически получать эти данные в необходимом формате из авторизованного источника.

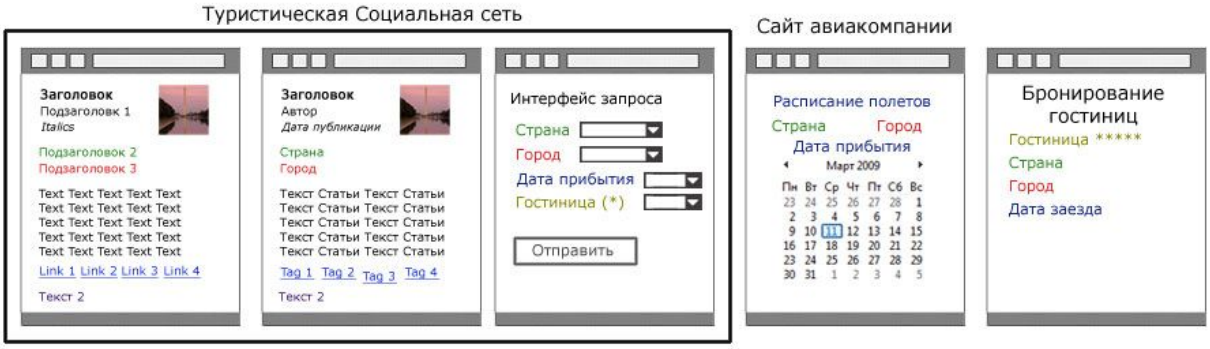
Таким образом, до сих пор не решены две проблемы – встраивание стандартизованных семантических данных в веб-страницы и возможность валидации и получения актуальной и полной информации о стандартных сущностях.

Рассмотрим процесс добавления семантики на веб-страницу и связь одинаковых сущностей между различными сайтами. Возьмем для примера туристическую социальную сеть (далее ТСС), которая позволяет пользователям как писать в своих блогах заметки о местах, так и возможность организовать путешествие. На рис. 1 (а) показана типичная страница статьи о каком-либо городе, на которой имеется несколько элементов. Сначала идет заголовок, потом подзаголовок, блок курсивного текста, потом еще два отдельно стоящих подзаголовка, несколько абзацев текста, и в конце немного ссылок и еще один блок текста. Однако машина и человек воспринимают страницу по-разному. Для человека (б) заголовок – это, название статьи, подзаголовок – автор, курсив – дата публикации, зеленым цветом на рисунке выделена страна, а красным цветом город, односложные ссылки – это тэги, и в конце рейтинг, который определил пользователь для данного места.

На рис. 1 (в) показан интерфейс запроса, где можно выбрать страну и город, куда вы хотите поехать, дату прибытия и желаемый уровень гостиницы. Если мы не используем средства СВ, то страна и город, выделенные на (в) также зеленым и красным цветом и страна и город на (б) – это никак не связанные слова. Однако в мире СВ мы имеем возможность связать эти понятия на различных страницах как на нашем сервере, так и на любых других серверах.

После выбора данных в интерфейсе для поиска путешествий (рис.1, в) – посредством предлагаемых списков стран, городов, даты и прочего, пользователь отправляет запрос на сервер. Сервер ТСС разумеется ничего не знает о расписании авиаперелетов и свободных гостиницах в указанном городе. Он ничего и не должен знать, потому что это не в его компетенции. Авиакомпании предоставляют информацию о полетах (г), сервис гостиниц (д) собирает информацию о гостиницах с сайтов гостиниц и предоставляет для использования. Благодаря тому, что на всех сайтах используется один формат (выделены одинаковыми цветами) представления одних и тех же данных (страна, город, дата, уровень гостиницы), проблем в понимании между различными ресурсами при передаче запроса от одного к другому не возникает.

[9] http://www.amazon.com/



а) б) в) г) д)

Рис.1. Расхождения в восприятии одного и того же веб-документа браузером (а) и человеком (б), интерфейс запроса (в), сервис авиаперелетов (г), сервис бронирования гостиниц (д)

Идентификация объектов в СВ будет осуществляться посредством Uniform Resource Identifier (URI)[10]. Поскольку RDF использует URI-идентификаторы для кодирования информации о сущностях в документе, эти самые URI-идентификаторы гарантируют то, что каждое понятие, используемое в документе – это не просто слово, а нечто, привязанное к единому определению, которое каждый желающий может найти в Сети.

Ниже показан фрагмент кода, в котором используется атрибут RDF-a `@property`, предназначенный специально для разметки существующего текста XHTML-страницы. А также указывается с помощью `xmlns:dc="http://owrus.org/tr/elements/1.1/`, где описаны сущности (*лексиконы*, или библиотеки сущностей). Благодаря этому такие сущности, как «Страна», «Город», «Дата» и прочие получают вполне определенный смысл.

```
<div xmlns:dc="http://purl.org/dc/elements/1.1/
                    xmlns:tr="http://owrus.org/tr/elements/1.1/">
      <h2 property="dc:title">Мое путешествие в Петербург</h2>
      <h3 property="dc:creator">Vitaly</h3>
      <h3 property="dc:country">Russia</h3>
      <h3 property="dc:city">Saint-Petersburg</h3>
      … <div>Текст страницы</div> …
      <div property="tr:rating">Рейтинг</div>
</div>
```

RDF является абстрактным машиночитаемым представлением данных, призванным максимизировать повторное использование словарей. RDF-a – это способ выражения RDF-данных в XHTML, в рамках которого данные, предназначенные для человека, используются повторно. Из триплетов языка RDF формируются сети информации о взаимосвязанных вещах. В примере показано применение понятий из разных словарей.

Аналогично добавляются метаданные и в поля формы, например списки:

```
<select xmlns:tr="http://owrus.org/tr/elements/1.1/" name=”country”
                            property=”tr:country”>
      <option property=”tr:country:ru”>Россия</option>
      <option property=”tr:country:ua”>Украина</option>
      <option property=”tr:country:by”>Белоруссия</option>
      <option property=”tr:country:kz”>Казахстан</option>
      …
</select>
```

Однако, если с представлением данных все более менее ясно, то что касается самой архитектуры СВ, то статей и исследований чрезвычайно мало. Изначально, еще в статье

[10] http://ru.wikipedia.org/wiki/URI

[1] Тим Бернерс Ли полагал, что подобно Интернету, СВ будет максимально децентрализован. Одни пользователи будут создавать словари, другие будут использовать их, однако взаимодействие между различными создателями словарей абсолютно никак не регламентируется. Одни и те же понятия могут существовать в разных словарях. А чтобы программы могли определять, что используемые в разных словарях понятия на самом деле одно и то же и предлагается использовать OWL. Однако в результате, мы все равно приходим к тому, что где-то должен быть свод всех понятий. И поскольку сейчас такой проблемы не возникает, потому что количество словарей не очень большое, то при наступлении эры СВ, безусловно такое количество словарей будет расти огромными темпами. В конце концов, различные компании захотят предлагать именно свои словари, как дополнительный повод обратить на себя внимание.

Введение архитектуры на основе сети лексикон-провайдеров может решить эту проблему в самом ее зачатке. В основе данной архитектуры лежит принцип централизованного управления и распределенного хранения словарей на серверах лексикон-провайдеров (далее ЛП) (рис. 2).

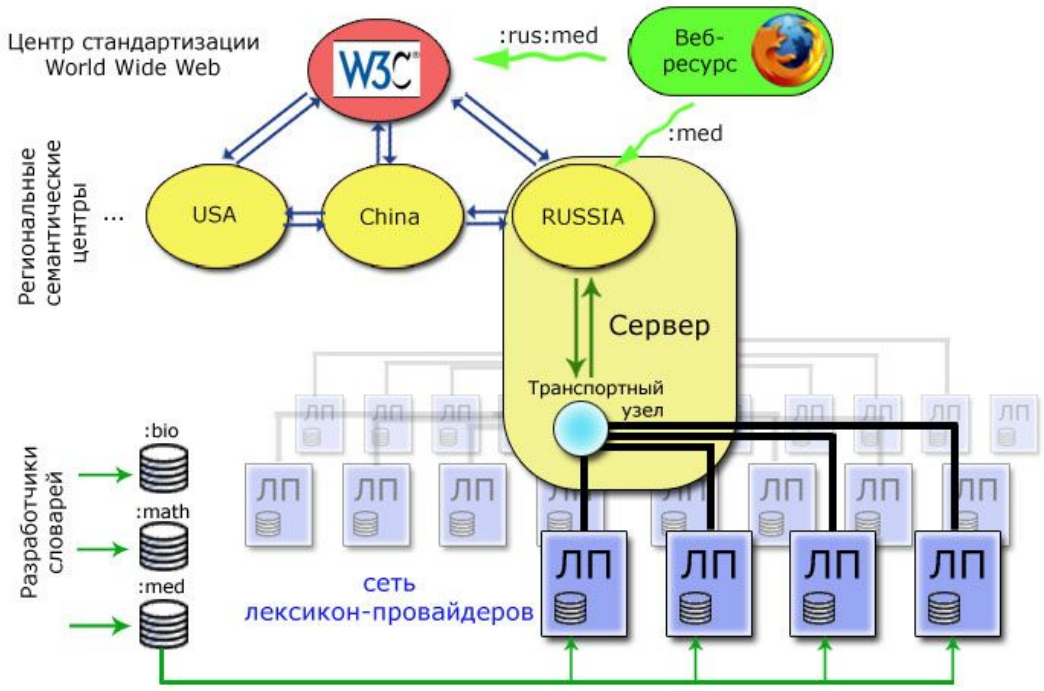


Рис. 2. Архитектура распределенной сети лексикон-провайдеров

За главный центр (ГЦ) принимается W3C, который авторизовывает региональные семантические центры (РСЦ). Семантические центры – это не просто сервера, но и в первую очередь организации, которые обеспечивают актуальность и полноту словарей, разделение компетенций между ЛП и разработчиками словарей. Обеспечивает безопасность и доступность данных в любой момент. Семантические центры в свою очередь делегируют разработку словарей сторонним организациям или сообществу, как это сделала Wikipedia. Однако здесь понадобится армия модераторов, которая будет следить за корректностью данных, потому что кроме сбора словарей сущностей, необходимо еще поддерживать словари логического вывода и связей между сущностями, что безусловно должны делать специалисты. После того, как разработчики, или инженеры по знаниям, создают словари, они передают их РСЦ, который утверждает и сертифицирует их. Сертифицированные словари могут храниться на серверах РСЦ, однако для пользователей сети они доступны только с серверов ЛП. Однако непосредственный доступ к ЛП веб-ресурсы не имеют.

Получение словарей осуществляется по следующей схеме. Веб-ресурс отправляет запрос либо ГЦ, либо в РСЦ на свое усмотрение. Запрос от ГЦ все равно будет перена-

правлен в РСЦ. В РСЦ имеются агенты, или транспортные узлы (ТУ), которые отвечают за доставку словарей. ТУ контролируют такие вопросы, как распределение нагрузки между серверами ЛП и получение словарей. Количество ЛП, отвечающих за одну и ту же библиотеку может доходить до десятков, или даже сотен, в зависимости от загруженности сети и потребностей. Из сотни доступных ЛП ТУ выбирает наименее загруженные и подключает механизм отправки данных по схеме обратно – ЛП – ТУ – РСЦ – веб-ресурс. Таким образом, решается проблема нагрузки и защищенности словарей. Выход из строя одного из ЛП не выводит из строя всю сеть. Разумеется, это не касается основных транспортных узлов, таких как ГЦ и РСЦ, однако в связи с масштабностью архитектуры данные сервера должны быть исключительно надежными. А надежность одного управляющего сервера и ненадежность и легкая заменимость серверов ЛП – это также один из принципов данной архитектуры.

В вопросах представления знаний исключительную важность получает возможность использования национальных языков. Использование английского языка ограничивается определенным набором имен тэгов и атрибутов и использование для этих целей одного языка – вполне логичное решение. Было бы странно, если бы в каждой стране одни и те же тэги структуры и оформления документа были бы представлены разными языками: латиница, кириллица, иероглифы и прочее. Однако, что касается знаний то представление знаний человеком может быть эффективно только, если он использует родной язык, а не чужеродный, пусть и общеупотребимый. Это будет также способствовать распространению и массовому внедрению OWL, стимулировать людей публиковать свои знания в структурированном виде, на родном языке. Данная архитектура позволяет легко взаимодействовать как между РСЦ, так и ГЦ перераспределять запросы между ними, если возникают вопросы в интернационализации словарей (возможности получать их партиями из нескольких языков).

Заключение

В статье представлен новый подход в создании архитектуры следующего поколения Интернета, а также показаны основные возможности внедрения семантики в веб-страницы, с помощью словарей, получаемые от лексикон-провайдеров. Новая архитектура строится на принципе централизованного управления и распределенного хранения словарей сущностей. Также была предложена возможность использования национальных языков, как основы для развития СВ и региональных семантических центров. Использование национальных языков в разметке – абсолютно новая концепция, которая открывает новые перспективы и горизонты в управлении коллективными знаниями.

Однако, в статье не были освещены такие важные вопросы, как обеспечение целостности словарей на серверах ЛП, обеспечение безопасности и достоверности данных. Вопрос национальных языков также требует более подробного описания, но в формате данной статьи его невозможно было раскрыть полностью.

Литература

1. T. Berners-Lee, J. Hendler, O. Lassila. The Semantic Web // Scientific American Magazine – May 2001 – http://www.sciam.com/article.cfm?id=the-semantic-web
2. T. O'Reilly, What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software – 2005 – http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html

УДК 004.054

ОРГАНИЗАЦИЯ ПРОЦЕССА СОЗДАНИЯ ВЕБ-ПРИЛОЖЕНИЙ, СВОБОДНЫХ ОТ ОШИБОК

Д.Г. Юдин
Научный руководитель – к.т.н., доцент Б.А. Крылов

В этой статье рассматривается комплекс организационно-технических мер, применяемых для организации процесса создания веб-приложений, устойчивых к появлению ошибок в коде. Также обращается внимание на ошибки в подходах к решению проблем с качеством программ.
Ключевые слова: контроль качества, тестирование, организация производства ПО

Введение

Целью разработки любой программы является рабочая программа. Рабочая, значит что программа выполняет возложенные на неё задачи и делает это без ошибок (идеальный случай). Если программа изготавливается одним единственным программистом, то о процессе разработки можно не задумываться, а вернее, этот программист сам для себя решит как ему удобней. Однако, в случае командной разработки возникают многочисленные проблемы, влияющие на качество готового продукта. В этом случае необходимо рационально организовать работу команды для получения наилучшего результата.

Кому и зачем нужен контроль качества

Контроль качества необходим, прежде всего, при разработке больших долгосрочных проектов, которые в будущем будут поддерживаться, и улучшаться разработчиками. В таких условиях поддержание качества является весьма важной задачей. Можно даже сузить необходимость поддержания качества к необходимости поддерживать продукт, либо несколько продуктов на базе центрального фреймворка.

Типичный случай последнего – разработка веб-приложений. Как правило компания-разработчик занимается одновременно несколькими проектами. А для облегчения труда используется один и тот же фреймворк, который используют все программисты компании. Фреймворк может быть взят из opensource, а может быть написан внутри компании. Естественно этот фреймворк не лишён недостатков, которые выявляются со временем. Как правило, эти недостатки выявляются при реализации какого-либо функционала очередного проекта. А так как проектов много, а времени мало, эта ошибка будет исправлена только в рабочем проекте и может возникнуть вновь на очередном проекте. Для того, чтобы этого не происходило, необходима регламентация процесса разработки.

Необходимые инструменты и технологии

Перечислим основные критерии, которые упрощают поддержание качества продукта:

1. Контроль версий.
2. Разделение рабочих копий.
3. Одинаковое окружение.
4. Одинаковые инструменты.
5. Обновляемая документация.
6. Автоматические тесты.

Контроль версий

Работа программиста – продолжительный процесс, в течение которого происходит поиск решения поставленной задачи. При этом зачастую перебираются различные варианты. Особенно это проявляется при работе в незнакомой области. Важно заметить, что, даже перейдя к следующему варианту решения, программист может не знать, был ли предыдущий лучше или хуже, поэтому есть необходимость сохранять промежуточные результаты работы. Хотя бы для того, чтобы иметь возможность откатиться к предыдущему коду.

Если же работа над задачей осуществляется несколькими программистами (особенно на удалённой основе), требуется некоторая информация о том, что же сделано остальными членами команды. Требуется некоторая документация в процессе разработки.

Системы контроля версий дают нам решение для всех перечисленных выше проблем. Это сохранение промежуточных результатов работы и документирование изменений. И даже больше. Возможно, проследить за списком изменений выбранного кусочка проекта. Кто, когда и какие правки делал.

Системы контроля версий подходят не только для хранения исходных кодов программ, но так же текстов, документов, бинарных файлов.

Использование системы контроля версий снижает количество потерь работоспособного кода, уменьшает стрессы программистов, а, следовательно, напрямую влияет на качество программного кода.

Идентичное окружение

Идентичное окружение означает, что все программисты запускают проект в одних и тех же условиях. Это требование должно выполняться для того, чтобы отдельные части проекта были совместимы между собой. Кроме того, такой подход позволяет отбросить влияние окружения на возникновение ошибок. Т.е. не будет ситуации «ничего не знаю, у меня всё работает».

Как такой критерий реализуется? В случае с веб-проектами всё достаточно просто. Выделяется отдельный сервер для разработки. Все члены команды работают на это сервере. Поскольку сервер один и тот же, для всех участников он работает единообразно. Иными словами мы добились идентичного окружения.

Разделение рабочих копий

Этот критерий тесно связан с критериями идентичности окружения и использования систем контроля версий.

Понятие рабочей копии введено системами контроля версий. Имеется репозиторий, содержащий последнюю версию проекта со всеми правками, которые были сделаны при создании это самой «последней версии». Программист работает с копией репозитория в какой-то момент времени. Эта копия и носит название рабочей копии.

Критерий идентичности окружения, возможно, заставит некоторых сделать одну копию проекта на сервере разработки, для работы команды. Однако, часто случается так, что несколько программистов начинают работать над одними и теми же файлами. Это не только может повлечь порчу результата деятельности одного из разработчиков, но и вызывает простои в работе, пока один работает, остальные ждут.

Существуют способы убить двух зайцев одним выстрелом, создать идентичное окружение и раздельные рабочие пространства для каждого из разработчиков. Проблема синхронизации результатов труда решается с помощью системы контроля версий.

Одинаковые инструменты

Одинаковые инструменты, значит, что все программисты имеют одинаковый набор программ, с помощью которых выполняют свою работу. Это текстовые редакторы или среды разработки, браузеры, файловые менеджеры, операционные системы. В таком случае взаимная помощь при общении будет наиболее эффективна. Этот критерий касается не только программистов, сидящих в одной комнате, как можно подумать. Ведь в процессе работы будут создаваться некоторые рецепты решения проблем и достаточно важно, чтобы эти рецепты были переносимы.

Обновляемая документация

Никто не любит писать документацию, мало кто любит её читать. Но есть моменты, когда без неё не обойтись никак и альтернативой служит только вычитывание всего исходного кода проекта для понимания как оно работает. Это, конечно, полезно, однако, занимает слишком много времени. Гораздо проще было бы ознакомиться с словесным описанием искомой функциональности.

На помощь приходят форматы автодокументирования. Суть заключается в следующем: в процессе написания кода программист оставляет в нём комментарии, оформленные особым образом, которые затем специальным парсером преобразуются в документацию по проекту.

Процесс создания документации отлично автоматизируется. Единственным условием является правильное ведение комментариев программистами, а документацию можно иметь практически произвольной актуальности (день, час, минута).

Автоматические тесты [1]

Если предыдущие критерии лишь косвенно способствовали улучшению качества за счёт удобства разработки, то тесты влияют на качество непосредственно. Протестированная функциональность – качественная (работающая) функциональность. Естественно настолько, насколько адекватны тесты и их количество.

С автоматическими тестами всё весьма сложно. Они требуют времени, желания, умений. Часто этого всего не хватает. Сроки, данные на реализацию проекта обычно не предусматривают процесс создания тестов. Программисты, написав программу, уже не хотят ничего тестировать – ведь и так уже всё работает. Написание тестов довольно скучное занятие для программиста, ведь их суть – быть простыми, чтобы было трудно допустить ошибку в коде теста. Однако, не все программы одинаково подвержены проверке автоматическими тестами. Некоторые программы довольно трудно протестировать, поэтому для написания тестирующего кода нужны специальные навыки, с помощью которых будет возможно определить правильную стратегию тестирования.

Очевидно, что только для двух проблем из перечисленных есть решения. Отсутствие умения разработки тестов ничем не возместишь, нечего и думать, надо приобретать умения. Время на написание тестов можно согласовать, а вот с программистами надо что-то делать.

В общем случае они вовсе не против написания тестов. Если программист сталкивался с доработкой программы, для которой написаны тесты, то он оценил то ощущение уверенности, которое ему дают тесты. После внесения изменений, он мог запустить процедуру тестирования и увидеть, что, по крайней мере, то, что было сделано ранее не сломалось после его вмешательства. Это весьма ценно, когда проект незнакомый, либо большой и окинуть мыслью его не получается. В этот момент у беспокоящегося за ре-

зультат своей работы человека появляется неуверенность в том, что его действия не сломали работу программы в другом месте.

На помощь приходит концепция Test Driven Development(TDD)[2] – разработка через тестирование. TDD – это метод разработки, ставящий написание юнит тестов на первое место. Суть его заключается в следующем:

1. Сначала пишется тест, который падает (обязательно). Если нет тестов, которые падают, код писать не надо.
2. Затем пишется код, который работает в этих тестах.
3. Чистим код от всего лишнего, оптимизируем, если требуется – рефакторинг. В процессе запускаем тесты и проверяем, что они по-прежнему работают.

Собственно, написание тестов затевается для третьего пункта. Когда нам надо что-то поменять, то, возможно, прошло уже много времени, и мы не помним каких-то особенностей работы программы. Запуск тестов «возвращает нам память».

Кроме облегчения рефакторинга есть и ещё одна положительная черта в написании тестов.

Так как тест пишется до программы, то программисту приходится заранее обдумывать архитектуру программы (на сегодняшний день очень большое количество людей пишут программы стихийно, не обдумывая их структуру, а решая сиюминутно возникающие проблемы), что позволяет зачастую улучшить качество кода, ещё до его написания.

Особенности тестирования веб-приложений

Последние несколько лет имеется тенденция реализовывать новые программы в виде веб-сайта (веб-приложения). Предпосылками этому были следующие вещи:

1. Совершенствование браузеров (особенно появление Internet Explorer 7);
2. Широкое распространение технологий, позволяющих писать веб-приложение.
3. Стабилизация взглядов на разработку веб-приложений.

Причины же создания таких приложений (они же преимущества веб-приложений перед традиционными программами):

1. Простота обновления.
2. Простота поддержки.
3. Простота распространения (распространения нет, или есть, но в другом смысле);
4. Простота внедрения.
5. Лёгкость управления подписчиками.

Особенность веб-приложений заключается в том, что при его создании используется сразу несколько языков программирования. Кроме того сред выполнения веб-приложения ещё больше.

Рассмотрим по отдельности

Языки, для написания веб-приложений.

Языки можно разделить изначально на две категории по местоположению среды выполнения: серверные и клиентские.

К серверным языкам относятся PHP, Python, Perl, C, Ruby и прочие.

К клиентским JavaScript, HTML.

Соответственно, и тестировать нам надо как клиентские так и серверные модули приложения. Притом надо иметь ввиду, что клиентская часть напрямую зависит от серверной, т.к. генерируется на сервере, но протестировать её как часть тестов серверной части никак не получится.

Как правило, серверный код можно условно разделить на две части: код, который

что-то делает, и код, который занимается выводом. Так вот код, который занимается выводом протестировать не получится (вернее это неоправданно сложная и затратная по времени операция), т.к. вывод может меняться в довольно больших пределах, при этом выдавая один и тот же результат на клиентской стороне. Однако не стоит переживать на этот счёт, функции вывода будут протестированы опосредованно через тесты клиентской части.

Под кодом, который «что-то делает», подразумеваются части программы, которые производят какие-либо вычисления или работают с данными. Это достаточно формальные процессы, результат которых очень просто «предсказать» (т.е. высчитать из имеющихся исходных данных), поэтому на первый взгляд тесты здесь получатся весьма простыми. Однако, здесь необходимо затронуть ещё одну сущность, входящую в состав веб приложения – базу данных.

Операции с данными, это такие операции, которые создают новые данные, удаляют существующие данные, изменяют данные, переводят данные из одного состояния в другое. Легко представить себе такую функцию, которая при каждом запуске будет давать разный результат, т.к. в процессе своей работы изменяет содержимое базы данных, которое в свою очередь используется как входные параметры для работы функции. Таким образом появляется необходимость задавать начальные состояния различных объектов(расширяя пример с базой данных) до начала тестирования.

Среды выполнения веб-приложения

Для отдельно взятого веб-приложения имеется серверная часть, которая выполняется на сервере в одном и том же окружении и клиентская часть. Клиентская часть выполняется в браузерах. Браузеров много, и, несмотря на существующие стандарты интерпретации HTML разметки и JavaScript кода, результат работы может оказаться весьма различающимся. Поэтому важно тестировать работу веб-приложения в различных браузерах. Тестирование сводится не только к проверке работы JavaScript-модулей, но и к проверке работы HTML-элементов управления.

HTML (+CSS) дают нам внешний вид интерфейса, который протестировать автоматическим способом невозможно (слишком затратно). Да и, как правило, в этом нет необходимости. Но тестирование HTML имеет смысл – с помощью проверки наличия каких-либо тегов или конструкций можно судить о работоспособности серверного кода, отвечающего за вывод. Почему так? Потому что для пользователя веб-приложение – это интерфейс в браузере. Пользователь взаимодействует с приложением полностью через этот интерфейс. Тестируя правильность работы интерфейса, мы тестируем правильность работы кода на сервере, который этот интерфейс формируют. Интерфейс содержит 95% всех входных данных для работы веб-приложения.

К сожалению тест для интерфейса может быть создан только после того как интерфейс разработан, что довольно снижает мотивацию для написания теста.

Негативные аспекты тестирования

1. Если в команде нет человека, который занимается тестированием, то тесты приходится писать программистам, что они часто не любят делать.
2. При незначительном изменении кусочка программы, может оказаться, что этот кусочек участвует в большом количестве тестов, которые так же придётся переписать. При значительных изменениях в коде, возможно придётся переписать большинство тестов.
3. На создание тестов необходимо время.

Заключение

Для обеспечения создания веб-приложения, свободного от ошибок, необходимо выполнить ряд условий. Таких как одинаковые во всей команде инструменты разработки, одинаковая среда выполнения кода, контроль версий, оперативное создание и поддержание документации, автоматическое тестирование.

Как мы видим для выполнения всех этих критериев существует специальное программное обеспечение. Но тестирование вызывает наибольшее количество проблем.

Для написания тестов необходим человек хорошо знакомый не только с подходами и инструментами тестирования, но и хорошо разбирающийся в программном коде проекта. Такого человек весьма сложно найти, а программисты негативно относятся к написанию тестов для «уже работающего кода».

Литература

1. Элфрид Дастин, Джефф Рэшка, Джон Пол Автоматизированное тестирование программного обеспечения, ISBN 5-85582-186-2 - Лори, 2003. – 592 с.
2. Роберт Калбертсон(Robert Culbertson), Крис Браун(Chris Brown), Гэри Кобб(Gary Cobb) Rapid Testing First Edition, ISBN 5-8459-0336-X, 0-1309-1294-8 – Вильямс, 2002. – 384 с.

УДК 004056

КОНТРОЛЬ И УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ ПОТОКАМИ КРУПНЫХ ПРЕДПРИЯТИЙ

Т.С. Николаева
Научный руководитель – к.т.н., доцент Н.С. Кармановский

В данной статье рассматривается интегрированная система управления информационными потоками предприятия, позволяющая повысить эффективность контроля и управления информационными потоками предприятия.

Ключевые слова: информационные потоки, контроль, управление

Введение

Бурное развитие современных информационных технологий вынуждает предприятия и организации разных масштабов и сфер деятельности внедряться в мир распределенных компьютерных систем. При этом возникает множество вопросов, связанных с использованием огромного числа разнородных приложений, программных средств, аппаратных платформ и сетевых протоколов представленных на потребительском рынке товаров и услуг. В таких условиях применение информационных технологий связано с использованием многочисленных разнородных и территориально распределенных вычислительных ресурсов, которыми необходимо эффективно управлять [1].

Из-за применения различных подходов к управлению, каждый из которых использует свои собственные методы работы с определенным подмножеством ресурсов всего предприятия, на нем возникает неразбериха. В таком состоянии, организации испытывают острую потребность в интегрированном решении, которое помогло бы им совладать со сложной, хаотичной средой и извлечь максимум пользы из своей инфраструктуры.

Информационные потоки предприятия можно разделить на две категории: собственные и внешние. К собственным относится информация, зарождающаяся внутри предприятия. К такой информации можно отнести бухгалтерские документы, приказы и распоряжения, данные внутреннего документооборота и т.д. Собственные потоки формируется за счет внутренних источников информации, которые легко можно проверить на полноту и достоверность сведений.

В случае с внешними потоками такой возможности нет. Количество разновидностей внешней информации и ее источников весьма значительно. Это и всевозможные нормативные документы федерального уровня, нормативные акты отраслевого, регионального и местного уровней, комментарии к ним, реклама, информация партнеров и конкурентов, результаты маркетинговых исследований и т.д. все это добывается из средств массовой информации, информационных источников удаленного доступа, результатов заказных исследований достоверность которых может быть часто противоречивой. Из разных источников информация поступает в различном виде (на бумаге, устно, по электронной почте, в виде графиков и таблиц, Интернет-файлов и т.д.). Достаточно сложно организовать унификацию такой информации для дальнейшего ее хранения и обработки по единой технологии.

Формирование и поддержание в хорошем состоянии информационного поля предприятия – весьма непростая задача. Тем не менее, решать ее приходится, так как цена серьезной управленческой ошибки достаточно высока.

Для обеспечения высокой надежности над контролем и управлением информационными потоками в организации требуется внедрить интегрированную систему управления (ИСУ). Создание новой интегрированной системы в отличие от большинства су-

ществующих на сегодняшний день позволит ориентироваться на решение стратегических задач предприятий [2]. Рассмотрим особенности ИУС (рисунок).

Рисунок. Интегрированная система управления

Как видно из рисунка интегрированная система обеспечивает эффективную деятельность предприятия в целом: единая система управления организацией, автоматизированные системы управления технологическими процессами, сетевые и телекоммуникационные комплексы, системы передачи телеметрической информации, системы жизнеобеспечения, Internet и Intranet-решения.

Интегрированная система строится как единый комплекс программно-технических и организационных решений, охватывающих все производственные, технологические, финансовые и хозяйственные процессы и объединяя все подразделения предприятия в единое информационное пространство.

Круг конкретных целей, решаемых в результате создания системы, включает множество различных задач.

− объединение в единое информационное пространство большого числа территориально удаленных друг от друга объектов и подразделений предприятия;

− высокоскоростную передачу по каналам связи любых видов информационных потоков;

− поддержку деятельности всех подразделений и объектов предприятия;

− автоматизацию всех технологических и бизнес-процессов организации, оперативный контроль и управление процессами производства, транспортировки и сбыта, взаиморасчетов с потребителями и поставщиками, управление персоналом и т.д.;

− мощные средства обработки и анализа получаемой информации, расчет плановой и фактической себестоимости продукции.

Главным итогом внедрения системы должно явиться создание на предприятии эффективного и действенного механизма управления, охватывающего все процессы, циркулирующие на предприятии. В результате этого организация выйдет на качественно новый уровень управления и планирования своей деятельности.

Заключение

Таким образом, внедрение интегрированной системы в информационную структуру предприятий позволит централизовано отслеживать состояние системы, контролировать восстановление отдельных элементов при отказе, оперативно принимать решения и повысить уровень безопасности. В целом использование данного продукта приведет к повышению надежности контроля и управления информационными потоками предприятий, а также поможет снизить трудоемкости по эксплуатации системы.

Литература

1. [Электронный ресурс] – http://www.ict.edu.ru, свободный.
2. [Электронный ресурс] – http://www.smartcat.ru, свободный.

УДК 004.654

РАССМОТРЕНИЕ НЕКОТОРЫХ ВОПРОСОВ СОВМЕСТИМОСТИ СОВРЕМЕННЫХ САПР НА УРОВНЕ ФАЙЛОВЫХ ФОРМАТОВ

В.Н. Зимин, П.В. Федосов
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

В статье приводятся краткие сведения о форматах хранения данных САПР. Рассматривается история их развития. А так же описываются особенности совместимости различных реализаций форматов хранения данных от различных производителей САПР. Статья будет полезна тем, кто хочет подробнее узнать о форматах хранения денных САПР и их совместимости

Ключевые слова: САПР, хранение данных, форматы файлов

Введение

В современном мире почти каждый реализуемый проект, от постройки дома, до разработки нового микропроцессора требует больших затрат времени, что отчасти компенсируется использованием различных САПР. Однако одной из немаловажных проблем в данном случае является необходимость передавать полученные данные между несколькими средами разработки. Что подчас является не тривиальной задачей в силу поддержки рядом производителей САПР только своих собственных закрытых форматов хранения данных.

Сейчас, с силу глобализации и мысового появления на рынке свободно распространяемого программного обеспечения, все больше производителей включают в состав своих продуктов функции импорта и экспорта в открытые форматы или же раскрывают спецификации своих проприетарных форматов.

Краткая классификация современных САПР

В последнее время во всем мире компьютеризация охватила практически все области человеческой деятельности. Становится все больше и больше людей, ежедневно использующих компьютеры для решения сложных производственных задач и автоматизации трудоемких технологических процессов. Общепризнано, что одним из наиболее перспективных направлений применения вычислительной техники является внедрение систем автоматизированного проектирования САПР для разработки новых конструкция и изделий. САПР нужно рассматривать как неразрывную связку «пользователи – технические средства – программное обеспечение проектирования». Руководствуясь этим принципом, произведем обзор существующих систем автоматизированного проектирования [1, 2].

По назначению системы САПР делят на:

- Машиностроительные – разработка широчайшего спектра изделий: от создания аэрокосмических систем до проектирования кофеварок и кухонных комбайнов.
- Изделия микроэлектроники – проектирование принципиальных и монтажных схем, печатных плат, автоматическое размещение элементов изделий, автотрассировка.
- Электротехнические – разработка принципиальных схем и схем подключения электротехнического оборудования, его пространственная компоновка, ведение баз данных готовых изделий.
- Архитектурные – трехмерное проектирование архитектурно-строительных конструкций, расчет специальных конструкций типа крыш, типовые

статические расчеты строительных конструкций, ведение баз данных стандартных элементов, планирование территорий под строительство.

- Оборудование промышленных установок и сооружений – создание принципиальных схем установок, пространственная разводка трубопроводов и кабельных трасс, проектирование систем отопления, водоснабжения, канализации, электроснабжения, вентиляции и кондиционирования, ведение баз данных оборудования, трубопроводной арматуры, готовых электротехнических изделий.
- Геоинформационные – оцифровка данных полевой съемки, анализ геодезических сетей, построение цифровой модели рельефа, создание в векторной форме карт и планов, ведение земельного и городского кадастров, ведение электронного картографического архива.

На российском рынке широкое распространение получили практически все продукты компании AutoDesck, SolidWorks и многих других компаний.

Хотя приведенная выше классификация не претендует на полный охват всех возможных видов САПР, она дает представления насколько широко они сегодня применяются. Что неизбежно приводит нас к вопросу взаимодействия подобных систем друг с другом.

Исторический обзор вопросов совместимости

Вопросы переносимости электронных документов (файлов чертежей) из одной системы проектирования в другую исторически возникли практически одновременно с появлением самих этих систем. Это было связано не только с наличием на рынке программного обеспечения систем с близкими возможностями от различных производителей, но и с существованием инженерных задач, решение которых требовало использования сразу нескольких САПР, т.к. каждая из них в силу относительной специализированности не обеспечивала всей необходимой функциональности.

Например, если необходимо создать электронное устройство, состоящее из одной или нескольких печатных плат, корпуса, жгутов кабелей и других компонентов, то для разработки электрической схемы, компоновки и трассировки печатных плат необходима специализированная САПР, которая, очевидно, не предназначена для проектирования корпуса. Если рассматривать еще более сложный объект проектирования, например, автомобиль, то необходимость использования нескольких систем возникнет еще более остро [1].

Однако, само по себе простое использование совершенно различных узко специализированных САПР еще не исчерпывает проблемы. Возвращаясь к примеру с электронным устройством: плата должна правильно устанавливаться в корпус, т.е. два различных компонента должны быть строго согласованы между собой. Отсюда логически вытекала необходимость переноса электронного документа из одной САПР в другую. Очевидно, внутренние форматы хранения данных для этой цели не подходили: большинство из них закрыты и, кроме того, предназначено именно для хранения данных в рамках одной системы, а не для их переноса.

Распространенные графические растровые и векторные форматы подходили для этих целей еще меньше: первые уже в силу своей растровой природы (в то время как чертеж по своей сути является векторным), а вторые из-за своей неспециализированности, т.е. отсутствия в них поддержки многих необходимых возможностей. В этой ситуации вполне логичным выглядит появления открытого формата DXF (Drawing Exchange Format).

Его представила фирма Autodesk как один из форматов, поддерживаемых системой AutoCAD. Формат DXF в своей основе текстовый, что позволяло просматривать

такие файлы в любом текстовом редакторе, а так же относительно легко создавать программные продукты, работающие с ним. Пример такого файла на рисунке.

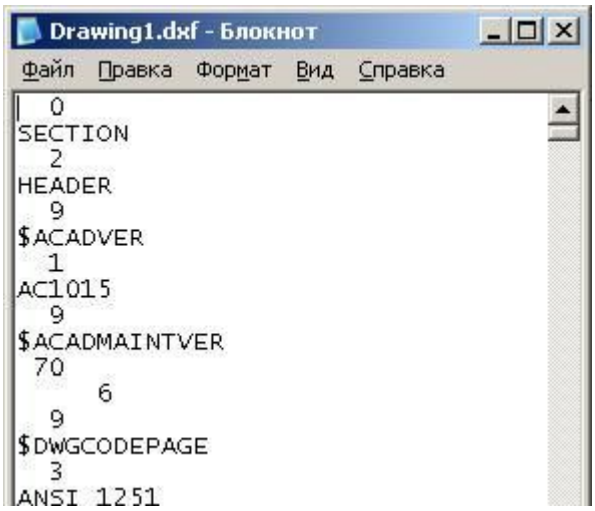


Рисунок. Пример содержимого DXF файла

Отрицательной стороной такого подхода были большой размер файлов и проблемы с производительностью. Это проблемы в середине 80-х годов прошлого века стояли особенно остро, учитывая объемы памяти и вычислительную мощность тогдашних компьютеров. Поэтому, основным файловым форматом САПР AutoCAD был и остается закрытый двоичный формат DWG. Кроме того, с 1988 года поддерживается двоичная версия DXF – DXB, который и был призван частично решить эти проблемы. Однако, этот формат не получил столь широкого распространения, как DXF, т.к. рост производительности компьютеров частично нивелировал недостатки текстового DXF [3, 4].

Таким образом, де-факто стандартным форматом межсистемного обмена стал открытый файловый формат DXF фирмы Autodesk, обеспечивавший, несмотря на присущие недостатки достаточный для большинства применений уровень совместимости.

Современное состояние

Специализированность формата DXF для решения задач, связанных с системами автоматизированного проектирования, и, при этом его достаточная универсальность вместе с открытостью и относительной простотой сделали его на данный момент основным форматом межсистемного обмена. На данный момент практически все современные САПР поддерживают экспорт и импорт в данный формат.

Однако, к сожалению, в области совместимости различных САПР по-прежнему существуют проблемы. Связаны они, в первую очередь с самим форматом DXF.

Формат DXF является, не смотря на свою открытость, разработкой фирмы Autodesk и нацелен, в первую очередь на основной продукт этой фирмы – AutoCAD. Эта САПР постоянно эволюционирует, что заставляет фирму Autodesk изменять спецификацию DXF практически с каждой новой версией AutoCAD. Что приводит к несовместимости версий формата. Т.е. сторонний программный продукт, работающий с одной версией DXF, может иметь проблемы при попытке чтения более новой версии. С одной стороны, стремление Autodesk совершенствовать свои форматы данных вполне логично, и вытекающая отсюда несовместимость версий закономерна. Но с другой стороны, возникает достаточно парадоксальная ситуация – формат, предназначенный для решения вопросов совместимости, сам имеет проблемы с совместимостью!

Однако, только описанным выше проблемы с DXF не ограничиваются. По мере усложнения AutoCAD, фирма-разработчик не полностью отражает внесенные изменения в спецификации DXF. Что постепенно снижает ценность DXF. Это заставило других фирм-разработчиков различных САПР искать альтернативу формату DXF.

Этой альтернативой стал формат DWG – двоичный файловый формат AutoCAD. DWG так же является разработкой Autodesk, но это закрытый формат, спецификации которого она никогда не открывала. Для разработки библиотек, которые позволили бы сторонним программным продуктам работать с форматом DWG, был создан консорциум ODA (Open Design Alliance) [5].

Консорциумом была произведена обратная разработка формата DWG и разработаны соответствующие программные библиотеки, разработаны спецификации OpenDWG, доступ к которым открыт всем желающим. ODA осуществляет поддержку OpenDWG в актуальном состоянии. Финансирование разработки программных библиотек производится на членские взносы участников консорциума. В Open Design Alliance состоит 32 участника-учредителя (Founding Members) и свыше 600 коммерческих (Commercial Members) и поддерживающих участников (Sustaining Members) (данные на начало 2008 года). В число поддерживающих участников (Sustaining Members) входят, например, ведущие российские производители САПР, такие как: АСКОН (Компас (САПР)), Топ Системы (T-FLEX CAD) и другие.

Таким образом, на данный момент времени подавляющее большинство различных САПР поддерживают форматы межсистемного обмена DXF или DWG. Это, несмотря на существующие ограничения, позволяет использовать разнонаправленные САПР в рамках одного проекта, а так же относительно безболезненно переходить с САПР одной фирмы на другую.

Заключение

В статье рассматривалась история развития форматов хранения данные САПР, современное положение дел. Глобализация процессов в современном мире, отразилась и на САПР. Редко когда при разработке продукта используется только один вид САПР. Обеспечение полноценного взаимодействия между ними и, в идеале, полной совместимости форматов файлов данных становится насущной необходимостью. Сейчас все еще возникают сложности с закрытыми форматами, однако поддержка экспорта в открытие форматы типа XML, уже сейчас во многом нивелирует этот недостаток.

Литература

1. Автоматизация инженерно-графических работ / Г. Красильникова, В. Самсонов, С. Тарелкин – СПб: Питер, 2001. – 256 с.: ил.
2. Латышев П. Н. Каталог САПР. Программы и производители. 2008-2009. – М.: Солон-Пресс, 2008. – 704 с.
3. DXF [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://ru.wikipedia.org/wiki/DXF, свободный. – Загл. с экрана. – Яз. рус., англ.
4. Создание AutoCAD [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://www.compkursy.ru/grafica/autocad_history.htm, свободный. – Загл. с экрана. – Яз. рус., англ.
5. Open Design Alliance [Электронный ресурс]. – Электрон. дан. – Режим доступа: http://ru.wikipedia.org/wiki/Open_Design_Alliance, свободный. – Загл. с экрана. – Яз. рус., англ.

УДК 004.91

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ПРОЕКТА JASPERREPORTS ДЛЯ ПОСТРОЕНИЯ ПОДСИСТЕМЫ СОЗДАНИЯ БИЛЕТОВ

В.А. Козак, Д.А. Шилкин
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

В статье отражены решения задач, возникающих при автоматической генерации документов, в данном случае театральных билетов, в системе JasperReports. Суть задачь сводится к автоматическому анализу существующих моделей данного документа, конвертированию моделей в другой вид, добавлению к моделям дополнительных аттрибутов, замене значений аттрибутов и подобным операциям.
Ключевые слова: JasperReports, модели, автоматизация, документы

Введение

Очень часто возникает задача создать множество однотипных документов, например, приказов или счетов. В таких случаях имеет смысл использовать некоторую автоматизирующую систему, способную создавать такой документ по шаблону, используя некоторые данные, уникальные для конкретного экземпляра документа. При этом данная система должна иметь графические средства для создания шаблонов, уметь работать с разными источниками данных и уметь экспортировать полученный документ в требуемый формат. Наиболее «продвинутые» подобные системы позволяют в качестве источника данных использовать различные базы данных и способны автоматически формировать на итоговом документе таблицы, графики, диаграммы и другие сложные объекты. Класс подобных систем принято называть генераторы отчётов. В данной статье отражены итоги исследования возможностей системы JasperReports для формирования кассовых билетов, продаваемых в театральных кассах Санкт-Петербурга. Выбор JasperReports обусловлен высокой производительностью и разнообразными возможностями системы, распространением её, в том числе, и по лицензии LGPL. Библиотека JasperReports легко интегрируется в существующую билетную систему. В задаче формирования билетов можно выделить следующие аспекты: создание новых шаблонов; создание механизма автоматического конвертирования существующих шаблонов другого формата в формат, требуемый JasperReports; создание механизма, предоставляющего необходимые данные для наполнения шаблона и формирования билета; экспорт получено билета в формат, который требует специализированный билетный принтер. Большинство из этих аспектов уникально для данной задачи и не имеют готового решения.

Создание шаблона билета

Как уже отмечалось, чтобы сгенерировать документ с помощью JasperReports, необходим шаблон – xml файл с разметкой будущего документа. По сути, этот файл является моделью представления, определяющей, как будет выглядеть документ. А также нужна Java программа, которая с помощью библиотек Jasper сгенерирует документ по указанному шаблону. Шаблон можно создать в любом текстовом редакторе, благо его формат совсем несложен. Ниже пример шаблона простого документа, содержащего слово «Тест». Обратите внимание на строку pdfFontName="c:\tahoma.ttf". По непонятной причине, если не указать явно путь к файлу шрифта, то PDF генерируется некорректно: русские буквы накладываются друг на друга.

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE jasperReport
```

```
 PUBLIC "-//JasperReports//DTD Report Design//EN"
 "http://jasperreports.sourceforge.net/dtds/jasperreport.dtd">
<jasperReport name="simple">
   <style
      name="Normal"
      isDefault="true"
      pdfFontName="c:\tahoma.ttf"
      pdfEncoding="Cp1251"
    />
   <detail>
      <band height="20">
         <staticText>
            <reportElement x="180" y="0" width="200" height="20" />
            <text><![CDATA[Тест !!]]></text>
         </staticText>
      </band>
   </detail>
</jasperReport>
```

Чаще для создания шаблонов используют не текстовый редактор, а графические средства. В случае с JasperReports можно использовать приложение iReport, внешний вид которого показан на рис. 1. Именно с помощью этого средства предлагается создавать шаблоны будущих билетов.

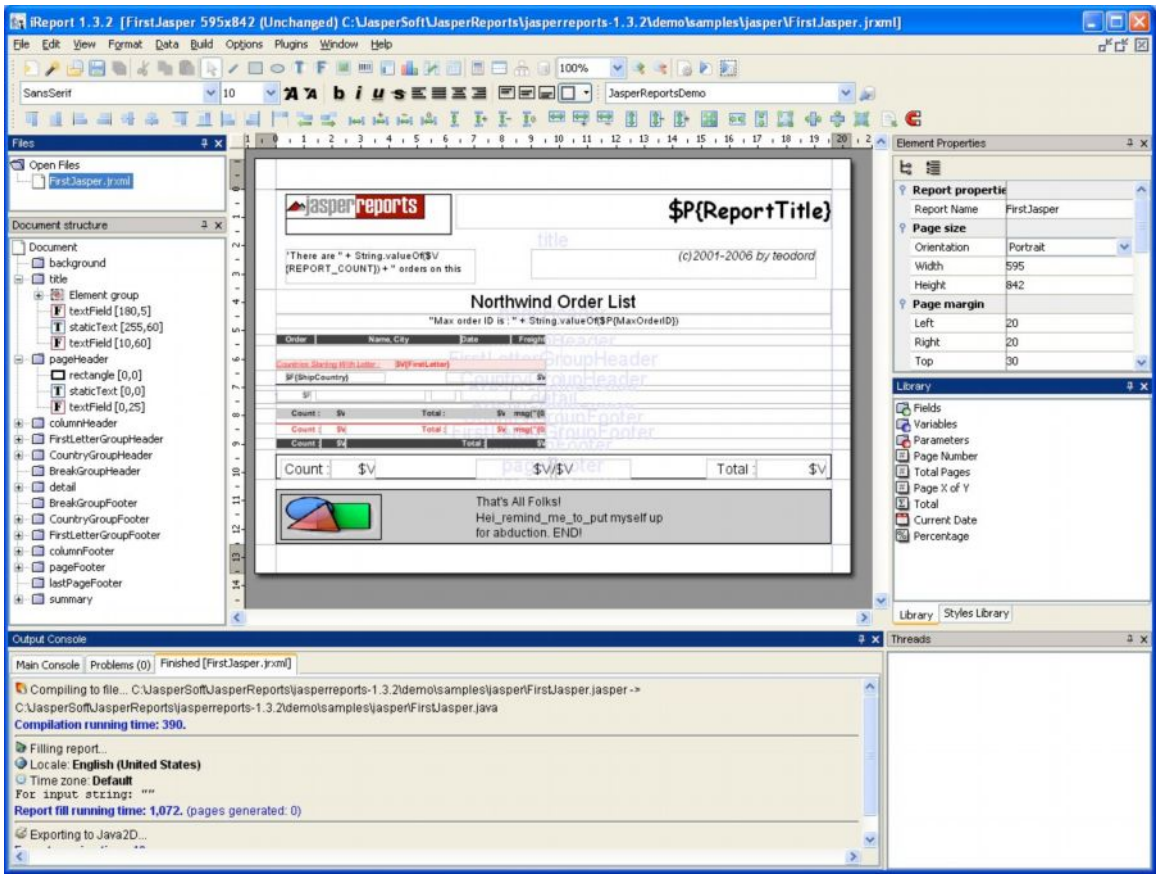


Рис. 1. Внешний вид программы iReport

Java код для генерации документа выглядит намного проще:

```
JasperReport jasperReport = JasperCompileManager.compileReport("reports/hello.xml");
JasperPrint jasperPrint = JasperFillManager.fillReport(jasperReport,
          new HashMap(), new JREmptyDataSource());
```

```
JasperExportManager.exportReportToPdfFile(jasperPrint, "reports/hello_report.pdf");
```

В этом коде вначале происходит компиляция шаблона и получение объекта JasperReport. Компиляция необходима, так как шаблон может содержать вставки Java кода. Далее производится наполнение из пустых источников данных и экспорт документа в формат PDF.

Конвертирование шаблонов билета

Проблема конвертирования существующих шаблонов в шаблоны JasperReports была решена с помощью XSLT (XSL Transformation). Эта технология, созданная W3C XSL Working Group, предоставляет способ для автоматического преобразования XML документов в другие XML документы или другие форматы. Чтобы выполнить преобразование, как правило, нужно создать таблицу стилей, написанную на XSL (XML Stylesheet Language – язык таблиц стилей). Таблицы стилей XSL определяют способ отображения XML данных. Помимо XSLT в данной задаче понадобится JAXP (The JavaTM API for XML Processing – технология позволяющая Java обрабатывать XML документы). JAXP поддерживает XSLT с помощью пакета javax.xml.transform [1]. Таким образом, задача конвертирования сводится к задаче создания таблицы стилей XSL и написанию простого Java класса, который вызовет нужные функции в JAXP и выполнит преобразование. В этом классе, чтобы выполнить преобразование, нужно получить XSLT конвертор и применить с его помощью таблицы стилей к XML данным. Данный код получает конвертор, для чего сначала инициализирует объект TransformerFactory, затем считывает таблицу стилей и XML файл существующего шаблона, затем создает файл для записи XML файла шаблона JasperReports и в итоге получает объект transformer класса Transformer из объекта tFactory типа TransformerFactory. Преобразование заканчивается вызовом метода transform, который помещает преобразованные данные в выходной поток (output stream).

```
TransformerFactory tFactory = TransformerFactory.newInstance() ;
String stylesheet = "templateTransformer.xsl";
String sourceId = "oldTemplate.xml";
File pricesHTML = new File("newTemplate.xml");
FileOutputStream os = new FileOutputStream(pricesHTM);
Transformer transformer = tFactory.newTransformer(new StreamSource(stylesheet));
transformer.transform(new StreamSource(sourceId), new StreamResult(os));
```

Наполнения шаблона, создание билета в памяти ЭВМ

Следующим этапом на пути создания билета является процесс наполнения шаблона данными, относящимися к конктетному билету. В шаблонах JasperReports для динамической подстановки данных можно использовать переменные (Variables), поля (Fields) и параметры (Parameters).

Переменные – это специальные объекты, которые могут работать с выражениями. В этих выражениях переменные могут ссылаться на другие переменные, поля и параметры, производить математические и другие операции. Посути, выражение это Java-код, который будет скомпилирован библиотекой JasperReports и исполнен во время наполнения шаблона, когда потребуется переменная с этим выражением.

Поля – специальные объекты, значение которых автоматически загружается из источника данных. Источник данных представляет собой Java класс, реализующий интерфейс JRDataSource, внешне очень похожий на java.sql.ResultSet.

Параметры – специальные объекты, значение которых автоматически загружается из коллекции параметров, передаваемой JasperReports во время наполнения шаблона [2].

Итак, В JasperReports для наполнения шаблона пользуются следующим методом:

```
JasperFillManager.fillReport(JasperReport  jR, Map params, JRDataSource dataSource).
```

В качестве параметров в метод передаются скомпилированный шаблон, мап (коллекция объектов ключ-значение) параметров и источник данных для полей. Проблема в том, что данный интерфейс разрабатывался для создания отчётов, а для задачи создания билета такой интерфейс неудобен. Логично предположить, что данные для создания билета будут содержаться в некотором Java объекте, который создаст внешняя билетная система. Таким образом, возникает задача конвертирования модели данных, выраженной некоторым, заранее неизвестным Java объектом в модель данных, требуемой JasperReports. Данная задача была решена с помощью Java Reflection. Reflection – это механизм, позволяющий динамически загружать и создавать экземпляры класса, а также осуществлять доступ к полям и методам класса. Для выполнения этих операций через reflection используется объект, имеющий тип Class. Этот объект содержит полную информацию, описывающую структуру класса – конструкторы, методы, поля и т.д. Объект типа Class создается автоматически Java-машиной для каждого класса, загруженного загрузчиком классов [3]. В рамках нашей задачи у полученного объекта рекурсивно проверяются все поля и методы, начинающиеся с «get». Из полученных данных строится источник данных, требуемый JasperReports. Далее этот источник передавался системе для создания объекта JasperPrint, то есть для формирования документа в оперативной памяти.

Печать билета

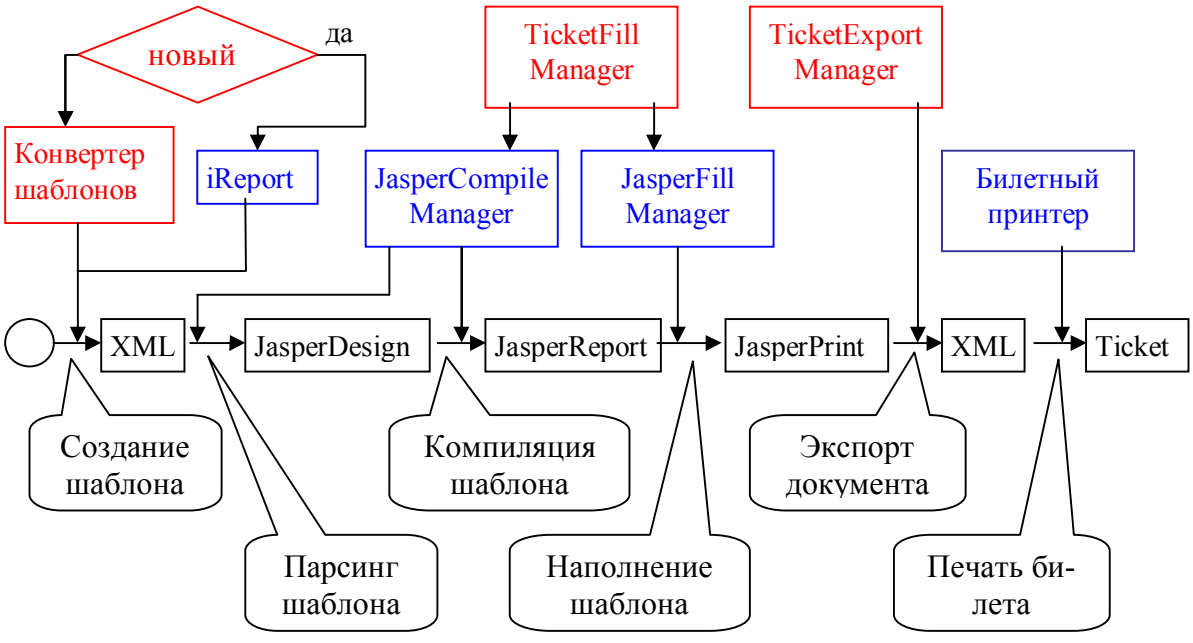


Рис. 2. Жизненный цикл модели билета с точки зрения подсистемы печати

Объект JasperPrint можно просмотреть и распечатать с помощью JasperPrintManager-а или же экспортировать докумет некоторый из поддерживаемых форматов. На сегодняшний день JasperReports поддерживает экспорт в PDF, XML, HTML, CSV, XLS,

RTF, TXT, и Flash [3]. Вот только имеющийся драйвер используемого билетного принтера данные форматы не поддерживает. Таким образом, мы сталкиваемся либо с задачей очередного конвертирования, либо реализуем свой вариант экспорта объекта JasperPrint в требуемый формат.

Реализованы были оба пути, но первый из-за неприемлеммых временных затрат использовать не представляется возможным. Дело в том, что по требованиям от нажатия кнопки печать до начала работы принтера должно пройти не более 0.5 секунды. А за это время необходимо загрузить шаблон, наполнить его, то есть создать JasperPrint, экспортировать в формат принтера, и ещё перед печатью некоторое время потребуется драйверу принтера.

Итоговый жизненный цикл модели билета перед его созданием с точки зрения подсистемы печати показан на рис. 2.

Заключение

В данной работе отражены нюансы, возникшие при создании кассовых билетов с помощью системы JasperReports. Описано как предполагается создавать шаблоны для новых билетов и автоматически конвертировать существующие шаблоны другого формата. Рассмотрено создание механизма, предоставляющего необходимые данные для наполнения шаблона и формирования билета; экспорт получено билета в формат, который требует специализированный билетный принтер.

Литература

1. Heffelfinger D.R. JasperReports for Java Developers – BIRMINGHAM-MUMBAI: Packt Publishing, 2006. – 339 с.
2. Кэй М. XSLT. Справочник программиста – М.: Символ-Плюс, 2002. – 1016 с.
3. Хорстманн К.С., Корнелл Г. Java 2. Библиотека профессионала. Том 2. Тонкости программирования – М.-СПб.-К.: Вильямс, 2007. – 1168 с.
4. Anglin S. The Definitive Guide to JasperReports™ – Berkeley: Apress, 2007. – 236 с.

УДК 378.37

СИСТЕМА ОРГАНИЗАЦИИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ И ИННОВАЦИОННОЙ ДЕЯТЕЛЬНОСТИ МОЛОДЕЖИ

А.Р. Орлов
Научный руководитель – к.т.н., доцент Р.Р. Магдиев

В данной работе рассматривается пример модели организации научно-технической и инновационной деятельности молодежи на уровне города и вуза с применением социальных сетей, создание необходимых условий развития подобной деятельности. Целью работы является отражение практического опыта в создании таких структур в Санкт-Петербурге, систематизация полученных данных в ходе этого процесса и формирование предложений для административных структур.
Ключевые слова: молодежная наука, инновации, социальные сети, сообщество, СНО

Введение

Данная работа является отражением проводимой с осени 2007 года молодежным коллективом работы по созданию системы нацеленной на развитие научно-технического творчества молодежи, коммерциализации инноваций и развитие региональной инновационной системы в целом. В начале этой работы было выявлено следующее:

- Показатели готовности студентов как к научной, так и к инновационной и организаторской деятельности крайне низки. Даже на старших курсах и при выпуске студенты часто не обладают базовыми компетенциями.
- Отсутствия внятных информационных механизмов на уровне города для информирования молодежи.
- Низкая мотивация студентов к развитию в области науки.
- Слабость студенческих научных структур.
- Очень большой процент выпускаемых специалистов работают не по специальности. Рассогласованность нацеленности профессиональной подготовки специалистов в вузе с реальными потребностями рынка труда.
- Слабое межвузовское взаимодействие.
- Низкий уровень коммерциализации разработок.

Связи с этим была поставлена задача создания механизмов устраняющие эти пробелы. В результате были созданы две структуры: Интеллектуальное молодежное сообщество города «МолНаука» и межвузовская организация «Молодежный Центр Инноваций» взаимодополняющие друг друга. В основу каждой из них были положены принципы сетевой работы, горизонтальных связей и гибких методов управления.

Молодежная наука – городской уровень

Для работы на городском уровне был выбран формат сообщества, как свободного объединения людей или молодежных организаций на основе интереса к интеллектуальной, научно-исследовательской и проектной деятельности. Основная аудитория молодые от 16 до 30 лет, но к участию привлекаются и люди более старшего возраста способствующие развитию молодежной науки. Формат сообщества был выбран не строго научный, а скорее нацеленный на интеллектуальную молодежь в общим смысле.

Основные функции сообщества:

- Коммуникационная – обеспечение интеллектуального круга общения.
- Информационная – сбор необходимой информации, оповещение о новостях всех заинтересованных лиц, ведение соответствующих баз данных.
- Консультативная – предоставление начальных консультаций по базовым вопросам.

- Организационная – самостоятельная или совместно с другими структурами организация мероприятий, конкурсов и различных проектов.
- Объединяющая – организация межвузовского взаимодействия.

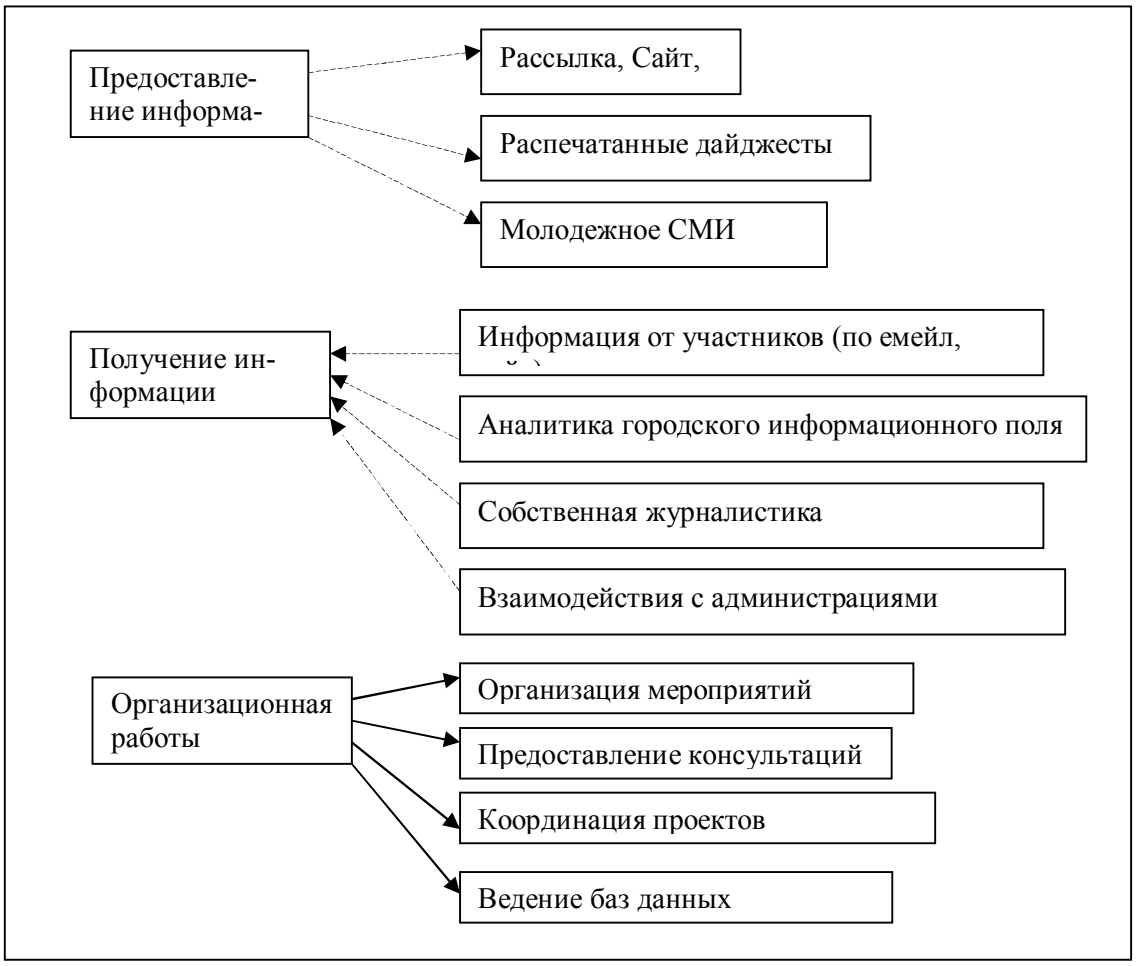


Рис. 1. Схема работы сообщества

Организацией работы сообщества занимается коллектив молодых людей из разных вузов возрастом 20–25 лет. Формат сообщества, основанный на принципе горизонтальных связей, предполагает отсутствие прямого подчинения входящих в него структур координаторам проекта. В связи с этим обыкновенная командно-административная система работать не будет. На первую позицию выступает установка общих принципов работы, обеспечение комфортных условий для участия, система мотивации и лидерство.

Одним из принципов взаимодействия является заключение с организацией вступающей в сообщество соглашения о сотрудничестве в мягкой форме определяющий формат информационного взаимодействия и взаимопомощи при реализации проектов.

Система мотивации и одновременно с ней обеспечение удобного формата участия в общей деятельности сообщества является чрезвычайно важным, так как участие в нем является доброй волей самих участников. Схема мотивации для рядовых участников и участников участвующих в организационной деятельности и тратящих значительно больше времени и сил на развитие сообщества – различаются.

Мотивация для простых участников:

- Получение интересной и полезной информации.
- Возможность быстрого и легкого распространение своей информации.
- Нахождение людей с похожими интересами в области науки.
- Возможность получение помощи в развитии своих проектов.

Для участников занимающихся еще и организаторской деятельности схема мотивации дополняется следующими пунктами:

- Получение дополнительных практических знаний и компетенций (управленческих, организационных, профессиональных).
- Стимулирование карьерного роста или получение более высокого социального статуса.
- Прохождение дополнительного обучения (семинаров и тренингов).
- Более представительный уровень контактов.

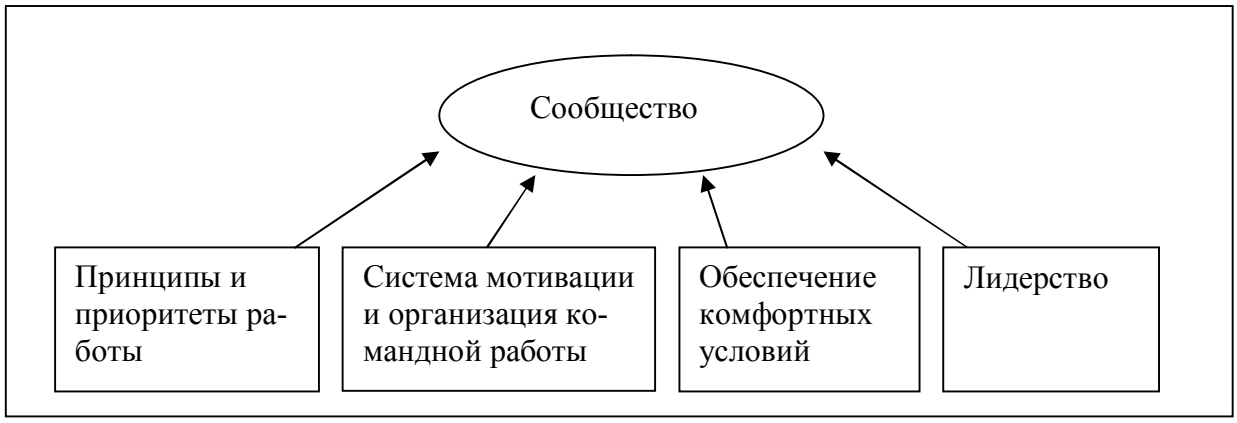


Рис. 2. Необходимые элементы для сетевых социальных структур

Принцип участия в сообществе максимально демократичен и прост в отличие от всех других подобных структур городского масштаба, например студенческого совета. Принимать участие с сообществе могут объединения, не носящего официального статуса или личности, не занимающие те или иные должности и регалии. Главным критерием является заинтересованность в развитии данного направления, активность и реально проводимая работа.

Конечно, важную роль во всех подобных молодежных структурах является институт лидерства – наличие ярких сильных личностей, являющихся флагманами развития сообщества [1].

Уровень университетов

На уровне университетов является перспективным развитие различных студенческих научных обществ, кружков и союзов. На практике в разных вузах они имеют совершенно различный формат и функции их работы во многом аналогичны функциям сообщества. Тем не менее, есть и различия. Например, как правило, такие структуры имеют более четкую управленческую вертикаль и несколько более жесткие способы управления.

Интересен и замеченный эффект фрактальности: обычно организация работы на кафедрах, факультетах и в университете в целом повторяет друг друга с различием в масштабах. В свою очередь, аналогичный эффект продолжается и в надуниверситетском уровне.

Организация инновационной деятельности

Конечно не вся научная деятельности напрямую коммерциализируема, что является вполне нормальным. Тем не менее, порядка 10% проводимых научно-исследовательских работ вполне могут претендовать на коммерческий успех. Для коммерциализации таких разработок создан городской молодежный инновационный центр.

В его функции в частности входит:

- Реализация инновационных проектов, внедрение разработок, Старт-ап, поиск инвестиций.
- Консультирование.
- Совместная работа с вузами.
- Развитие молодежной научной среды, пропаганда научно-технического творчества.
- Организация семинаров и обучения менеджеров.
- Организация практики студентов.
- Аналитика инновационной среды.
- Разработка концепции развития национальной и региональной инновационной системы.

Схема взаимодействия центра с другими субъектами инновационной среды показана на рис. 3

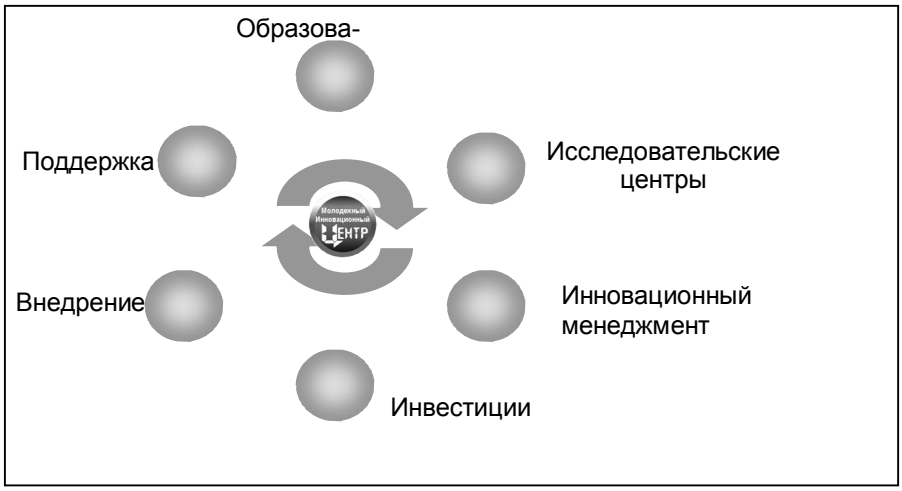


Рис. 3. Инновационная среда

Как видно, являясь действительно центром взаимодействия, он объединяет разрозненные элементы инновационной цепочки. Подобная схема работы показала свою эффективность во многих странах, например в США в знаменитой силиконовой долине [2].

Заключение

Данный формат развития молодежной научной и инновационной среды является одновременно и эффективным и гибким. Становиться понятным, что для подобного рода задач применение обыкновенных командно-административных систем не является эффективным. Им на смену приходят способы построения организация на основе социальных сетей, открытых информационных площадок и горизонтальных связей. Административным структурам, как на уровне университетов, так и на уровне региональной власти следует обратить больше внимания на такие сообщества и способствовать их развитию.

Литература

1. О принципиальной схеме федеральной инновационной системы. С.Б. Переслегин, Боровиков С.Е. Электронный ресурс: www.igstab.ru
2. Шихвердиев А.П., Вишняков А.А. Инновационная деятельность – главное условие устойчивого развития экономики Российского Севера. Электронный ресурс: www.miiris.ru

УДК 004.032.26

НЕЙРОСЕТЕВОЙ МЕТОД ОПТИМИЗАЦИИ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ВЫТЯЖКИ ОПТИЧЕСКОГО ВОЛОКНА

Д.В. Соловьев, И.Б. Бондаренко
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

В данной статье рассматривается разработка алгоритма оптимизации математической модели сложного технологического процесса вытяжки оптического волокна с помощью технологии нейронных сетей. Выведена математическая модель технологического процесса вытяжки оптического волокна. Показана сложность технологического процесса вытяжки оптического волокна, перечислены критерии качества оптического волокна.

Ключевые слова: оптимизация, сложный технологический процесс, вытяжка оптического волокна, нейросетевой алгоритм, математическая модель

Введение

В производственной деятельности встречаются физико-математические задачи, не формализуемые традиционными математическими методами, не имеющие аппарата для решения или существующий аппарат не удовлетворяет каким либо требованиям. Наилучшим для решения именно таких задач является нейросетевой подход.

Среди технологических процессов (ТП) широко применяется термическая обработка заготовок. Совершенствование процессов нагрева изделий на основе интенсификации теплофизических процессов позволяет повысить производительность продукции, обеспечить экономию энергоресурсов.

Эффективность решения указанных задач в значительной мере зависит от экспериментальной информации о тепловом состоянии процессов. Таким образом, объективно возникает необходимость разработки и исследования, работающих в реальном масштабе времени технологических процессов [1–2].

Рассматриваемый в данной статье технологический процесс вытяжки оптического волокна методом химического газофазного осаждения является сложным и многопараметрическим за счет различного рода вносимых возмущений. Сложность необходимых вычислений для решения задачи оптимизации скорости вытягивания оптического волокна делает актуальным разработку алгоритма решения данной задачи с применением нейросетевого метода [3–7].

ТП вытяжки оптического волокна

В нашем случае оптимизации подлежит ТП получения оптического волокна на MCVD-установке.

Исходными компонентами для получения синтетического стекла в MCVD-процессе являются газообразные галогениды кремния, германия, фосфора и бора.

После получения заготовки-преформы переходят к процессу формирования тонкого волокна. Для этого конец преформы нагревается в печи до пластичного состояния. При этом устройство вытягивает высоковязкий расплав в тонкую нить требуемого диаметра. Возможность такого ТП обуславливается из-за наличия у вытягиваемого вещества достаточно широкого температурного интервала вязко-пластичного состояния или зависимости вязкости от температуры.

В исследуемом ТП наиболее важными являются температурные зависимости поверхностного натяжения и вязкости материала, которые сильно отличаются друг от друга:

$$\eta = \eta_0 e^{-\frac{E_a}{RT}}, \quad (1)$$

где η_0 – вязкость в центре волокна; E_a – энергия активации вязкого течения (для кварцевого стекла энергия активации составляет 600 кДж/моль); T – абсолютная температура; R – газовая постоянная.

Температурные границы области вытягивания взаимосвязаны с величиной усилия вытяжки. При температуре ниже верхней границы отжига, где невозможна пластическая деформация материала, а также, если скорость вытягивания слишком велика, и расплав начинает проявлять упруго-пластичные свойства и разрывается, процесс вытягивания становится невозможным. В свою очередь, скорость вытягивания волокна определяется усилием вытягивания. При сопоставлении процессов упругой и пластической деформации твердых тел и вязкости упругих тел в условиях высокотемпературного нагружения, вытекает зависимость между временем деформации, усилием и вязкостью [8]:

$$\Delta l = \frac{Fl\tau}{3\pi R^2 \eta}, \quad (2)$$

где Δl – удлинение образца; F – сила натяжения; l – длина образца; τ – время деформации; R – радиус образца.

Учитывая квазистационарность процесса вытягивания волокна, сделано следующее преобразование зависимости (2):

$$V_в = \frac{\Delta l}{\tau}; A = \frac{l}{3\pi R^2} \Rightarrow V_в \eta = AF, \quad (3)$$

где А – постоянная для данного типа волокна, в которую входят геометрические размеры.

Из соотношений (1) и (3) имеем:

$$V_в = \frac{AF}{\eta_0} e^{\frac{E_a}{RT}}. \quad (4)$$

Полученная зависимость (4) будет использована в дальнейшей работе как исходная формула для формирования обучающего набора искусственной нейронной сети.

Показатели качества оптического волокна

Для контроля сложного ТП вытягивания оптического волокна исследуются следующие показатели качества:

- геометрия оптоволокна – отклонение диаметра от требуемого значения, цилиндричность;
- профиль показателя преломления;
- затухание в оптоволокне;
- прочность волокна.

На качество оптоволокна влияет как множество входных параметров, в том числе качество заготовки-преформы, так и множество случайных воздействий, действующих извне. Поэтому, учет всех воздействующих факторов, приводящих к ухудшению качества получаемого оптического волокна, является сложной задачей. Поставленную задачу предполагается решить с помощью математического аппарата искусственных нейронных сетей.

Нейросетевой подход

Анализ работ, связанных с использованием нейронных сетей для решения физико-математических задач, показал, что нейросетевой подход имеет преимущества перед традиционными математическими методами в трех случаях:

- задача в силу конкретных особенностей не поддается адекватной формализации, поскольку содержит элементы неопределенности, не формализуемые традиционными математическими методами;
- задача формализуема, но в настоящее время отсутствует аппарат для ее решения;
- решение задачи не удовлетворяет требованиям получения решений по времени, размеру, весу, энергопотреблению и др. (в данной ситуации приходится либо производить упрощение алгоритмов, что снижает качество решений, либо применять соответствующий нейросетевой подход при условии, что он обеспечит нужное качество решении задачи) [9–11].

Учитывая факторы, существенно влияющие на скорость вытяжки оптического волокна, для определения скорости вытяжки оптического волокна было решено использовать в качестве топологии сети схему трёхслойного персептрона с одним скрытым слоем. Количество нейронов входного слоя соответствует количеству входных данных и равно двум. В выходном слое находится один нейрон, что соответствует количеству выходных данных. Количество нейронов в скрытом слое было принято равным восьми.

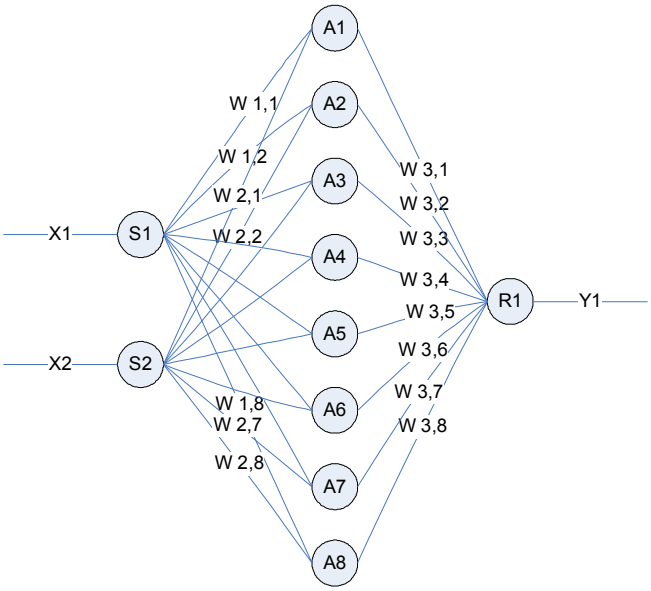


Рис. 1. Топология нейронной сети

Топология нейронной сети представлена на рис. 1, где X1 и X2 – входные значения температуры и силы натяжения; S1 и S2 – нейроны входного слоя; W 1,1–W 1,8 – веса от первого нейрона входного слоя к нейронам скрытого слоя; W 2,1–W 2,8 – веса от второго нейрона входного слоя к нейронам скрытого слоя; A 1–A8 – нейроны скрытого слоя; W 3,1–W 3,8 – веса от нейронов скрытого слоя к нейрону последнего слоя; R1 – нейрон последнего слоя; Y1 – выходное значение скорости вытяжки.

Активационная функция нейронов первого и последнего слоя линейная:

$$Y=K*S, \quad (5)$$

где S – взвешенная сумма входов нейрона; K – коэффициент пропорциональности (в данном случае его значение равно 1); Y – значение функции.

В качестве активационной функции нейронов скрытого слоя используется гиперболический тангенс:

$$Y=\tanh(S), \quad (6)$$

где S – взвешенная сумма входов нейрона.

Для определения размера обучающей выборки, для корректного обучения сети, были использованы рекомендации данные в работе Е. Баума и Д. Хасслера. Ими рекомендуется выполнение следующего неравенства:

$$N > W/e, \quad (7)$$

где N – размер обучающего набора; W – число весовых коэффициентов в сети; e – доля ошибок, допустимая в процессе работы сети.

Итак, учитывая, что в нашей топологии 24 весовых коэффициентов и доля ошибки будет задана не более 20%, количество обучающей выборки должно быть больше либо равно 120 обучающим наборам [12–15].

Обучение сети

Сеть обучалась по алгоритму Румельхарта-Хинтона-Вильямса (алгоритму обратного распространения ошибки).

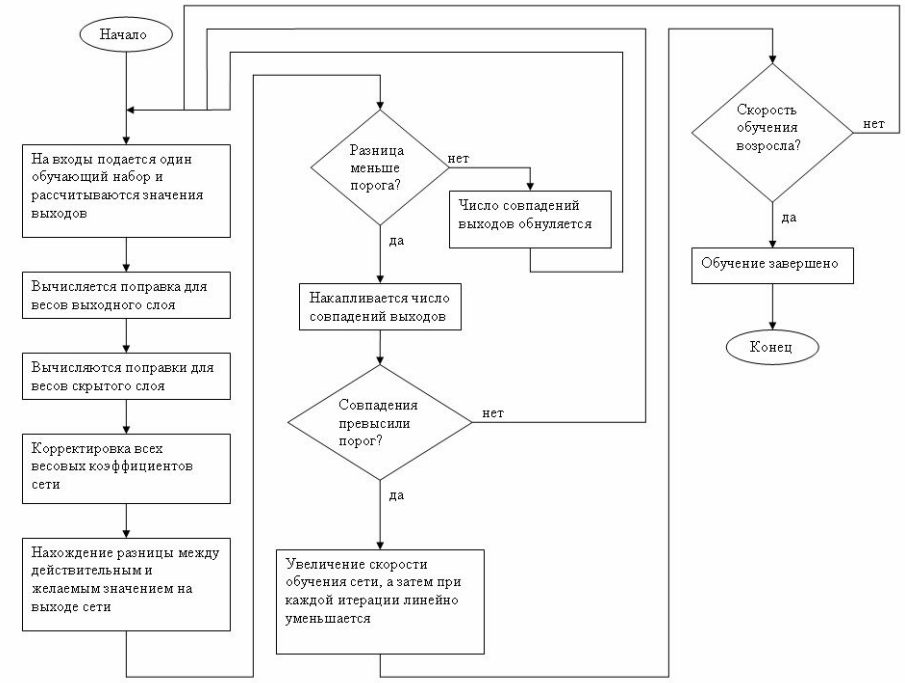


Рис. 2. Алгоритм обучения нейронной сети

В алгоритме Румельхарта-Хинтона-Вильямса (рис. 2) для минимизации функции ошибки используется метод градиентного спуска. Его применение не гарантирует, что в процессе обучения будет найден глобальный, а не локальный минимум этой функции. В данной реализации, для исключения случайных попаданий в локальные минимумы каждый раз после того, как работа сети стабилизировалась, значение скорости обучения кратковременно увеличивалось, чтобы начать градиентный спуск из новой точки. Если повторение этой процедуры несколько раз приводило алгоритм в одно и то же состояние сети, то предполагалось, что найден глобальный минимум функции с требуемой ошибкой и обучение сети прекращалось.

Максимизация целевой функции

На данном этапе непосредственно и производится оптимизация технологического процесса вытяжки оптического волокна нейросетевым методом. Теперь входы нейронной сети X1 и X2 становятся переменными для обученной сети, они подстраиваются с помощью того же самого обучающего алгоритма обратного распространения ошибки,

который применялся для выставления весов при обучении, однако теперь используется для максимизации целевой функции. Другими словами производиться поиск максимального значения Y1 – значения скорости вытяжки.

Результаты работы алгоритма

Результат работы алгоритма представлен в виде графика на рис. 3. Были выбраны 8 дискретных значений температуры (1900 – 2250)°С. Черным цветом отмечены графики зависимостей полученные из ранее выведенной математической модели вытяжки оптического волокна, а красным – графики, построенные по точкам, рассчитанным нейронной сетью. Анализируя графики можно заключить, что модель нейронной сети является адекватной, т.к. ошибка относительно математической модели составила менее 20%.

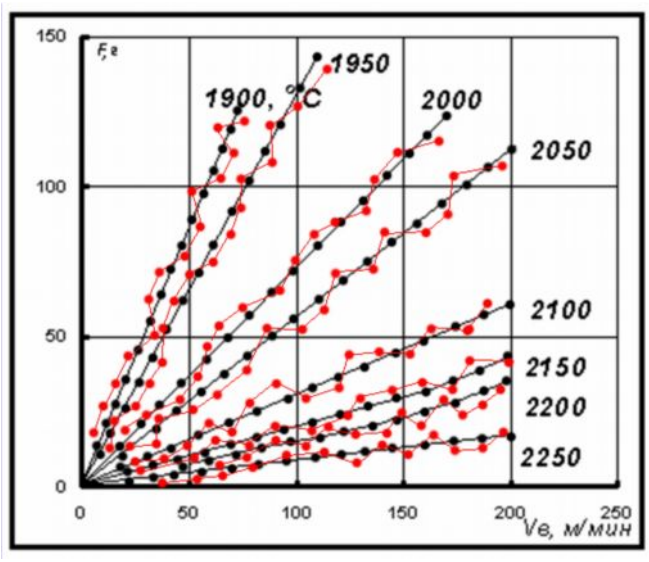


Рис. 3. Результаты работы алгоритма

Выводы

Резюмируя всё вышесказанное можно сформулировать следующие выводы:

1. технологический процесс вытяжки оптического волокна относится к сложным ТП;
2. для проведения оптимизации ТП его модель должна быть адекватна и содержательна;
3. получена математическая модель ТП вытяжки оптического волокна;
4. качество оптоволокна достаточно сложно контролировать в процессе его производства;
5. для оптимизации ТП был предложен нейросетевой подход;
6. нейросетевой подход показал свою адекватность, ошибка составила менее 20%.

Литература

1. Бондаренко И.Б., Андреев А.К., Гатчин Ю.А. Интегрированная система автоматизированного производства оптических материалов //Тезисы докладов научн.-технич. международной конференции «Прикладная оптика-96», г. Санкт-Петербург, 1996. – С. 109.
2. Бондаренко И.Б., Гатчин Ю.А. Методы автоматизированного проектирования сложных технологических систем по производству оптических материалов//Тезисы док-

ладов 29 научно-технической конференции «Проектирование и технология элементов компьютерных систем», СПбГИТМО(ТУ), 1997. – С. 6–7.
3. Алексеев А.В. Интеллектуальные системы принятия проектных решений. Рига. – 1997.
4. Гатчин Ю.А., Коробейников А.Г. Проектирование интегрированных автоматизированных технологических комплексов. – СПб: СПбГИТМО(ТУ). – 2000.
5. Бондаренко И.Б. Методы оптимального проектирования сложных технологических систем//Тезисы докладов 31 межвузовской научно-технической конференции профессорско-преподавательского состава. – 1999. – СПбГИТМО(ТУ). – С. 86.
6. Бондаренко И.Б., Гатчин Ю.А. Оптимизация выбора проектных решений//Тезисы докладов 30 межвузовского научно-технический семинара с международным участием «Автоматизация проектирования, технология элементов и узлов компьютерных систем», апрель 98г., СПбГИТМО(ТУ). – С. 7–8.
7. Бондаренко И.Б., Гатчин Ю.А. Оптимизация проектных решений в САПР автоматизированных технологических комплексов//Научно-технический вестник СПбГИТМО(ТУ). Выпуск 6. Информационные вычислительные и управляемые системы. СПбГИТМО(ТУ) 2002. – С. 127–135.
8. Соломин Н.Д. Жаростойкость материалов и деталей под нагрузкой. – М.: Стройиздат. – 1969.
9. Научная сессия МИФИ-2003, V Всероссийская научно-техническая конференция «Нейроинформатика-2003», лекции по нейроинформатике. Часть 1. – М.: МИФИ. – 2003. – 188 с.
10. Вороновский Г.К., Махотило К.В., Петрашев С.Н., Сергеев С.А. Генетические алгоритмы, искусственные нейронные сети и проблемы виртуальной реальности. – Х.:ОСНОВА. – 1997. – 112 с.
11. Заенцев И.В. «Нейронные сети: основные модели», учебное пособие, Воронеж. – 1999.
12. Дианов Р.С. Оптимизация технологического процесса разработки газоносного пласта с применением генетических алгоритмов и нейронных сетей: Дис. ... канд. техн. наук: 05.13.06 Астрахань. – 2004. – 167 с.
13. Уоссермен Ф. «Нейрокомпьютерная техника: Теория и практика», перевод на русский язык Ю.А. Зуев, В.А. Точенов. – 1992.
14. Соловьев Д.В. Нейросетевой метод оптимизации математических моделей сложных технологических процессов. Научно-технический вестник СПбГУ ИТМО. – 2008.
15. Гатчин Ю.А., Бондаренко И.Б., Соловьев Д.В. Интеллектуальная поддержка выработки оптимальных решений в САПР оптического производства. Труды Международных научно-технических конференций «Интеллектуальные системы» (AIS”09) и «Интеллектуальные САПР» (CAD-2008).

УДК 535.326

ОБЗОР ОПТИЧЕСКИХ УСТРОЙСТВ НА ФОТОННЫХ КРИСТАЛЛАХ

А.Н. Волченко, А.А. Киянов, И.В. Бейдина, А.В. Левшина
Научный руководитель – д.т.н., профессор В.Л. Ткалич

Рассмотрены физико-технические особенности фотонных кристаллов. Представлен обзор конструкций и характеристик устройств на их основе.
Ключевые слова: фотонная решётка, запрещённая зона, фотонно-кристаллические волноводы

Введение

В 1998 году западные информационные агентства сообщили, что в лаборатории Sandia National Laboratories, принадлежащей американскому департаменту энергетики, разработана новая «светоизгибающая» (light bending) технология, которая в недалёком будущем найдёт применение в телекоммуникационных сетях. Микроскопическая трёхмерная структура (получившая название фотонной решётки) создана на основе кремния и позволяет передавать когерентный свет в оптическом диапазоне длин волн с минимальными потерями. Эффективность передачи составляет 95 процентов, что значительно превосходит показатель стандартных светопередающих сред (около 30 процентов), используемых в настоящее время. При этом можно направлять лучи по сложной траектории, содержащей «изгибы», практически под прямым углом в заданную точку. Решётка представляет собой пачку тонких кремниевых двухмерных дифракционных решёток, каждый слой которой повёрнут на 90 градусов относительно соседнего. Для создания работающей «фотонной решётки» достаточно десяти таких слоёв.

При взгляде через микроскоп фотонная решётка похожа на подготовленный костёр, сложенный «колодцем» (рис. 3а). Она обладает уникальной способностью изгибать траекторию световых волн определённой частоты практически в любом направлении и практически без потерь. Это изобретение может привести к существенному прогрессу в области телекоммуникаций и оптических компьютеров.

Решётка из перекрёстных диэлектрических полосок является «идеально» отражающей средой для световых волн определённого диапазона частот, который называется «запрещённой зоной». Световые волны этого диапазона не могут распространяться внутри решётки, а при наличии внутри неё полостей или нерегулярностей оказываются «захваченными» такими «ловушками». Создавая цепочки нерегулярностей, можно формировать световедущие каналы, при помощи которых открывается возможность изменять направление световых волн даже на острые углы.

Обширная информация по ФК содержится в Интернете. На сайте [1], полностью посвященном ФК, сгруппированы ссылки с информацией по ФК.

Основная часть

Идея фотонной решётки была предложена ещё в 1987 году Эли Яблоновичем, работающим сейчас профессором в Калифорнийском университете. Первый фотонный кристалл размером с бейсбольный мяч был создан в 1990 году, он управлял микроволновым излучением. Тогда же был создан кристалл размером уже с шарик для пинг-понга (в университете штата Айова), он тоже работал в микроволновом диапазоне. Первые кристаллы-решётки собирались вручную из обычных металлических иголок. В

том же направлении работала и группа Иоаннопулоса в Массачусетсском технологическом институте.

Фотонные кристаллы, благодаря периодическому изменению коэффициента преломления, позволяют получить разрешённые и запрещённые зоны для энергий фотонов, аналогично полупроводниковым материалам, в которых наблюдаются разрешённые и запрещённые зоны для энергий носителей заряда. Практически, это значит, что если на фотонный кристалл падает фотон, обладающий энергией (частотой), которая соответствует запрещённой зоне данного фотонного кристалла, то он не может распространяться в фотонном кристалле и отражается обратно. И наоборот, это значит, что если на фотонный кристалл падает фотон, обладающий энергией (частотой), которая соответствует разрешённой зоне данного фотонного кристалла, то он может распространяться в фотонном кристалле. Другими словами, фотонный кристалл выполняет функцию оптического фильтра (рис. 6), и именно его свойствами обусловлены яркие и красочные цвета опала в женском браслете.

Фотонный кристалл (ФК) для оптического диапазона представляет собой пространственную решетку с периодом порядка длины волны света с пространственно модулированным показателем преломления. Различают два основных типа трехмерных ФК, показанные на рис. 1. В первом случае (рис.1,а) в узлах решетки ФК размещены одинаковые диэлектрические частицы, например, шары. Здесь ε_1 и ε_2 – диэлектрическая проницаемость вне и внутри шаров, соответственно. Противоположное решение – периодически расположенные отверстия в диэлектрике. В этом случае (рис. 1,б) узлы решетки в диэлектрике с проницаемостью ε_1 связаны друг с другом стержнями с диэлектрической проницаемостью ε_2.

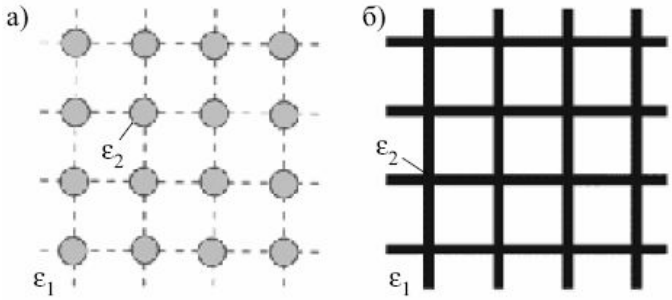


Рис. 1. Основные типы трехмерных ФК: а) в узлах решетки размещены диэлектрические частицы; б) узлы решетки связаны друг с другом стержнями

Помимо значения постоянной решетки, характеристики ФК определяются глубиной модуляции показателя преломления – оптическим контрастом, равным отношению показателей преломления элементов решетки и среды, в которой они размещены. ФК могут быть одно-, двух- и трехмерными. К одномерным ФК относят давно используемые тонкопленочные оптические фильтры, а также планарные отражательные решетки интегральных устройств оптоэлектроники. Принципиальные особенности ФК и других кристаллоподобных структур проявляются в одномерном варианте.

Зонные свойства электронных и фотонных кристаллов определяются дисперсионной характеристикой $\omega(k)$, где ω – круговая частота, k – волновое число. Эта характеристика определяет также и энергетическую зависимость $E(k)$, поскольку $E = \hbar\omega, \hbar = h/2\pi$, h – постоянная Планка.

Рис. 2 иллюстрирует зависимость $E(k)$, а также соответствие между электронными и фотонными запрещенными зонами. Здесь m^* – эффективная масса электрона; n^* – эффективный показатель преломления, соответственно характеризующие влияние кристаллической решетки на движущийся в ее поле электрон и движущийся в ФК фотон. На границах запрещенной зоны и в самой запрещенной зоне собственные функции кристалла – стоячие волны, так что волны с такими энергиями распространяться

не могут. Внутри запрещенной зоны значение k мнимое. Отрицательность m^* и n^* обусловлена значительным отражением, при котором амплитуда отраженной волны превышает амплитуду падающей. Электроны с отрицательной m^* (эти состояния расположены вблизи потолка зоны) соответствуют дыркам. Отрицательному n^* отвечает отрицательная рефракция – изменение направления распространения света на противоположное. При $n^* >> \langle n \rangle$, где $\langle n \rangle$ – средний показатель преломления ФК, свет существенно замедляется. В двухмерном ФК экспериментально достигнуто значение $n^* > 90$, что соответствует замедлению света приблизительно на два порядка [2].

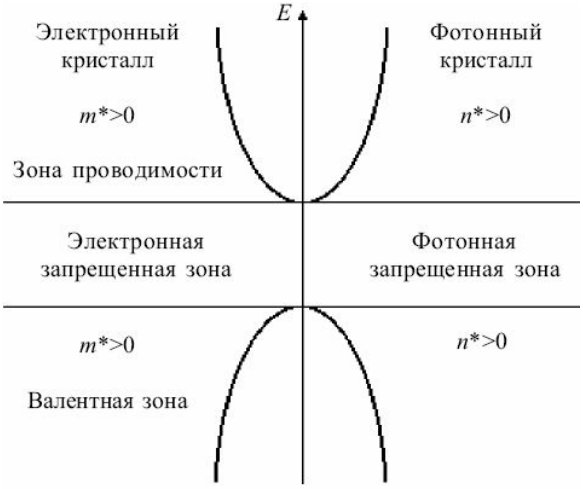


Рис. 2. Соответствие между электронными и фотонными зонами

В дисперсии фотонов и электронов имеются два принципиальных различия: 1) линейный закон дисперсии свободных фотонов вместо параболического закона дисперсии свободных электронов; 2) существенная малость размера зоны Бриллюэна ФК, равная π/d (d – постоянная решетки), по сравнению с размером зоны Бриллюэна электронов в полупроводниках, т.к. период ФК приблизительно в 10^3 раз превышает постоянную кристаллической решетки.

Фотонные кристаллы в природе – большая редкость. С древних времен человека, нашедшего такой кристалл, завораживала в нем особая радужная игра света. Это оптическое явление, получившее название иризация (от греч. iriV – радуга), характерно для таких минералов, как кальцит, лабрадор, опал. От игры света в последнем происходит термин опалесценция, обозначающий особый, характерный только для этого кристалла тип рассеяния излучения. Кластерная сверхрешетка опала послужила прототипом для создания искусственных фотонных кристаллов. Например, в одной из самых первых работ по синтезу фотонных кристаллов, выполненной в Физико-техническом институте (СПб) и МГУ в 1996 году, была создана технология получения оптически совершенных синтетических опалов на основе сфер микроскопического размера из двуокиси кремния. Технология позволяла варьировать параметры синтетических опалов: диаметр сфер, пористость, показатель преломления.

ФК для микроволнового диапазона изображены на (рис**.** 3.) На (рис. 3,а) показан металлический ФК, имеющий простую тетрагональную структуру [3]. Кристаллическая ячейка ФК образована металлическими брусками смежных слоев. Размеры бруска: ширина 0,8 мм, толщина 2,5 мм, длина 120 мм, расстояние между центрами смежных параллельных брусков 7,6 мм. Запрещенная зона такого ФК расположена в диапазоне от нуля до 20 ГГц.

ФК, показанный на (рис. 3,б) образован диэлектрическими стержнями, расположенными между проводящими плоскостями [4].

В [5] предложено использование ФК для улучшения диаграмм излучения антенн, предназначенных для контроля электромагнитной совместимости. В случае печатной микрополосковой антенны трехмерный ФК используется в качестве подложки. Такие структуры виртуально невидимы на некоторых частотах и ведут себя как проводники на других частотах, не позволяя сигналу распространяться. Антенны, предназначенные для контроля электромагнитной совместимости, отличаются очень широкой полосой. ФК может использоваться в качестве структуры, формирующей поле излучения антенны. В [5] предложено использование ФК для расширения частотного диапазона рупорной антенны за счет уменьшения уровня излучения мод высокого порядка.

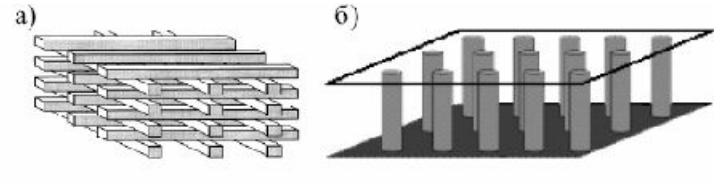


Рис. 3. ФК для микроволнового диапазона: а) металлический ФК; б) ФК, образованный диэлектрическими стержнями, расположенными между проводящими плоскостями

Фотонные кристаллы служат основой нового поколения компактных элементов и устройств интегральной оптики и волоконно-оптических линий связи. Среди этих элементов и устройств – миниатюрные расщепители, волноводы с остроугольным изгибом, переключатели, поверхностно излучающие лазеры с вертикальной полостью, светодиоды с резонансной полостью, фильтры, волоконные световоды. Трехмерные ФК открывают возможность полного управления фотонными модами и, следовательно, конструирования лазеров и светодиодов с предельной эффективностью. ФК обеспечивают важное для технических приложений удержание излучения по всем направлениям с малыми потерями.

В настоящее время известны два типа волоконных световодов со структурой фотонных кристаллов. Это волоконные световоды со сплошной световедущей жилой, и волоконные световоды с полой световедущей жилой. В России и те, и другие называются дырчатыми волокнами, хотя на самом деле между ними существует важное различие в механизмах, обеспечивающих волноведущие свойства световодов.

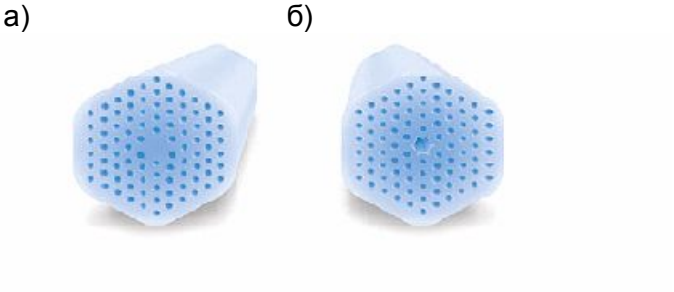


Рис. 4. Конструкция волноводов

На (рис.4,а) показан одномодовый ФК-световод, выполненный из нелегированного кварцевого стекла с воздушными отверстиями. Такой световод имеет ряд существенных преимуществ по сравнению с обычным световодом. Обычный одномодовый световод обладает одномодовым характером лишь в ограниченном диапазоне длин волн (свыше длины волны отсечки). ФК-световод не имеет такого ограничения. Большая длина и изгибы в обычном световоде приводят к потерям из-за утечки света. ФК-световод позволяет передавать мощность, приблизительно в 20 раз превышающую предельную мощность для обычного световода. В световоде с полой сердцевиной (рис. 4,б) уменьшены потери по сравнению с предыдущей конструкцией. Использо-

вание воздушного волноведущего канала позволяет полностью исключить оптическую нелинейность, так что порог мощности, при котором проявляются нелинейные эффекты, возрастает в 10^3 раз по сравнению с обычным световодом. На концах световода нет рассогласования показателей преломления, что исключает отражение волны. ФК-световоды существенно менее чувствительны к температурным и механическим воздействиям.

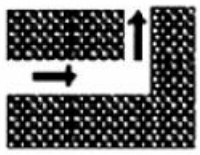


Рис. 5. Волновод с остроугольным изгибом

Современные световедущие каналы на основе оптического волокна не могут иметь крутых изгибов из-за недопустимого увеличения потерь, вызванного нарушением полного внутреннего отражения в них. Световедущие каналы в фотонном кристалле основаны на другом принципе: практически идеальное отражение света под любым углом от стенок световедущего канала обеспечивается наличием «запрещённой зоны» для световой волны передаваемой частоты, препятствующей проникновению света вглубь фотонного кристалла (рис. 5).

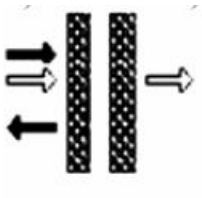


Рис. 6. Проходной фильтр

На (рис. 6) представлен проходной фильтр на ФК. ФК-световоды изготавливаются из пучка трубок и прутков из кварцевого стекла, образующих «макроскопическую» преформу структуры световода. Преформа скрепляется танталовой проволокой и помещается в печь для вытяжки. При температуре приблизительно 2000°С кварцевое стекло размягчается. В результате двухэтапной вытяжки формируется ФК-световод с расстоянием между соседними отверстиями, равным 1мкм, и диаметром отверстий 25 нм.

Привлекательность использования ФК в интегральной оптике объясняется следующими обстоятельствами:

1) высокая функциональная плотность, обусловленная тем, что ФК позволяют реализовать оптические функции в пределах размеров порядка длины волны без потерь (т.к. колебания связаны только с затухающими модами);

2) возможность изготовления в едином литографическом цикле конструктивно разнообразных структур для большого числа функций;

3) новые функции, обусловленные особенностями ФК (такими как дифракция, положительная рефракция со значительным замедлением, отрицательная рефракция).

Заключение

Таким образом, фотонные кристаллы предоставляют принципиально новые возможности управления световыми потоками благодаря наличию полной фотонной запрещенной зоны в плотности электромагнитных состояний в заданной области частот. Такие возможности экспериментально продемонстрированы для микроволновой

области, частично в инфракрасном и видимом диапазонах спектра. Трудности в создании фотонных кристаллов несоизмеримо возрастают по мере увеличения частоты фотонной запрещенной зоны, однако можно надеяться, что значительные усилия, прилагаемые в этом направлении, делают решение проблемы вопросом времени.

Литература

1. www.pbglink.com
2. www.brl.ntt.co.jp/group/shitsubi-g/project2-e.html
3. Temelkuran B., Ozbay E., Sigalas M. et al. Reflection properties of metallic photonic crystals //Appl. Phys. A. – 1998. – Vol. 66, N 3. – P. 363–365.
4. Maradudin A.A., McGurn A.R. Photonic band structure of a truncated, two-dimensional, periodic dielectric medium // J. Opt. Soc. Am. B. – 1993. – Vol. 10. – N 2. – P. 307–313.
5. Rodriguez-Pereyra V Photonic bandgap structures and their application to EMC antennas // ITEM. – 2002. – P. 90–95.

УДК 004.085

ОБЗОР ТЕХНОЛОГИИ ЗАПИСИ ИНФОРМАЦИИ НА ОПТИЧЕСКИХ НОСИТЕЛЯХ

А.А. Киянов, А.Н. Волченко, И.В. Бейдина
Научный руководитель – д.т.н., профессор В.Л. Ткалич

В статье представлен обзор технологий записи информации на оптических носителях, произведён сравнительный анализ оптических носителей.
Ключевые слова: оптические носители информации, CD, 3D, FMD,DVD, питы, лазер

Введение

Очень часто возникает задача длительного хранения большого объёма данных, с помощью записи на компактный и дешёвый носитель информации. Оптические носители информации, к которым относятся диски таких форматов, как CD-R, CD-ROM, CD-RW и DVD получили широкое распространение благодаря довольно большой вместимости, надежности хранения и невысокой цене. Что касается вместимости, то объем информации, которую можно хранить на CD-х до 700 Мбайт данных, а на DVD – до 17 Гбайт! При этом они обладают просто поражающей надежностью: срок хранения чистого диска до записи составляет от 5 до 10 лет, а записанный диск может храниться по разным оценкам от 70 до 200 лет. Малогабаритные оптические накопители в виде CD удобны в обращении и позволяют записывать большие объемы данных. Малогабаритные оптические накопители в виде CD удобны в обращении и позволяют записывать большие объемы данных. Поэтому диски CD нашли широкое распространение, как в профессиональных информационных системах, так и в бытовой электронике. В зависимости от характера записи информации и области использования различают несколько типов дисков.

CD диск

«Компактный диск с только читаемой памятью» CD-ROM имеет вид тонкой круглой пластины толщиной 1,2 мм. Состоит диск из поликарбонатной основы, с одной стороны покрытой тонким алюминиевым слоем, защищенным пленкой лака. Информация записывается производителем в процессе изготовления диска благодаря созданию углублений в его поверхности. Считывание информации осуществляется лазером со скоростью 150–450 Кбит/с.

Добавление к алюминиевому фоточувствительного слоя позволяет использовать технологию «компактного диска, записываемого» CD-R. Ее сущность заключается в том, что одноразовая запись данных на компактный диск осуществляет сам пользователь. Для этого он должен иметь и включить в абонентскую систему устройство, именуемое CD-рекордером. Запись осуществляется лучом лазера этого устройства. Основную часть структуры CD-R составляет прозрачный пластик, обладающий исключительными оптическими свойствами (именно в нем происходит фокусировка лазерного луча), и придающий диску необходимую механическую прочность. Далее располагается активный слой, необратимо меняющий свои свойства под действием лазерного луча. За ним находится отражающий слой, который представляет собой тончайшую напыленную пленку из серебра. Изменение условий экспонирования фоточувствительного слоя и по-разному нагретые участки покрытия диска вызывают точечную деформацию алюминиевого слоя, образуя на нем углубления. Данные размещаются на спиральной дорожке (как на граммофонной пластинке). Завершением этой конструкции часто является дополнительный защитный слой, допускающий нанесение на диск различных изо-

бражений. Этот слой исключает контакт красок, с помощью которых выполняется полиграфия, с отражающим слоем. Это может быть тонкое лаковое покрытие или полимерный слой. CD-RW диски (т.е. CD диски с возможностью многократной перезаписи) построены на основе технологии с изменением фазового состояния носителя.

Первые CD-RW диски (т.е. CD диски с возможностью многократной перезаписи) разработал и запустил в производство концерн RICOH. Современные диски такого типа построены на основе технологии с изменением фазового состояния носителя. Суть этой технологии состоит в том, что специальный активный слой обладает различным коэффициентом отражения в случаях, если его кристаллизация после разогрева происходила быстро или медленно. Таким образом, слой можно разогреть или медленно остудить, чтобы стереть записанную информацию (кристаллическая фаза), или разогревать только отдельные точки (соответственно, быстро остывающие), чтобы записать информацию (аморфная фаза).

Существенным фактом является то, что количество циклов его перезаписи ограниченно. Многие фирмы заявляют, что число циклов перезаписи для их дисков достигает 1000 раз, однако на практике это число оказывается значительно меньшим. Причем с ростом числа перезаписей параметры диска (коэффициент отражения и уровень ошибок) ухудшаются [1].

Digital Versatile Disc (DVD)

В конце 1990-х годов появились компакт-диски нового поколения – DVD (Digital Versatile Disc – цифровой многоцелевой, или универсальный диск) с большой емкостью, которые применяются для записи полнометражных фильмов, звука сверхвысокого качества и компьютерных программ. Существует несколько вариантов DVD, отличающихся по емкости: односторонние и двухсторонние, однослойные и двухслойные.

Основой записи и хранения данных на дисках DVD-RAM и DVD-RW является технология изменения фазового состояния вещества. При записи и считывании информации используется различие отражательной способности поверхности в зависимости от того, находится ли она в кристаллическом или аморфном состоянии.

При считывании информации с диска измеряется различие между темными аморфными и яркими прозрачными зонами. Эту технологию вполне можно назвать оптической – для чтения и записи достаточен всего лишь лазер. Луч лазера вызывает кристаллографические изменения в активном слое оптического диска. Короткий лазерный импульс высокой мощности расплавляет записывающий материал.

Принцип работы

Луч лазера вызывает кристаллографические изменения в активном слое оптического диска (а именно, в результате облучения вещество меняет свое состояние с кристаллического на аморфное и наоборот). Короткий лазерный импульс высокой мощности расплавляет записывающий материал (температура нагрева превышает температуру плавления материала, $T > T_{плавл.}$). Затем следует охлаждение ниже температуры кристаллизации ($T_{крист.}$). Результат охлаждения – предотвращение образования центров кристаллизации. Таким образом, роста кристаллической фазы не происходит, и вещество остается в аморфном состоянии.

Для стирания надо вернуть вещество в кристаллическое состояние. Опять же с помощью лазера аморфное вещество нагревают до температуры T, которая меньше температуры плавления, но больше температуры кристаллизации ($T_{крист} < T < T_{плавл}$). Нагрев (а точнее, отжиг) продолжается в течение времени ($t_{отж}$), достаточного для восстановления кристаллического состояния вещества. Это время должно быть больше, чем так называемое время кристаллизации ($t_{крист}$, $t_{крист} < t_{отж}$).

Форматы DVD

Возможны четыре разновидности DVD дисков: DVD-5, DVD-9, DVD-10 и DVD-18:

DVD-5 – это первая рыночная версия DVD диска: односторонний диск с однослойной записью и емкостью 4,7 Гб. DVD состоит из 0,6 мм пленки, покрытой алюминием и наклеенной на чистую подложку. Технология напыления та же, что используется при изготовлении обычного CD. Алюминиевая пленка имеет толщину 55 нанометров, как и для аудио-CD и CD-ROM.

DVD-10 – двухсторонний однослойный диск с емкостью 9,4 Гб. В принципе, это двойной DVD-5 без чистой подложки. Два диска, покрытых металлическими пленками, соединены вместе. Чтобы считывать информацию с двух сторон диска, используется один лазер.

DVD-9 – это односторонний двухуровневый диск с емкостью 8,5 Гбайт. Для производства такого диска необходимо создать полупрозрачный слой, который отражает 18–30% лазерного излучения. Этого достаточно, чтобы можно было считывать информацию с верхнего слоя. И в то же время полупрозрачный слой будет пропускать достаточно излучения, чтобы сигнал от нижнего уровня с высокой отражательно способностью тоже читался. Информационные уровни разделяет высокооднородный клей, (толщина клеевой прослойки составляет 40–70 микрон) используемый для соединения двух половин диска. Это расстояние необходимо, чтобы различить сигнал, отраженный от одного и другого уровней.

DVD-18 в принципе то же самое, что DVD-9, но DVD-18 может читаться с обеих сторон. Результат – двойная емкость по сравнению с DVD-9

Производство CD - DVD

Вначале берется специальное полированное стекло в виде диска, обработанное с высокой точностью. На поверхность этого диска в центрифуге наносится определенной толщины светочувствительный фоторезистивный слой. Лазерный луч, управляемый компьютером перемещается в радиальном направлении. При этом в результате импульсной модуляции, фоторезист засвечивается в определенных местах. Итогом последующей проявки фоторезиста в специальных растворах, является образование на стекле некоего рельефа – так называемых «пиитов». Далее, в специальных реактивах диск покрывается тонким слоем никеля, необходимого для дальнейшей операции электроформинга. В гальванических ваннах на диск осаждается слой никеля необходимой толщины. Почти готовая матрица отделяется от стекла, отмывается, шлифуется, рубится, тестируется, покрывается защитным лаком или пленкой. Все, можно печатать тираж [2].

«Синий луч» – конкурент DVD?

Sony, Philips и Matsushita, уже приступил к разработке нового стандарта оптических носителей информации. Эта система, получившая условное обозначение «blue-ray», то есть «синий луч», основана на использовании лазера, излучающего в сине-фиолетовом диапазоне светового спектра. Благодаря значительно более короткой длине волны – предполагается, что будущий стандарт установит для неё значение 405 нанометров – такое сине-фиолетовое считывающее устройство будет способно воспринимать гораздо более мелкие и плотнее расположенные микроуглубления на поверхности диска. Ёмкость нового носителя в стандарте «blue-ray» может быть доведена до 27-ми гигабайт. Кроме того, новый стандарт обеспечит исключительно высокую скорость передачи информации – до 36-ти мегабит в секунду, – что в принципе даст возможность, например, одновременно записывать на один диск два разных фильма. В отличие от

нынешних дисков DVD, новые оптические носители, ввиду их повышенной уязвимости и чувствительности к пыли и механическим повреждениям, будут заключены в специальную защитную оболочку-картридж. Однако у стандарта «blue-ray» есть и очень существенный недостаток – полная несовместимость с предшественниками [3].

«Трехмерный» диск

Компанией Constellation 3D (C3D) был продемонстрирован новый формат: FMD (Fluorescent Multilayer Disk), который уже скоро может стать новым лидером. Первым поколением дисковых продуктов компании C3D станет семейство 120 мм многослойных FM-дисков с вместимостью до 140 Гбайт и со скоростью чтения до 1 Гбита в секунду. На рис. 1 представлен внешний вид FMD-ROM. Из него мы видим, что FM диск прозрачный, данная технология не нуждается в присутствии отражающего слоя. Рассмотрим FM диск более детально.

В носителях FMD не используется отраженный луч лазера, так как при воздействии лазерного луча на информационный слой последний сам начинает излучать.

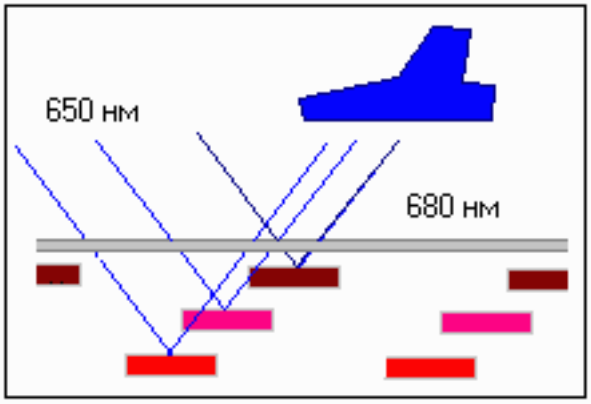


Рис. 1. Принцип считывания информации в FMD-носителях

Принцип действия флуоресцентных дисков основан на явлении фотохромизма. Несколько лет назад российские химики открыли стойкий органический материал «стабильный фотохром», под воздействием лазерного луча, приобретающий флуоресцентные свойства (флуоресцентное свечение). Дело в том, что информационный элемент FM-диска (фотохром) может менять свои физические свойства (такие как цвет или наличие флуоресценции) под воздействием лазера определенной мощности и длины волны. Изначально фотохром не обладает флуоресцентными свойствами. При воздействии лазера большой мощности, инициируется фотохимическая реакция, в результате которой и начинают проявляться флуоресцентные свойства.

При считывании данное вещество опять же возбуждается, но посредством лазера меньшей мощности, и начинает флуоресцировать. Это свечение улавливается фотоприемником и принимается как значение «1». Возбужденный фотохром излучает свет, сдвигая спектр падающего на него излучения в сторону красного цвета на определенную величину (в пределах 30–50 нм), что позволяет легко различить сигнал лазера и свет, излучаемый материалом диска. Необходимо отметить, что данная технология позволяет обойти проблему множественной интерференции между слоями, которая может привести к потери луча в многослойном диске, так как излученный фотохромом свет не когерентен и хорошо контрастирует с отраженным лазером, свободно проходит сквозь слои, и легко определяется фотодатчиком.

Сравнение с DVD

В обычных оптических носителях (CD/DVD) при увеличении числа информационных слоев происходит качественное ухудшение сигнала. Это объясняется тем, что в данных технологиях используется отраженный от информационного слоя сигнал, то есть существует необходимость в зеркальных поверхностях. Поэтому в технологии DVD при изготовлении двухслойных дисков внешний информационный слой делается полупрозрачным для того, чтобы дать возможность лазеру добраться до внутреннего слоя. При этом сигнал, проходящий через внешний слой, «оставляет» в нем часть энергии вследствие отражения. Причем отраженные от обоих слоев сигналы интерферируют (накладываются друг на друга или складываются) из-за их когерентности (совпадение частоты, и постоянной во времени разности фаз), в результате чего происходят потери полезного сигнала. Увеличение количества слоев усугубляет эффект множественной интерференции между слоями, и усложняется процесс считывания. Эту проблему можно решить путем усовершенствования детекторов-приемников, но это пока возможно осуществить только в лабораторных условиях. В случае флуоресцентных дисков такое качественное ухудшение сигнала при нарастании числа слоев происходит гораздо медленнее. Если это представить в виде графика, то выглядеть все будет примерно так: (см. презентацию). По заявлению разработчиков FMD-ROM, даже при количестве слоев больше сотни не будет происходить сильного искажения полезного сигнала, так как все слои диска прозрачны и однородны.

FM – диск

Диск состоит из нескольких пластиковых (поликарбонатных) слоев, соединенных между собой. Слой содержит поверхностные структуры («питы»), которые заполняются флуоресцентным материалом. При считывании лазер фокусируется на определенном слое и возбуждает его флуоресцентные элементы, после чего это свечение улавливается фотодетектором. Разработчики заявляют, что при использовании синего лазера (480 нм) возможно увеличение плотности записи до десятков Тбайт на один FM диск. Другая интересная особенность данной технологии заключается в возможности параллельного считывания. Если записывать последовательность бит не вдоль дорожки, а вглубь по слоям, то можно значительно повысить скорость выборки данных. Вследствие этого разработчиками FM диска, в шутку или всерьез, было предложено название своему детищу как «трехмерный диск». И действительно! Приведем список ряда преимуществ FMD/C: Малая потеря полезного сигнала при прохождении нескольких слоев. Меньшая, чем у CD/DVD, чувствительность к различным недостаткам устройств считывания.

Флуоресцентная технология не требует особых производственных условий. Излучающийся флуоресцентный свет с любого слоя не когерентен, тем самым устраняется проблема множественных интерференций, которая присутствует в технологиях CD/DVD. FMD-технология совместима с CD и DVD форматами, поддерживая ту же систему распределения данных на каждом слое [4].

Параллельное чтение

Как уже и упоминалось выше, в данной технологии существует возможность параллельного чтения, то есть последовательность бит записывается не вдоль дорожки, а вглубь по слоям. Таким образом, появляются три способа чтения данных: последовательный, последовательно-параллельный и параллельный. Процесс чтения производится с помощью фоточувствительного элемента, который представляет собой массив CDD камер. Данный прибор способен считывать маломощное свечение с частотой в несколько десятков МГц. При этом скорость считывания достигает 1 Гбит/с. Надо от-

метить, что механическая скорость работы привода при этом в 450 раз меньше чем у DVD [5].

Параметры	**CD**	**DVD**	**FMD**
Диаметр диска, мм	120	120	120
Вместимость, Гбайт	0,64	17,4	50,3
Число слоев	1	2 (на каждой стороне)	12
Расстояние между слоями, мкм	-	40	25+/-5
Общая толщина информационных слоев, мкм	0,11	2	275
Формат	CD	DVD	Модифицированный DVD
Расстояние между треками, мкм	1,6	0,74	0,8
Длина волны, нм	780	635-650	532

Таблица. Сравнительная сводная таблица

Заключение

В данной статье осуществлён обзор существующих технологий записи информации на различный типы оптических носителей. Описан процесс производства оптических носителей, и технология записи информации. Произведен сравнительный анализ характеристик оптических носителей информации.

Литература

1. Соболенко Р. « Три взгляда на одну историю » HARD'n'SOFT №5 .М.: Ил., 2004 – 29 с.
2. Жаров А. « Железо IBM 2004 » М.: 2004. – С. 5–35.
3. Сайт http://www.terralab.ru/print/storage/39182/
4. Олег Нечай 10.06.2005 г.
5. R. Grolf. «Blu-Ray systems» LaserFocusWorld. L: Newport Corporation, 2009 – 62 с.
6. Сайт http://www.ferra.ru/online/storage/25974/ Александр Радаев 21.07.2005 г.

УДК 535.326

РАСЧЕТ ЗАПРЕЩЕННОЙ ЗОНЫ ФОТОННОГО КРИСТАЛЛА

А.Н. Волченко, А.А. Киянов, И.В. Бейдина, А.В. Левшина
Научный руководитель – д.т.н., профессор В.Л. Ткалич

Представлен расчет запрещенной зоны фотонного кристалла. Определено основное свойство фотонного кристалла (ФК).

Ключевые слова: запрещённая зона, «Band gap»

Введение

В 1987 году Яблонович предложил рассмотрение нового класса оптических сред, так называемых фотонных кристаллов [1]. В [2] он определил термин «фотонный кристалл» как искусственную двух- и трёхмерную периодическую среду, взаимодействие фотонов с которой происходит аналогично тому, как взаимодействуют электроны с полупроводником. Решётка из перекрёстных диэлектрических полосок является «идеально» отражающей средой для световых волн определённого диапазона частот, который называется «запрещённой зоной». Световые волны этого диапазона не могут распространяться внутри решётки, а при наличии внутри неё полостей или нерегулярностей оказываются «захваченными» такими «ловушками». Создавая цепочки нерегулярностей, можно формировать световедущие каналы, при помощи которых открывается возможность изменять направление световых волн даже на острые углы.

Основная часть

Оптические свойства ФК можно описать тензорами диэлектрической проницаемости и восприимчивости, которые вследствие трансляционной симметрии среды являются периодическими функциями координаты $\vec{x}$ [3]:

$$\vec{\varepsilon}(\vec{x}) = \varepsilon(\vec{x} + \vec{a}), \mu(\vec{x}) = (\vec{x} + \vec{a}),$$

где $\vec{a}$ – любой произвольный вектор решетки. В случае трехмерной периодической среды, такой, как кристалл, периодичность решетки определяется элементарными векторами $\vec{a}_1$, $\vec{a}_2$ и $\vec{a}_3$. Среда остается инвариантной относительно перемещения на любой вектор $\vec{a}$, представляющий собой сумму целого числа этих векторов.

В случае одномерной периодической среды, тензор диэлектрической проницаемости ε удовлетворяет условию

$$\varepsilon(z) = \varepsilon(z + l\Lambda),$$

где Λ – период, а l – некоторое целое число. Предположим, что на одномерную периодическую немагнитную среду, представляющую собой последовательность чередующихся слоев двух прозрачных материалов, падает пучок лазерного излучения. Свет будет претерпевать отражение и преломление на каждой границе раздела. Пусть θ – угол падения. Интерференционные максимумы при отражении возникают при условии

$2\Lambda \cos\theta = m\lambda$, которое называется условием Брэгга [4]. Распространение электромагнитного излучения в периодических средах подчиняется волновому уравнению

$$\Delta \times (\Delta \times \vec{E}) - \omega^2 \mu \varepsilon \vec{E} = 0.$$

Поскольку среда является периодической, диэлектрический тензор ε можно разложить в ряд Фурье:

$$\varepsilon(\vec{z}) = \sum_{\vec{G}} \varepsilon_{\vec{G}} \vec{z} e^{-iG\vec{x}},$$

где G пробегает все векторы обратной решетки, включая $G = 0$. В одномерном случае

$$\vec{G} = l \times \vec{g} = \frac{(l2\pi)}{\Lambda}\vec{z}, \quad , l = 0, \pm1, \pm2, \pm3, \ldots,$$

$$\varepsilon(z) = \sum_l \varepsilon_l e^{-il\frac{2\pi z}{\Lambda}} .$$

В одномерной периодической среде вектор обратной решетки $\vec{g}$ параллелен оси *z*. Вектор электрического поля в этой периодической среде в общем случае можно выразить через интеграл Фурье:

$$\vec{E} = \int d^3k \vec{A}(\vec{k}) e^{-i\vec{k}\vec{x}} .$$

Отсюда, подставляя это в волновое уравнение, получаем

$$\vec{k} \times [\vec{k} \times \vec{A}(\vec{k})] + \omega^2 \mu \sum_{\vec{G}} \varepsilon_{\vec{G}} \vec{A}(\vec{k} - \vec{G}) = 0 \quad \text{для любого } k, \qquad (1.1)$$

где суммирование производится по всем векторам обратной решетки. Это условие представляет собой однородную бесконечную систему уравнений относительно неизвестных коэффициентов $\vec{A}(\vec{k})$. При условии, что частота ω задана, из уравнения (1.1) можно получить волновой вектор $\vec{k}$. Если среда однородна в *x*- и *y*- направлениях, т.е. если ε не зависит от *x* и *y*, то получаем следующее выражение для электрического поля $\vec{E} = e^{-i(k_x x + k_y y)} e^{-ik_z z} \vec{E}_k(z)$, (1.2)

где $\vec{E}_z(z)$ – периодическая функция от *z*. Существуют области значений ω, для которых k_z становится комплексным числом, и, следовательно, волна (1.2) становится затухающей. Падающее излучение от этих областей будет полностью отражаться. В диапазоне рентгеновского излучения это явление называется брэгговским отражением.

Для простоты будем считать далее, что волна распространяется в направлении оси *z* (т.е. $k_x = k_y = 0$) и вектор поля перпендикулярен волновому вектору, т.е. $(\vec{K} \times \vec{E}) = 0$. Кроме того, будем считать среду изотропной, т.е. считать, что ε_i является скалярной величиной. В этом случае уравнение (1.1) принимает вид

$$k^2 A(k) - \omega^2 \mu \sum_i \varepsilon_i A(k - l \times g) = 0 . \qquad (1.3)$$

Отсюда можно получить [4] в явном виде дисперсионное уравнение, определяющее зависимость $\omega(k)$

$$\left(k^2 - \omega^2\mu\varepsilon_0\right)\left\{\left((k-g)^2 - \omega^2\mu\varepsilon_0\right)\right\} - \left(\omega^2\mu|\varepsilon_1|\right)^2 = 0 , \qquad (1.4)$$

где ε_0 – нулевая, а ε_1 – первая Фурье компонента диэлектрического тензора. Условие Брэгга $|\vec{k} - \vec{g}| \sim \vec{k}$ точно выполняется при $k = (1/2)\, g = \frac{\pi}{\Lambda}$. При этом значении *k* из уравнения (1.4) получаем следующие два корня ω^2:

$$\omega_{\pm}^2 = \frac{k^2}{\mu(\varepsilon_0 \pm \varepsilon_1)}. \qquad (1.5)$$

Эти корни определяют границы спектральной полосы. При значениях частоты ω, попадающих в интервал между ω_+ и ω_- корни уравнения (1.4) для *k* являются комплексными числами, вещественная часть которых равна $\frac{\pi}{\Lambda}$. Волны при этом являются затухающими, а их спектральный диапазон называется «запрещенной зоной».

При частотах ω, лежащих вне этой запрещенной зоны, корни уравнения (1.4) для *k* являются вещественными и решения отвечают распространяющимся волнам. Ширина запрещенной зоны определяется величиной $\Delta\omega_{gap} = |\omega_+ - \omega_-|$ и в соответствии с (1.5), дается выражением $\Delta\omega_{gap} = \omega \frac{\varepsilon_1}{\varepsilon_0}$. Выше был рассмотрен случай, когда волна распространяется в направлении периодического изменения диэлектрической проницаемости. Для

произвольного направления распространения, т.е. когда k_x или $k_y \neq 0$, дисперсионное уравнение оказывается более сложным и зависит от состояния поляризации.

Запрещенная зона, связанная с брэгговским условием $\left|\vec{k} - \vec{g}\right| \approx \vec{k}$, определяется коэффициентом Фурье-разложения ε_l диэлектрической функции $\varepsilon(z)$. В общем случае существует запрещенная зона, связанная с каждым коэффициентом Фурье ε_i диэлектрической функции $\varepsilon(z)$. Условие Брэгга в этом случае можно записать

$$\left|\vec{k} - \vec{g}l\right| \approx k. \tag{1.6}$$

Принимая во внимание, что $k^2 \approx \omega^2 \mu \varepsilon_0$, получаем запрещенную зону при

$$k = l\frac{g}{2} = l\frac{\pi}{\Lambda}. \tag{1.7}$$

При этом ширина зоны определяется как $\left(\Delta\omega_{gap}\right)_l = \omega\dfrac{|\varepsilon_1|}{\varepsilon_0}$, где l – номер коэффициента Фурье-разложения. Если $l \neq 1$, то эти зоны называются запрещенными зонами высшего порядка, поскольку в соответствии с (1.6)–(1.7) они имеют места при более высоких частотах. Коэффициенты Фурье-разложения ε_1 обычно с ростом l уменьшаются. При этом соответствующие запрещенные зоны имеют небольшую ширину. На рис. 1.1 представлены дисперсионные зависимости $\omega(k)$ для основной запрещенной зоны (l=1) и запрещенных зон высшего порядка (l=2,3)

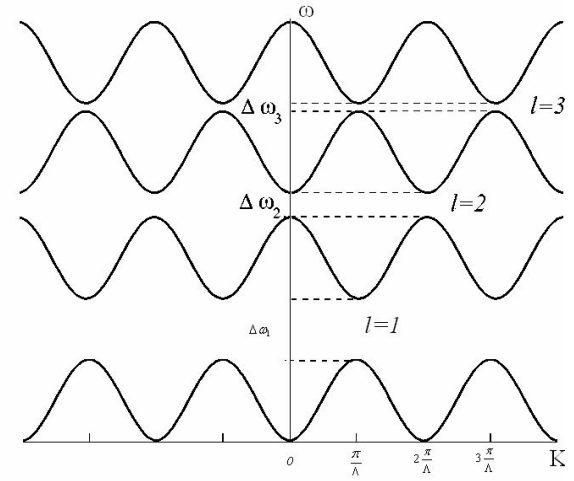


Рис. 1.1. Общий вид дисперсионных зависимостей w(k) для основной запрещенной зоны (l=1) и запрещенных зон высшего порядка (l=2,3)

Заключение

Таким образом, основным свойством ФК является наличие, так называемой, брэгговской запрещенной зоны, в которой в линейном приближении не происходит распространение света.

Литература

1. Eli Yablonovitch. Inhibited Spontaneous Emission in solid-state Physics and Electronics // Physical review letters. – Vol. 58. – No 20. – 2059–2062 (1987).
2. E. Yablonovitch. Photonic crystals.// Journal of Modern Optics. – Vol. 41. – No 2. – 173–194 (1994).
3. Борн М., Вольф Э. Основы оптики. – М: Наука. – 1973.
4. Ярив А., Юх Л. Оптические волны в кристаллах. – М: Мир. – 1987.

УДК 004.056

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СМАРТФОНОВ И КОММУНИКАТОРОВ

С.Ю. Колесникова
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

Смартфоны и коммуникаторы («умные» мобильные устройства) за последние несколько лет стали широко использоваться сотрудниками компаний. Они по производительности практически «догнали» персональные компьютеры 10–15-летней давности. Однако архитектура этих карманных мобильных устройств значительно отличается от архитектуры ноутбуков и настольных компьютеров. С внедрением новых технологий появляются новые угрозы информационной безопасности, поэтому в этой статье мы рассмотрим наиболее опасные угрозы, которые несут в себе эти «умные» мобильные устройства для корпоративных пользователей.

Ключевые слова: смартфоны, коммуникаторы, вредоносное ПО, хакеры, защитное ПО, мобильная безопасность

Введение

Современные «умные» мобильные обладают таким же функционалом как настольные компьютеры обладали несколько лет назад: возможность подключения к сетям 3G, WiFi, доступ в Интернет, электронная почта, множество приложений, большой объем памяти. Благодаря этим устройствам, стало возможным отправлять е-мэйлы, проверять почту, редактировать файлы, пользоваться корпоративными ресурсами независимо от того, где мы находимся. Тем не менее, многие пользователи относятся к этим «умным» мобильным устройствам как к обычным мобильным телефонам, не придавая значения той угрозе ИТ безопасности, которую коммуникаторы и смартфоны представляют. Особенно ощутима эта проблема среди корпоративных пользователей. Такими устройствами, как правило, пользуются топ-менеджеры, начальники отделов, руководители предприятий, но очень немногие управленцы осознают серьезность рисков использования корпоративных смартфонов и КПК для безопасности предприятия. Сотрудники как правило подключают их к WiFi сетям в Интернет-кафе, не устанавливают пароль доступа для защиты конфиденциальности корпоративной информации.

Основная часть

Специалисты по информационной безопасности доказали, что смартфон или коммуникатор может быть использован злоумышленниками как инструмент для атаки на корпоративную сеть, корпоративные ресурсы, для сканирования корпоративной сети и информации. Однако, в большинстве организаций даже не разработаны и не внедрены политики безопасного использования «умных» мобильных устройств.

Смартфоны и коммуникаторы с каждым годом становятся все более доступными, растущая популярность этих мобильных устройств способствует росту вирусных угроз. В целом число мобильных вирусов увеличивается не так лавинообразно как для ПК. Однако, эксперты, утверждают, что в будущем ситуация будет стремительно ухудшаться и мы столкнемся с массовым заражением «умных» мобильных устройств. Во-первых, число пользователей с каждым годом растет. Во-вторых, вычислительная мощность этих мобильных устройств последние годы росла по экспоненте. Как следствие, стремительно увеличивалась скорость передачи данных и число сетей, используемых мобильными устройствами, соответственно увеличилась быстрота (выросла и скорость) заражения.

Если настольные персональные компьютеры, как правило, оснащены одним портом 100BaseT Ethernet, то мобильное устройство может использовать соединение с сетями 3G, программа для синхронизации ActiveSync и синхронизационный кабель для

подключения к настольному компьютеру, карты для Wi-Fi в офисе, дома и в кафе. «Умные» мобильные устройства способны подключаться к нескольким сетям, поэтому инфекция одной из них может легко поразить и другие.

В отличие от традиционных компьютерных вирусов, мобильные вирусы используют другие каналы распространения. Они могут проникать на «умные» мобильные устройства посредством MMS-сообщения и сменных карт памяти, через Bluetooth соединение с другого телефона, через инфракрасное соединение, USB, WiFi с персонального компьютера, через WEB- или WAP-сайты.

В 2006м году появились первые шпионы для смартфонов и коммуникаторов. Такие программы-шпионы контролируют все действия с телефоном: какие сообщения приходят и уходят, какие звонки производятся, какие веб-сайты посещает пользователь – вся эта информация собирается и отсылается злоумышленнику. С тех пор ситуация с программами-шпионами и вредоносными программами только осложнилась.

Современные вредоносные программы способны сохранять и отсылать номера из телефонной книги, удалять и пересылать файлы, читать SMS, управлять фотокамерой и диктофоном, предоставлять злоумышленнику удаленный доступ к устройству, расходовать средства с мобильного счета пользователя, заставляя устройства отправлять SMS-сообщения и звонить на платные номера, загружая трафик без ведома пользователя. Более того эти вредители могут полностью блокировать работу «умного» мобильного устройства и частично блокировать работу сетей мобильных операторов посредством DDoS атаки и даже распределенных атак отказа в обслуживании.

Поскольку ресурсы смартфона сильно ограничены, в отличие от стандартного ПК, смартфон является более уязвимым к атакам отказа в обслуживании. Мобильные операторы тоже находятся в зоне риска. По данным аналитиков центра информационной безопасности Технологического института Джорджии (Georgia Tech Information Security Center) [2], в 2009 году зомбированные вирусами телефоны, управляемые злоумышленниками удаленно, будут использоваться для атак отказа в обслуживании на сети сотовых операторов, перегружая их.

В операционной системе Windows Mobile наиболее распространенными вирусами являются утилиты удаленного администрирования (backdoor) [3]. Как правило, это небольшой файл (около 5–10 Кб), который после запуска устройства записывается в каталог WindowsStartUp, получая таким образом управление при каждом запуске зараженного «умного» мобильного. При активности устройства он скрытно устанавливает соединение с Интернетом и отправляет IP-адрес жертвы по электронной почте автору, информируя его о том, что смартфон находится в сети и backdoor активен. Затем такая утилита открывает различные порты для приема команд, что позволяет автору вируса получить персональные данные пользователя или загрузить в зараженное устройство программу, уничтожающую все заложенные в него данные.

Установленное на «умный» мобильный антивирусное ПО серьезно истощает ресурс батареи и тормозит работу устройства, всилу ограниченности ресурсов памяти. В результате многие пользователи отказываются от использования антивирусных программ. Эксперты утверждают, что [4] ресурсов смартфона или коммуникатора никогда не хватит на полноценную фильтрацию входящего трафика, детектирование и блокирование вредоносного кода, в частности, встроенного в MMS-сообщения. Следовательно, для обеспечения должного уровня информационной безопасности необходимы совместные усилия не только разработчиков программного обеспечения, но и мобильных операторов и производителей устройств. Наиболее адекватным методом противодействия любым Web-угрозам является решение по обеспечению безопасной работы с Web-ресурсами в сети провайдера, предоставляющего корпоративным пользователям доступ в Интернет. Именно на стороне провайдера должна быть установлена многоуровневая система очистки почтового и Web-трафика от вредоносного ПО и нежелательной корреспонденции, а никак не на конечном устройстве, которым в данном случае является

смартфон или коммуникатор. Однако, по мнению авторов этой статьи, первым шагом должна стать на корпоративном уровне разработка грамотной политики безопасности. Специалисты по ИТ-безопасности должны разработать специальные политики для администрирования и использования «умных» мобильных устройств. В корпорациях необходимо выработать другой подход, стандарт управления, администрирования смартфонами и коммуникаторов чем обычными ПК и ноутбуками.

Некоторые политики могут быть внедрены с помощью технологий, а исполнение других политик зависит исключительно от компетентности сотрудников, поэтому важно регулярно обучать конечных пользователей и своевременно доводить до их сведения важную информацию. Более того, сотрудники часто приносят свои смартфоны (что не запрещается регламентом компании), копируют на них конфиденциальную информацию, подключаются к сети организации. Как правило, эти действия не запрещаются корпоративным регламентом. Такое поведение сотрудников может обернуться катастрофой для бизнеса в результате утечки конфиденциальной, секретной информации при потере устройства. Июльские исследования 2008 года показали [5], что 89% респондентов используют свои собственные смартфоны или смартфоны компании для доступа к корпоративной почте или другой информации компании, и больше половины опрошенных сказали, что компании, которые не выдают сотрудникам рабочие смартфоны, должны позволять им получать доступ и хранить информацию компании на собственных смартфонах. Основная сложность заключается в том, что системные администраторы не могут контролировать, конфигурировать устройства дистанционно. Удаленное администрирование корпоративных смартфонов и коммуникаторов становится доступным только после приобретения организацией специального программного обеспечения. Однако, многие компании в целях экономии средств не утруждают себя этой покупкой. В дополнение ИТ-администраторы должны постоянно проводить преднастройку смартфонов и коммуникаторов, устанавливать четкие наборы ПО, антивирусные и защитные программы, а также системы шифрования.

Заключение

Популярность «умных» мобильных устройств в корпоративных средах несет с собой серьезные угрозы информационной безопасности компании. При помощи создания и внедрения политик безопасного использования мобильных устройств и четкого учета того, какие типы устройств разрешены, а также установки защитных программ, возможно значительно минимизировать степень угроз.

Литература

1. Алексей Доля. Угрозы информационной безопасности глазами экспертов [Электронный ресурс] // КомпьютерПресс, 2006. Режим доступа свободный: http://www.compress.ru/article.aspx?id=16717&iid=776
2. Юрий Стрельченко. В этом году смартфоны станут вовлекаться в «зомби»-сети, полагают эксперты [Электронный ресурс] // Сотовик. Режим доступа свободный: http://www.sotovik.ru/news/smartfoni-vovlekut-v-zombi-seti.html
3. Максим Букин. Антивирусы для мобильных терминалов. [Электронный ресурс] // PCWEEK, 2007. Режим доступа свободный: http://www.itsec.ru/newstext.php?news_id=38492
4. Максим Букин. Антивирусы для мобильных терминалов. [Электронный ресурс] // PCWEEK, 2008. Режим доступа свободный: http://www.itsecurity.groteck.ru/newstext.php?news_id=51662
5. Marcia Savage. Smartphones opening up enterprise risks . [Электронный ресурс] // Information Security magazine, 2008. Режим доступа свободный: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1322575,00.html

УДК 004.056

СИСТЕМА МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ В ИГРОВОМ КОМПЛЕКСЕ

О.О. Зорькина, В.И. Зак
Научный руководитель – к.т.н., доцент И.Б. Бондаренко

В статье рассматривается система защиты информации в игровом комплексе. Главной задачей является: тотальный контроль игрового процесса на столах и разоблачение возможных мошеннических действий посетителей и/или сотрудников казино. Видеокамеры контроля столов должны хорошо отрабатывать блики, одновременно сохраняя изображение как в сильно освещенных, так и в темных областях. Стационарные камеры, транслирующие изображение с одного игрового стола, размещаются рядом так, чтобы на мониторе получалась единая картина.

Ключевые слова: микрофон, видео система, система контроля управления доступом

Введение

В условиях формирования общего экономического пространства перед руководством игровых комплексов особо остро встает задача сохранения коммерческой тайны. Любая утечка информации о протекающем игровом процессе может принести убыток. Особенно опасна утечка информации по оптическому каналу, который предоставляет большие возможности мошенникам. Из-за особенностей игрового процесса необходимо предъявлять особые требования к средствам и системам защиты информации.

Задачей данной работы является выявление особенностей защитных систем и мероприятий в игровом комплексе.

Постановка задачи

В типовой системе охранного телевидения (СОТ) главная задача – регистрация факта проникновения злоумышленника в охраняемую зону и оповещение охраны об этом событии. Для этого достаточно увидеть на экране силуэт нарушителя или услышать сигнал тревоги сработавшего детектора движения. В такой системе допустимо не различать цвета и не распознавать лица, главное – не пропустить проникновение объекта через охраняемую зону [1].

В игровом комплексе ситуация принципиально иная. У системы видеонаблюдения в игровых залах охранная функция второстепенна, но есть две другие, решающие следующие задачи: тотальный контроль игрового процесса на столах и разоблачение возможных мошеннических действий посетителей и/или сотрудников казино.

При проектировании СОТ необходимо учитывать, что:

- распознавание карт (или фишек) происходит в сложных условиях: свет от точечных светильников образует блики на глянцевых поверхностях карт, а сам уровень освещенности – низкий;
- часто красный цвет карт такой темный, что даже человеческим глазом при определенном освещении и угле зрения воспринимается как черный;
- игровой процесс происходит с большой скоростью;
- наблюдение должно осуществляется за несколькими десятками игровых столов;
- для эффективного «разбора» конфликтных ситуаций необходима детальная запись видео- и аудиоданных.

К сотрудникам, осуществляющим контроль за игровым процессом, предъявляются следующие требования:

- четко представлять себе не только смысл игры, но и знать о возможных мошеннических приемах игроков и собственных дилеров (крупье);

− уметь оперативно принимать сложные и ответственные решения при возникновении конфликтных ситуаций.

Пути решения задач

Для решения поставленных задач использование поворотных камер недопустимо, т.к. оператор может «наехать» на одну точку и безвозвратно утратить информацию с соседней части стола. Поэтому предлагается установить над каждым игровым столом две стационарные камеры с частично перекрывающимися полями зрения. Одна камера не позволяет при просмотре уверенно различать значения карт или фишек на всей площади стола, а также контролировать колесо (на столах с рулеткой). На карточных столах для игры в «Блек Джек» и «Покер» при постоянном наблюдении оператором одна камера может различать номиналы карт, но при записи даже на самый качественный регистратор разрешение неизбежно снижается, и данные могут быть потеряны.

Камера контроля столов должна хорошо отрабатывать блики, одновременно сохраняя изображение как в сильно освещенных, так и в темных областях. Наиболее подходящими являются телекамеры, которые обрабатывают сигнал по пикселям. В этом случае сигнал от каждого отдельного элемента изображения (пикселя) обрабатывается отдельно. Влияние соседних пикселей друг на друга минимально, что позволяет избежать «заплывания» и «столбов» на экране и, таким образом, расширить динамический диапазон.

Учитывая невысокий уровень освещенности столов, необходима достаточная чувствительность камеры: иначе, помимо снижения яркости и контрастности, изображение будет «шуметь», что приведет к невозможности эффективной цифровой обработки и сжатия и, как следствие, к значительным артефактам при просмотре записи.

В видеокамерах необходимо использовать варифокальные (для точной настройки поля зрения) объективы с ручной диафрагмой, так как освещенность столов постоянна. Чем выше светосила объектива, тем лучше.

Для уверенного различения карт и фишек телекамеры должны обладать помимо высокого разрешения еще и высокой цветопередачей.

Камера, используемая для видеонаблюдения в игровом зале, должна иметь максимум ручных настроек, таких как: баланс белого, электронный затвор и другие. Это позволит настроить параметры изображения таким образом, чтобы они соответствовали условиям конкретного зала, с его освещенностью, цветовой температурой осветителей, местами их расположения относительно телекамер и игровых столов и т.д.

Скоростные поворотные камеры (Speed Dome) в игровых залах казино используются для противодействия мошенничеству и в качестве дополнительных инструментов контроля самого игрового процесса. Поворотные камеры устанавливаются из расчета одна камера на один-два игровх стола; они позволяют оператору детально рассмотреть действия любого игрока или крупье с 2–3 сторон одновременно. При выборе поворотной камеры (как и стационарной) необходимо учитывать:

− условия ее работы;
− динамический диапазон;
− показатель кратности изменения угла зрения трансфокатора выбирается не менее 20 крат, без учета возможностей цифрового увеличения;
− наличие предустановок, позволяющих мгновенно возвращаться к просмотру наиболее ответственных зон;
− достаточная чувствительность;
− высокое разрешение ПЗС-матрицы;
− высокая надежность.

Микрофон

Рядом с каждой телекамерой следует поставить микрофон. Звуковое сопровождение поможет при возможных разбирательствах и придаст большую достоверность видеоматериалу. При установке микрофона нужно придерживаться правил:

- обеспечивать минимальный акустический контакт с потолком;
- максимально удалить или акустически изолировать микрофоны от систем кондиционирования и вентиляции;
- настроить чувствительность всех микрофонов на средний уровень, чтобы не перегрузить аудиовход регистратора и не перенастраивать каждый раз громкость аудиоколонок при переключении с канала на канал.

Средства регистрации и воспроизведения

Компьютерные системы записи на платах с аппаратной обработкой сигнала позволяют записывать 16–32 канала видео в режиме Real Time/D1 с синхронным аудио по каждому каналу на один видеосервер. При построении системы необходимо учитывать возможность подключения к серверу нескольких мониторов. Помимо серверов устанавливается несколько рабочих мест, чтобы на экран монитора (с диагональю не менее 19 дюймов) не приходилось более 9, а лучше 4 «картинок» одновременно. Стационарные камеры, транслирующие изображение с одного игрового стола, размещаются рядом так, чтобы на мониторе получалась единая картина.

Управление поворотными камерами осуществляется с пультов управления, связанных с мониторами через матричный коммутатор. Возможность одновременной работы нескольких пультов и мониторов, отсутствие сбоев и «зависаний» позволяет сохранять контроль над игровым залом даже при повреждении или сбое в работе видеорегистраторов, компьютерной сети и т.п. Видеосигнал подается непосредственно со сквозных выходов матричного коммутатора, без каких-либо усилителей-распределителей.

Компьютерная сеть системы видеонаблюдения должна быть отдельной, не связанной с общей сетью здания. Все элементы системы, включая сетевые коммутаторы и кабельное хозяйство, должны быть надежно защищены и недоступны для злоумышленников.

Для контроля и протоколирования действий операторов устанавливается одна-две телекамеры с микрофонами в помещении видеонаблюдения, у самих операторов не должно быть полномочий для работы с этими камерами.

Системами видеоконтроля должны быть помимо игрового зала оснащены кассы, зоны reception, коридоры и комнаты отдыха. Они должны охватывать прилегающую к входу уличную территорию и автомобильную стоянку.

Обязательными объектами, где должны устанавливаться камеры являются:

- центральный вход в казино;
- служебный вход для персонала;
- «черный», «пожарный» выходы;
- входы в раздельные помещения внутри комплекса;
- зал-холл, где собираются гости, когда только приходят;
- гардероб, вешалки;
- раздевалки персонала;
- стойка гардероба;
- все игровые столы;
- окошко кассы;
- помещение комнаты кассы;

- счетная комната;
- игровые автоматы;
- стойка бара, бар, подсобные помещения;
- места щитов электропитания, водоснабжения, вентиляции, теплообеспечения, автоматического управления дверями и разными процессами;
- места хранения ценностей, сейфы, витрины с ценностями, дорогостоящее оборудование, и т.д.;
- общий вид помещений, залов;
- все комнаты – тупики (замкнутые помещения);
- посты охраны;
- опасные участки: лифты, зеркала, стеклянные витрины, средства охраны и т.д.
- Дополнительно камеры устанавливаются на:
- автостоянки, въездные ворота, проходные;
- офисы менеджмента;
- вход в комнату видеонаблюдения;
- служебные помещения персонала, раздевалки, подсобные комнаты, кухню [2].

Наряду с системой видеонаблюдения необходимо использовать систему контроля доступа для ограничения и разрешения перемещения людей в помещениях, зданиях и по территории охраняемого объекта. Схема системы контроля доступа изображена на рис. 1.

Работа системы контроля доступа базируется на считывании кодов с идентификаторов и их сравнении с кодами (данными) заложенными в памяти системы, для определения права сотрудника на проход на охраняемую территорию.

Рис. 1. Схема системы контроля доступа

Всем сотрудникам компании, в которой установлена система контроля доступа, выдаются специальные электронные пропуска, например, RFID-ключи, представляющие собой пластиковые карты или брелоки, которые содержат персональные коды доступа. Считыватели, устанавливаемые у входа в контролируемое помещение, распознают код ключей. Информация поступает в систему контроля доступа, которая на основании анализа данных о владельце идентификатора, принимает решение о допуске или запрете прохода сотрудника на охраняемый объект, территорию или помещение. В случае разрешения доступа, система приводит в действие исполнительные устройства, такие как электромеханические замки, турникеты, автоматические шлагбаумы или приводы ворот. В противном случае, в зависимости от настроек и конфигурации системы, либо доступ на объект запрещается с последующей записью попытки входа в элек-

тронный журнал, либо происходит блокировка дверей, включается сигнализация и оповещается охрана.

СКД – это фискальная система, отслеживающая события, происходящие в системе СКУД. На основании полученных данных осуществляется контроль прохождения сотрудниками точек контроля, актуальная на сегодняшний день задача - учет рабочего времени. Базы данных позволяют оперативно разыскать сотрудника по последней точке контроля.

В состав системы входят:

- серверное оборудование и главный контроллер;
- считывающие устройства (считыватели карт, считыватели биометрических параметров, клавиатуры ввода цифрового кода);
- управляющие устройства (контроллеры) (блоки управления турникетом, калиткой, кнопка открывания замка);
- управляемые устройства (электромеханические и электромагнитные замки, турникеты);
- кабельная подсистема, строящаяся как на базе уже имеющейся структурированной кабельной системы (СКС) и системы передачи данных (СПД), так и на собственных магистралях;
- подсистема питания.

В состав аппаратно-программного обеспечения входят:

- электромеханические и электромагнитные замки;
- доводчики для дверей;
- шлагбаумы;
- ключи-идентификаторы и их считыватели;
- сервера-контроллеры и ПО к ним [3].

Заключение

Предложенная в работе интегрированная система безопасности, представляет собой совокупность технических средств охраны и обеспечения безопасности объекта. Система включает в себя: подсистему контроля и управления доступом, подсистему видеонаблюдения, целью которой является своевременное выявление и нейтрализация причин и условий, препятствующих реализации предприятием его основной задачи, – получению прибыли и поступательному развитию его капитала.

Описанные в работе средства должны соответствовать перечисленным требованиям и могут быть использованы при проектировании системы безопасности для современного игрового комплекса.

Литература

1. Герасименко В.А., Мецатунян М.В. Организация комплексной защиты информации на современных объектах//Вопросы защиты информации. – № 1. – 1995.
2. http://www.spektrsec.ru
3. http://www.dssl.ru

УДК 004.4

ФОРМИРОВАНИЕ И ПРИМЕНЕНИЕ ЭЛЕКТРОННЫХ СТРУКТУР ИЗДЕЛИЯ

Ю.В. Донецкая
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

В статье рассматривается метод автоматизации проектирования изделия, состоящий из двух частей. Первой частью метода является формирование электронных структур изделия при разработке схемотехнической составляющей изделия. Второй частью метода является применение сформированной структуры изделия для формирования и оформления технической документации средствами PLM систем.

Ключевые слова: автоматизация проектирования, САПР, структура изделия

Введение

В последнее время все большее распространение получают системы управления жизненным циклом изделия (PLM – Product Lifecycle Management). Руководство предприятий или проектных организаций, принимая требования конкурентной борьбы и контроля качества продукции, начинают внедрение систем управления.

Указанные системы позволяют решать задачи взаимодействия с автоматизированными системами, управления составом изделия, конфигурациями и версиями изделия и пр. [1, 2], что позволяет получать всю необходимую информацию об изделии в любой момент времени. Для этого в системах содержатся объекты – структуры изделия, являющиеся основными источниками информации.

Структуры изделия представляют собой, состав сборочной единицы, комплекса или комплекта и иерархические отношения (связи) между его составными частями и другие данные в зависимости от его назначения [3].

Таким образом, в ней содержатся все необходимые сведения об изделии, что свидетельствует о важности этого объекта. Однако следует отметить необходимость дальнейшей унификации использования PLM систем и их взаимодействия с системами автоматизации проектирования, так как в настоящее время не определен порядок автоматизации формирования структур изделия и их дальнейшего применения.

Учитывая это, в работе представлен метод формирования и применения электронных структур.

Особенности существующих методов

В настоящее время разработано несколько методов автоматизации проектирования. Они включают в себя методы формирования электронной структурой изделия (ЭСИ) на основе моделей сборок на этапе конструирования изделия [4–10] и методы применения электронных структур изделия для разработки табличных документов [11].

Как отмечалось в более ранних работах автора [12], этапу конструирования предшествует этап схемотехнического проектирования, для которого еще не проработан метод автоматизации формирования ЭСИ. Это является существенным недостатком, так как при этом возникает большое число ошибок, которые очень трудно отследить.

Еще одним недостатком является отсутствие универсального метода применения ЭСИ, так как все существующие методы разработаны для определенных систем управления данными изделия (Product Data Management – PDM), что затрудняет применения методов в других PDM-системах.

Перечисленные недостатки обусловили необходимость разработки универсального метода автоматизации формирования и применения электронных структур изделия, что и описано в статье.

Метод формирования и применения электронных структур изделия

Метод формирования и применения ЭСИ состоит из нескольких, связанных между собой, частей. Это проектирование изделия и его составных частей, формирование ЭСИ и разработка технической документации.

Рассмотрим подробнее проектирование изделия и формирование ЭСИ, как две связанные части.

При проектировании изделия выделят три этапа [12] – проектирование схемотехнической, конструкторской и программной составляющей изделия, наиболее интересным из которых является проектирование схемотехнической составляющей. В этом случае выделяют: выбор элемента и помещение элемента на схему. Выбор элемента представляется схемой на рис. 1.

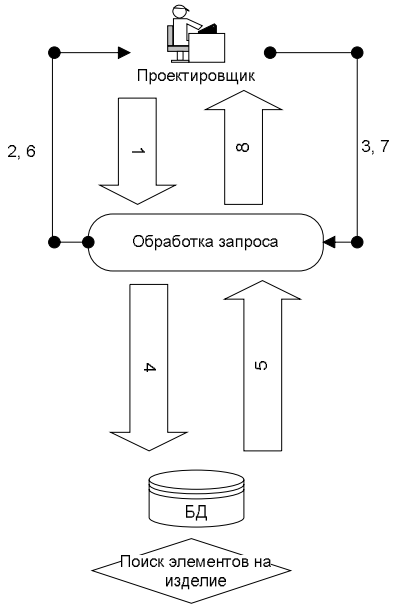


Рис. 1. Схема выбора элементов

Числовые обозначения на схеме имеют следующие значения.

1. Запрос на получение элементов. Информационный поток представляет действие проектировщика по получению элемента для установки на проектируемую схему. Получение элемента (в данном случае, это попытка получить элемент) производится с помощью специализированного интерфейса, встраиваемого в электронную САПР, используемую разработчиком.

2. Запрос на получение наименования, разрабатываемого изделия. Информационный поток, представляет собой отклик системы на запрос проектировщика.

3. Наименование изделия. Отклик проектировщика на запрос системы. Содержит наименование проектируемого изделия. Необходим, так как для изделия могут существовать перечни ограничения применения элементов.

4. Запрос элементов по наименованию изделия. Обработчик запросов производит обращение (в виде запроса) к базе данных о получении всех возможных элементов для проектирования заданного изделия.

5. Набор элементов. После обработки поступившего запроса из базы данных, в обработчик запросов передается информационный поток, содержащий набор всех элементов, которые можно использовать при проектировании изделия.

6. Сформированный список элементов. Элементы, полученные из базы данных, передаются в интерфейс проектировщика.

7. Запрос элемента. Проектировщик, используя информацию об элементах, разрешенных к применению в разрабатываемом изделии, «запрашивает» элемент, который необходимо поместить на схему.

8. Элемент. Обработчик запросов, обработав поступивший запрос об элементе, передает информацию о нем в интерфейс схемотехнической САПР. Данные представляю собой условно-графическое обозначение этого элемента.

Представленная последовательность потоков данных, которыми обмениваются проектировщик и система автоматизации, позволяет сформировать список данных о применяемых элементах, которые записываются в определенную область для последующего их применения при формировании ЭСИ. Ее формирование производится непосредственно после завершения работы над схемой.

Описанный подход позволяет корректировать не только схемы работы изделия, но, на основе их, и ЭСИ.

После того как ЭСИ полностью сформирована, ее данные можно использовать для автоматизации формирования табличных документов. Этот процесс представлен на рис. 2.

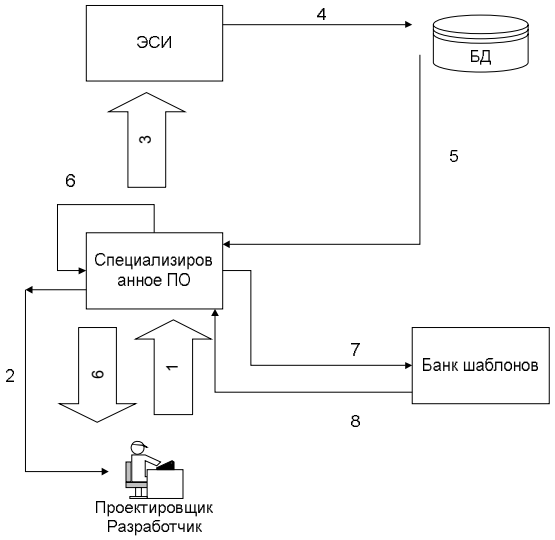


Рис. 2. Схема автоматизации формирования табличных документов

Рассмотрим подробнее потоки данных.

1. Запрос на формирование документации. Информационный поток представляет действие проектировщика или разработчика по обращению к специализированному программному обеспечению (СПО) для формирования табличной текстовой документации.

2. Запрос об указании вида разрабатываемой документации. Поток данных отклика СПО на запрос проектировщика или разработчика. Запрос обусловливает указание той табличной технической документации, которую необходимо сформировать.

3. Получение данных для разрабатываемой документации. Для документа заданного вида формируется запрос к ЭСИ на получение данных для него.

4. Запрос к БД на получение требуемой документации. Поскольку ЭСИ является структурой, данные которой хранятся в виде записей в БД, то запрос о получении нужной информации адресуется к БД.

5. Список данных. В ответ на сформированный запрос к базе данных получаем перечень информации, необходимый для генерации документа, указанного вида.

6. Компоновка данных в последовательности, определяемой видом документации. Результаты обработки запроса передаются в СПО. Здесь производится их компоновка, согласно требованиям вида документации.

7. Запрос шаблона документа. В определенной области, известной в СПО, хранятся шаблоны табличных документов, которые могут быть сформированы по запросу проектировщика. После того, как все данные скомпонованы, СПО запрашивает шаблон документа, требуемого вида. На этом же этапе производится формирование реквизитной части документа.

8. Получение запрашиваемого шаблона. Из хранилища шаблонов в СПО передается шаблон, содержащий форму табличного документа. Подготовленные данные и реквизитная составляющая документа записывается в шаблон и объект системы управления.

9. Получение документации. После того, как документация сформирована, она отображается на экране монитора рабочего места проектировщика или разработчика.

Такая последовательность обмена данными предполагает, что документация будет не только сформирована, но и добавлена в ЭСИ, как ее составная часть.

Заключение

Рассмотрен метод формирования электронных структур изделия на этапе схемотехнического проектирования изделия, позволяющий вводить данные об изделии в ЭСИ после того, как они были определены в схеме. Такой метод подразумевает, что при корректировке схемы будет откорректирована и ЭСИ, что уменьшит число ошибок, вносимых в ЭСИ при ее формировании «вручную».

Еще одним результатам, полученным при разработке метода, является применение структуры для автоматизации формирования табличных документов, что позволяет существенно сократить не только время на разработку таких документов, но и сократить количество допускаемых при этом ошибок.

Литература

1. Норенков И.П., Кузьмик «Информационная поддержка наукоемких изделий. CALS – технологии». – М.: Издательство МГТУ им. Н.Э.Баумана, 2002. – 302 с.
2. Яцкевич А., Страузов Д. Построение интегрированной информационной среды предприятия на основе системы управления данными об изделии PDM STEP SUITE. – САПР и графика. – №6. – 2002.
3. ГОСТ 2.053 – 2006. Электронная структура изделия.
4. Буланов А., Шевченко О., Гусаров С. «Pro/ENGINEER Wildfire 3. Первые шаги». – М.: Издательство «Поматур», 2008. – 238 с.
5. Сайт компании «Би-Питрон» [Электронный ресурс]/CATIA V5 – Режим доступа http://www.bee-pitron.ru, свободный.
6. Сайт компании «IBM» [Электронный ресурс]/CATIA V5 – Режим доступа http://www.ibm.com/catia/, свободный.
7. Сайт компании «Солвер» [Электронный ресурс]/Pro/ENGINEER – Режим доступа http://www.solver.ru, свободный.
8. Сайт компании «Simens» [Электронный ресурс]/Pro/ENGINEER – Режим доступа http://www.simens.com, свободный.
9. Сайт компании «Autodesk» [Электронный ресурс]/Autodesk Inventor – Режим доступа http://www.autodesk.ru, свободный.
10. Автоматизация проектирования в Казахстане [Электронный ресурс]/Autodesk Inventor 2009 – Режим доступа http://www.cad.kz, свободный.
11. Мигунов В.В. «Модель табличных документов для работы с электронными каталогами и спецификациями в САПР».
12. Донецкая Ю.В. «Метод формирования электронного описания изделия». Сборник трудов V всероссийской межвузовской конференции молодых ученых.

УДК 620.19

ДИАГНОСТИРОВАНИЕ ВЫСОКОТЕМПЕРАТУРНЫХ ПРОТЯЖЕННЫХ ОБЪЕКТОВ МЕТОДОМ АКУСТИЧЕСКОЙ ЭМИССИИ

Н.П. Лузина
Научный руководитель – д.т.н., профессор В.Л. Ткалич

При помощи метода акустической эмиссии можно диагностировать протяженные высокотемпературные объекты в процессе их эксплуатации. Кроме того, с использованием метода акустической эмиссии предоставляется возможность выполнения 100% обследования оборудования с выявлением зон концентрации напряжений и дефектов на раннем этапе их развития. В работе отражены экспериментальные и расчетные данные, позволяющие составить более полную картину о методике диагностировании высокотемпературных протяженных объектах.

Ключевые слова: акустическая эмиссия, давление, высокотемпературные волноводные преобразователи акустической эмиссии, напряженно-деформированное состояние, пьезоматериал, волновод

Проблема обеспечения безопасной эксплуатации и эффективности работы сложных технических систем и оборудования опасных производственных объектов имеет в настоящее время особое значение. Существенный износ основного промышленного оборудования предполагает поиск новых подходов к решению задач, стоящих перед технической диагностикой.

Тенденция перехода от традиционной дефектоскопии к технической диагностике с применением комплексного подхода, включающего: определение параметров дефектов, оценка распределения внутренних (остаточных) напряжений, определение фактических структурно-механических характеристик металла сдерживается, в первую очередь, низкой эффективностью существующих методов и средств контроля напряженно-деформированного состояния оборудования. Например, в работе [1] отмечается, что на современном этапе ни одно из испытанных средств определения напряжений (было испытано около 10 различных приборов контроля напряжений) в реальных условиях эксплуатации трубопроводов не может обеспечить достоверных сведений о напряженно-деформированном состоянии (НДС).

Анализ возможностей известных методов контроля и измерений напряжений и деформаций в основном металле изделий и сварных соединениях оборудования и конструкций позволяет назвать их существенные недостатки. Основными недостатками являются:

– невозможность использования большинства методов в области пластической деформации;

– локальность контроля, их непригодность для контроля протяженных конструкций;

– не учитывается изменение структуры металла;

– контроль выполняется только на поверхности изделий, невозможность оценки глубинных слоев металла и металла сварных соединений;

– требуется построение градуированных графиков на предварительно изготовленных образцах;

– требуется подготовка контролируемой поверхности и объектов контроля (зачистка, активное намагничивание, клейка датчиков и прочее);

– сложность определения положения датчиков контроля по отношению к направлению действия главных напряжений и деформаций, определяющих надежность конструкции.

Работа металла оборудования в основном определяется скольжением дислокаций и сдвиговой деформацией. При этом накопление усталостной повреждаемости металла во многих случаях происходит в условиях рабочей нагрузки. Спрашивается, каким образом традиционные методы контроля напряжений могут оценить фактическое НДС конструкции, когда в общем случае неизвестны зоны концентрации напряжений, обусловленные сдвиговой деформацией. Очевидно, что только «пассивные» методы диагностики НДС могут ответить на поставленные вопросы и являются наиболее пригодными для практики.

К пассивному методу НК, использующему энергию излучения конструкций, прежде всего, следует отнести метод акустической эмиссии (АЭ).

Этот метод получили в настоящее время наибольшее распространение на практике для ранней диагностики повреждений оборудования и конструкций.

Имея полную информацию о выявленных дефектах, можно без особых затруднений решить задачу определения объема восстановительных работ, необходимого для доведения ресурса работоспособности узлов до требуемого уровня.

Только в отдельных, наиболее ответственных отраслях промышленности (например, атомная и тепловая энергетика) имеются специальные инструкции о порядке и периодичности контроля и продлению срока службы оборудования [2–4]. И даже в этих передовых отраслях (с точки зрения организации контроля за состоянием металла оборудования) существует проблема определения предельного состояния металла и оценки индивидуального ресурса оборудования [5].

В данной работе рассматривается случай применения метода акустической эмиссии для диагностирования высокотемпературных протяженных объектов, применяемых в энергетике.

Метод акустико-эмиссионного неразрушающего контроля основан на регистрации и последующей обработке параметров акустических сигналов ультразвукового диапазона, и реализуется в процессе активного нагружения контролируемого объекта. Для проведения АЭ диагностики к объекту контроля должны быть приложены статические и/или динамические нагрузки повышением давления при гидравлических или пневматических испытаниях. Основной задачей АЭ-контроля является оценка технического состояния объекта по параметрам сигналов, отображающих информацию об источниках АЭ.

Диагностирование высокотемпературных протяженных объектов – это весьма сложная задача, как с точки зрения ее реализации, так и с экономически дорогой ее составляющей. Стали в трубопроводах испытывают постоянные вибрационные нагрузки и периодические перегрузки и поэтому необходимо проводить исследования повреждаемости конструкционных сталей на различных стадиях деформирования с привлечением метода акустической эмиссии.

В нашем случае необходимо использовать высокотемпературные преобразователи АЭ. Основной проблемой при создании таких преобразователей является выбор высокотемпературных пьезокерамических материалов. Следует выбирать материал по рабочей температуре с учетом значений пьезомодуля (желательно высокими) и диэлектрической проницаемостью (малой). Контакт преобразователя АЭ с нагретым контролируемым объектом можно осуществлять тремя способами: сильным поджатием преобразователя к объекту, приклеиванием преобразователя высокотемпературным клеем и применение преобразователя с волноводом [6].

Для реализации поставленной задачи необходимо:

1. Составить техническое задание для высокотемпературных волноводных преобразователей акустической эмиссии (ВВ ПАЭ):

1.1. Конструктивно ВВ ПАЭ должен состоять из:

- волновода (материал – сталь 12Х1МФ), привариваемого одним концом к наружной поверхности трубопровода;
- преобразователя акустической эмиссии (ПАЭ), устанавливаемого на другой конец волновода;
- устройства соединения ПАЭ и волновода.

1.2. Длина волновода определяется, исходя из условий эксплуатации, при обеспечении максимальной температуры в месте установки ПАЭ не более +300ºС.

1.3. Устройство соединения должно обеспечивать необходимые прочность крепления и акустический контакт между волноводом и ПАЭ.

1.4. ПАЭ может крепиться как на волновод, так и самостоятельно на электромагнитных держателях.

1.5. ПАЭ должен иметь (по возможности) встроенный тестовый канал, обеспечивающий возможность проверки функционирования приёмного акустического канала.

1.6. ПАЭ должен иметь размещаемый соосно с волноводом кабель, неразъёмно соединённый с корпусом преобразователя.

1.7. Кабель должен быть помещён в металлорукав.

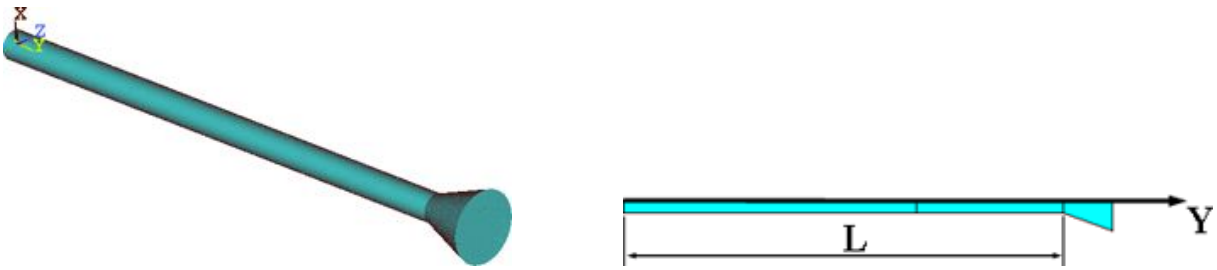
1.8. Длина кабеля от датчика до усилителя составляет около 0,5 метра.

1.9. Резонансная частота ВВ ПАЭ должна находиться в диапазоне 30…50 кГц.

1.10. В полосе частот затухание акустико-эмиссионного сигнала должно составлять не более 40 дБ на расстоянии не менее 100 м.

1.11. Чувствительность (коэффициент преобразования) ВВ ПАЭ на резонансной частоте должна быть максимально возможной и определена для различных длин волновода.

2. Получить необходимые размеры волновода, для чего была решена задача распространения тепла в стержне при помощи программного комплекса ANSYS. Для экспериментальной модели был взят стержень из стали 12Х1МФ (рис. 1) и выведена закономерность затухания температуры в зависимости от распространения тепла по всей длине волновода.



а) б)

Рис. 1. а) трёхмерная модель; б) расчётная модель

Исходные данные взяты следующие:

Для обеспечения распространения в волноводе первой моды продольной волны Лемба необходимо выбирать диаметр d из условий $d \le 0{,}4 \times {c_L}/{f}$, где c_L – скорость продольной волны, f – рабочая частота [6].

1. Диаметр стержня 8 мм, диаметр конуса 20 мм, L = 200 мм, температура воздуха 80°С.
2. Коэффициенты теплопроводности (k) для стали 12Х1МФ в зависимости от температуры приведены в табл. 1

Температура (T), °C	k, Вт/(м·°C)
20	44,0
100	44,2
200	43,7
300	41,8
400	39,7
500	37,2
600	35,0

Таблица 1. Зависимость коэффициента теплопроводности (k) от температуры

3. Коэффициент теплоотдачи от наружной поверхности горизонтальной трубы (стержня) к воздуху в условиях естественной конвекции при T = 80°C: h = 4,9416 Вт/(м^2·°C).

Результаты расчёта приведены на графике (рис. 2) и сведены в табл. 2.

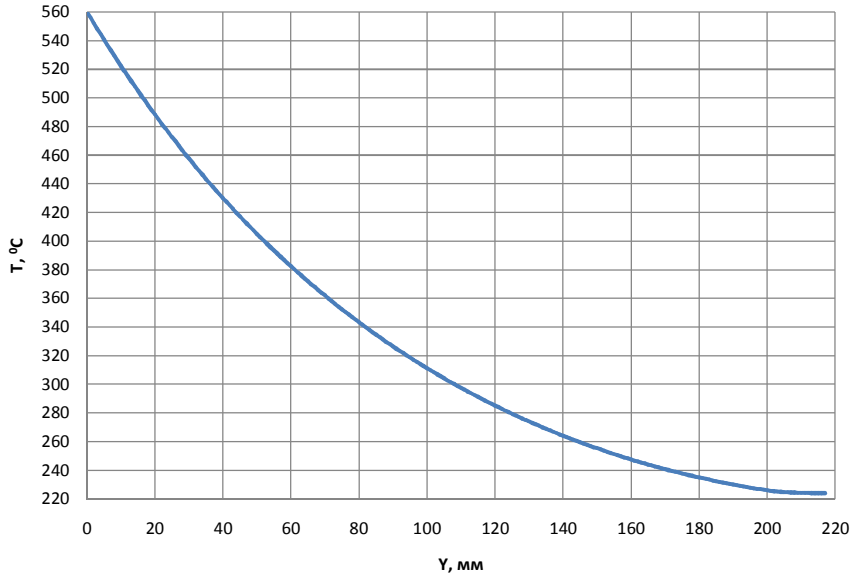


Рис. 2. Зависимость длины от температуры

Y, мм	T, ^{0}C
20	488,3
40	430,0
60	382,4
80	343,3
100	311,3
120	285,2
140	264,2
160	247,6
180	235.0
200	226,0
217	224,0

Таблица 2. Значения зависимости длины от температуры

Из полученных результатов можно сказать следующее: при длине стержня 217 мм температура на конце волновода достигает лишь 224ºС и это означает, что при разработки ВВ ПАЭ мы можем выбирать пьезоматериал с диапазоном рабочих температуры до 250ºС.

Волноводы являются акустическими дисперсионными системами, сигналы АЭ, распространяясь по ним, меняют свои параметры. Это вносит определенные искажения в получаемую через волновод информацию, однако, для производственного контроля использование волноводов допустимо, а в нашей конкретной задачи без них обойтись невозможно.

Следующим этапом работы является проработка метода диагностирования протяженных объектов [7, 8]. Важной особенностью контроля является тот факт, который показывает, на сколько близко необходимо устанавливать датчики АЭ друг от друга.

Максимальная длина участка трубопровода, охватываемого контролем одного акустико-эмиссионного датчика, составляет 6–8 м (т.е. 3–4 м по длине трубопровода от места установки датчика в обе стороны) [8]. Если датчики ставить на более дальнее расстояние, то возникают сильные помехи от среды, и их фильтрация будет убирать полезные сигналы, что для нас неприемлемо.

Однако, существуют экспериментальные данные, полученные при диагностировании подобных объектов: при давлении 1,6 МПа и температуре ниже 300ºС датчики АЭ можно ставить на расстоянии 40–65 метров друг от друга. Но это расстояние сопоставимо для труб с диаметром 279–426 мм. При уменьшении диаметра расстояние так же необходимо уменьшать в связи с появляющимися помехами.

Вывод

В работе отражены экспериментальные и расчетные данные, позволяющие составить более полную картину о методике диагностировании высокотемпературных протяженных объектах.

Главным выводом данной работы является то, что при помощи предложенного метода контроля можно диагностировать протяженные высокотемпературные объекты в процессе их эксплуатации. А это необходимо для стратегически важных объектов, от отключения которых зависит работа целых цехов и даже заводов и, как следствие, экономически невыгодно для любого предприятия.

Кроме того, с использованием метода акустической эмиссии предоставляется возможность выполнения 100% обследования оборудования с выявлением зон концентрации напряжений и дефектов на раннем этапе их развития. Имея полную информацию о выявленных дефектах, можно решить задачу определения объема восстановительных работ, необходимого для доведения ресурса работоспособности оборудования до требуемого уровня.

Направлением дальнейших исследований будет поиск зависимостей между такими основными параметрами, как давление, температура, материал и диаметр трубопроводов, а так же моделирование этих зависимостей при помощи различных программных комплексов.

Литература

1. Дубов А.А., Демин Е.А., Миляев А.И., Стеклов О.И. Контроль напряженно-деформированного состояния газопроводов // Газовая промышленность. – 2002. – №2. – С. 58–61.
2. РД 10-577-03. Типовая инструкция по контролю металла и продлению срока службы основных элементов котлов, турбин и трубопроводов тепловых электростанций. – М.: ОРГРЭС. – 2003.
3. РД ЭО 0186-00. Методика оценки технического состояния и остаточного ресурса сосудов энергоблоков АЭС. – М.: Концерн "Росэнергоатом". – 1999. – 75 с.

4. РД ЭО 0185-00. Методика оценки технического состояния и остаточного ресурса трубопроводов энергоблоков АЭС. – М.: Концерн "Росэнергоатом", 1999. – 63 с.
5. Концепция технического перевооружения энергообъектов электростанций РАО "ЕЭС России" в период до 2015 года. – М: Департамент науки и техники РАО "ЕЭС России". – 2001. – ноябрь.
6. Иванов В.И., Власов И.Э. // Неразрушающий контроль. Том 7. – 2-е изд., перераб. и испр. – М.: «Машиностроение». – 2006. – С. 213–216.
7. РД 34.17.444-97: Методика проведения акустико-эмиссионного контроля при испытаниях трубопроводов тепловых сетей на герметичность и плотность. – М.: Департамент науки и техники РАО «ЕЭС России». – 1997.
8. РД 34.17.443-97: Методика проведения акустико-эмиссионного контроля паропроводов в процессе эксплуатации. – М.: Департамент науки и техники РАО " ЕЭС России ", 1997. – 2 с.
9. ПБ 03-593-03. Правила организации и проведения акустико-эмиссионного контроля сосудов, аппаратов, котлов и технологических трубопроводов. – М.: Госгортехнадзора России от 09.06.03 г. – № 77.
10. ГОСТ 27.655-88. Акустическая эмиссия. Термины, определения и обозначения.
11. МР 38.18.015-94. Методические рекомендации по акустико-эмиссионному контролю сосудов, работающих под давлением, и трубопроводов нефтехимических производств. Согласованы с Госгортехнадзором РФ 06.06.94 г.
12. Acoustic Emission: Special Publication STR 505. Philadelphia: ASTM. – 1972. – 337 p.
13. Клюев В.В., Соснин Ф.Р., Филинов В.Н. и др. // Машиностроение: Энциклопедия. Т. III-7: Измерения, контроль, испытания и диагностика – М.: Машиностроение, 1997. – С. 460.
14. Юдин А.А., Иванов В.И. Связь сигнала акустической эмиссии с пластической деформацией металла // Проблемы прочности – 1986, № 6. – С. 103–105.

УДК 004.514.6

ОБЗОР МЕТОДОВ ВИЗУАЛИЗАЦИИ ОНТОЛОГИЙ

А.Н. Злобин
Научный руководитель – к.т.н., доцент Д.И. Муромцев

Приводится обзор различных методов визуализации онтологий и методов визуализаций подобных структур (графов, деревьев и т.п.). Строится классификация этих методов. В заключение предпринимается попытка сформулировать основные преимущества и недостатки выделенных классов методов для различных целей.

Ключевые слова: онтология, визуализация, таксономия, дерево, граф

Введение

Методы могут быть сгруппированы различными способами: по способу представления, размерности изображения, способа взаимодействия с пользователем. Для задач данного обзора методы были разбиты на следующие группы по типам визуализации:

- Иерархический список.
- Узлы-связи и деревья.
- Масштабируемые.
- Заполнение пространства.
- Фокусирование и искажение.
- Трёхмерные ландшафты.

Методы, попавшие в одну из категорий могут содержать в себе черты другой группы. В таком случае они относились к группе, признаки которой доминируют. Дополнительно методы в каждой группе разделены на 2-х и 3-х мерные. 2-х мерные методы используют поверхность экрана как плоскость без каких-либо элементов глубины. 3-х мерные методы вводят еще одно измерение для того, чтобы приблизиться к представлению реального мира или улучшить взаимодействие с пользователем. Также некоторые 3-х мерные методы позволяют пользователю передвигать и вращать объекты в виртуальном мире и/или перемещаться в нём.

Иерархический список

Многие инструменты визуализации онтологий, в том числе Protege [1], OntoEdit [2], Kaon [3] и некоторые другие, предлагают в качестве основного способа визуализации представления в стиле Windows Explorer. При этом таксономия онтологии представляется как дерево.

Узлы-связи и деревья

Методы этой категории отображают онтологию как набор соединяющихся узлов, представляющих онтологию. Пользователю обычно предоставляется возможность разворачивать и сворачивать узлы и поддеревья для управления детализацией информации.

2 мерные

OntoViz [4] – плагин визуализации для Protege, использует библиотеку GraphViz для создания простого представления онтологии в виде двумерного графа. Есть возможность для каждого класса отображать имя, свойства, наследование и роли. Индивиды отображаются отличными от классов цветами.

IzaVis [5] – визуальная среда для создания и редактирования rdf-онтологий в форме направленных графов. Графы визуализируются с помощью эллипсов, прямоугольников и рёбер между ними. Узлами являются классы, индивиды и значения свойств, свойства представляются как рёбра графа.

SpaceTree [6] – визуализатор деревьев, выполненный на основе диаграмм узел-связь с использованием сворачивания узлов, которые не могут быть отображены. В данной реализации свёрнутые узлы представляются специальными иконками, затенение кото-

рых пропорционально количеству свёрнутых узлов, а ширина глубине скрываемого поддерева.

3 мерные

OntoSphere [7]. Предлагает визуализацию типа узел-связь, и использует три различных представления онтологии для представления пользователю обзора или деталей, в зависимости от его потребностей. Корневая сцена представляет сферу с расположенными на её поверхности классами верхнего уровня, представляемых как малые сферы. Она визуализирует не таксономию, а ролевые отношения между классами. Цвет и размер используются для выделения поддеревьев и их размера. Сцена дерева отображается по левому щелчку на классе и показывает класс и его поддерево.

Масштабируемые

Grokker. Система для отображения карт знаний. Она предлагает графическое представление для информации типа результатов web-поиска или файлового поиска. Механизм кластеризации показывает документы как наборы вложенных диаграмм Вена. Пользователь может перемещаться по иерархии простыми кликами на круге. Когда круг выделен он увеличивается, делая своё содержание видимым. Круги заполнены цветом, подсказывающим, что они находятся на нижних уровнях иерархии. На нижних уровнях иерархии пользователь может выбирать документы для просмотра в большом окне.

Jambalaya [8]. Плагин визуализации для Protege, использующий SHriMP(Simple Hierarcical Multi-Perspective). SHriMP использует вложенный просмотр графа и концепцию вложенных перемещаемых представлений.

CropCircles. Визуализация, представляющая дерево иерархии классов в виде набора окружностей. Узлам выделяется соответсвующее место для того, чтобы обеспечить размещение всех поддеревьев. Единственный потомок помещается как концентричекий круг в своего родителя, несколько потомков помещаются в родителя от больших к меньшим. Пользователь может щелчком по окружности выделить её и просмотреть список непосредсвенных потомков соответсвующего узла.

Заполнение пространства

TreeMaps. Использует 2-х мерный подход к заполнению пространства для представления иерархий, с помощью прямоугольной области с прямоугольным разбиением. Размер и цвет используются для представления данных. Пользователь может более детально просмотреть интересующую его область двойным щелчком, при этом она увеличится до размера всего окна.

Information Slices. Использует один или несколько дисков для компактного двумерного представления иерархий. Каждый диск представляет многое уровни иерархии, обычно на каждом диске размещается 5–10 уровней иерархии.

Фокусирование и искажение

2 мерные

TGVizTab. Встраивает визуализацию Touchgraph в Protege. Touchgraph – это среда с открытым исходным кодом для создания и просмотра графов. Она размещает семантически схожие узлы рядом. Это визуализация позволяет пользователю выполнять навигацию постепенно делая видимыми разные части графа. Также возможно сворачивать и разворачивать узлы. Кроме того пользователь имеет полный контроль над цветом и видимостью отдельных типов связей, может менять степень увеличения или делать граф гиперболическим.

3 мерные

3D Hyperbolyc Tree. Было создано для визуализации вёб-сайтов, но использовалось как файловый браузер. Он представляет дерево в гиперболическом пространстве для достижения большей плотности отображаемых данных. Узлы дерева размещаются на поверхности сферы.

Информационные ландшафты

File system navigator. Создавался как трёхмерный файловый обозреватель для UNIX-систем. Высота узлов на плоскости представляет количество содержащихся в них файлов. При взгляде сверху узлы образуют двухмерное дерево, представляющее иерархию файловой системы. Выбор узла подсвечивает его, а двойной щелчок открывает его для детального просмотра.

Harmony Information Landscape. Был разработан для гипертекста и упорядочивает узлы, представляемые как трёхмерные объекты, непосредственно на плоскости. Объекты при этом отличаются цветом и размером в зависимости от содержимого. Кроме того, так как документы гипертекстовые, между ними также отображаются связи. В случае с онтологией аналогично могут визуализироваться роли.

Заключение

Для наглядности и простоты анализа все исследованные методы визуализации были собраны в таблицу и охарактеризованы по набору критериев:

➔ Простота восприятия – показывает насколько легко понять визуализируемый объект (онтологию, таксономию и т.д.) «с первого взгляда».

➔ Детализация представления – характеризует насколько детально и полно отображается структура объекта.

➔ Скорость навигации – показывает насколько быстро возможно перемещение от одного концепта к другому через определённое количество уровней таксономии или партономии.

➔ Потребность в пространстве – отражает насколько масштабной должна быть область визуализации для полноценного её восприятия.

➔ Полнота представления – показывает насколько полно отображается объект «крупным планом», т.е. все ли части попадают в поле обзора одновременно.

Название метода	Простота восприятия	Скорость навигации	Потребность в пространстве	Детализация представления	Полнота представления
Иерархические списки	Высокая	Средняя	Низкая	Низкая	Высокая
Узлы и связи	Высокая	Средняя	Средняя	Высокая	Средняя
Масштабируемые	Средняя	Низкая	Высокая	Средняя	Средняя
Заполнение пространства	Средняя	Низкая	Высокая	Средняя	Высокая
Фокус и искажение	Высокая	Высокая	Средняя	Низкая	Низкая
Трёхмерные ландшафты	Средняя	Высокая	Высокая	Средняя	Средняя

Таблица. Сравнение различных методов визуализации

Полученная классификация и оценки каждого из классов были практически применены при разработке системы разработки порталов на онтологической основе Ontolinge. А также использовались как составная часть пояснительной записки к дипломного проекту.

Литература

1. Protégé is a free, open source ontology editor and knowledge-base framework [электронный ресурс] – Режим доступа: http://protege.stanford.edu/, свободный – Загл. с экрана. – Яз. англ.
2. The OTK Tool Repository: OntoEdit [электронный ресурс] – Режим доступа: http://www.ontoknowledge.org/tools/ontoedit.shtml, свободный – Загл. с экрана. – Яз. рус., англ.
3. The KArlsuhe Ontology and Semantic Web tool suite [электронный ресурс] – Режим доступа: http://kaon.semanticweb.org/, свободный – Загл. с экрана. – Яз. англ.
4. OntoVis – Protégé Wiki [электронный ресурс] – Режим доступа: http://protegewiki.stanford.edu/index.php/OntoViz, свободный – Загл. с экрана. – Яз. англ.
5. IzaVis Overview [электронный ресурс] – Режим доступа: http://www.w3.org/2001/11/IsaViz/, свободный – Загл. с экрана. – Яз. англ.
6. SpaceTree: a novel node-link tree browser [электронный ресурс] – Режим доступа: http://www.cs.umd.edu/hcil/spacetree/, свободный – Загл. с экрана. – Яз. англ.
7. Ontosphere 3d [электронный ресурс] – Режим доступа: http://ontosphere3d.sourceforge.net/, свободный – Загл. с экрана. – Яз. англ.
8. Jambalaya – Protégé wiki [электронный ресурс] – Режим доступа: http://protegewiki.stanford.edu/index.php/Jambalaya, свободный – Загл. с экрана. – Яз. англ.

УДК 681.4

АЛГОРИТМ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ЕДИНИЧНЫЙ КОЭФФИЦИЕНТ МАТРИЦЫ ДИСКРЕТНО-КОСИНУСНОГО ПРЕОБРАЗОВАНИЯ

О.В. Михайличенко, Н.Н. Прохожев
Научный руководитель – д.т.н., профессор А.Г. Коробейников

В статье предлагается метод встраивания цифровых водяных знаков в область дискретно-косинусного преобразования, обладающий повышенной устойчивостью к внешним воздействиям. Отличительной особенностью метода является использование единичного коэффициента матрицы ДКП для кодирования бита встраиваемой информации. Приводится сравнительная оценка устойчивости данного метода к основным внешним воздействиям на изображение контейнер. На основании практического применения даются рекомендации по выбору областей и параметров встраивания.

Ключевые слова: стеганография, алгоритмы частотной области, цифровые водяные знаки

Введение

Построение устойчивой стеганосистемы является актуальной и до конца не решенной задачей. Устойчивость к разного рода внешним воздействиям является ключевой характеристикой для алгоритмов, на основе которых строиться стеганосистемы решающие задачу защиты авторских прав. Целью данной работы является разработка алгоритма обладающего повышенной устойчивостью к одному из видов внешних воздействий – к JPEG сжатию с потерями.

Стеганографические алгоритмы на основе ДКП

Все современные алгоритмы, в основе которых лежит ДКП, можно классифицировать по выбору областей встраивания с псевдослучайным и качественным выбором, по количеству коэффициентов участвующих в кодировании бита скрываемой информации: на 2-х коэффициентные, 3-х коэффициентные и использующие множество коэффициентов. Несмотря на заявления авторов большинства алгоритмов, устойчивость алгоритмов по некоторым внешним воздействиям явно недостаточная для построения надежной стеганосистемы. Как показывает анализ устойчивости, алгоритмы не могут успешно противостоять такому распространенному воздействию, как JPEG сжатие с коэффициентом качества ниже 50, масштабированию и усредняющей фильтрации с размером окна фильра 3x3 пикселя и более [1]. Если разного рода фильтрации и зашумления являются достаточно специфическими видами воздействий, то сжатие и масштабирование широко практикуются при использовании изображений. При исходных размерах большинства современных цифровых изображений, часто превышающих 10 мегапикселей, сжатие с низким коэффициентом качества не является препятствием для коммерческого использования такого изображения. Поэтому, наличие алгоритма устойчивого к JPEG сжатию с потерями, является одним из условий построения устойчивой стеганосистемы внедрения ЦВЗ в графические контейнеры.

Деградирующее воздействие JPEG сжатия на матрицу ДКП

Чтобы понять причины недостаточной устойчивости стеганоалгоритмов к JPEG сжатию, рассмотрим природу деградирующего воздействия JPEG сжатия на матрицу ДКП в целом. Основные потери информации происходят на этапе квантования. Коэффициенты ДКП квантуются матрицей квантования стандарта JPEG представленной на

рис. 1. Матрица была разработана исходя из психофизической модели человеческого зрения, с целью минимизировать видимые искажения в результате сжатия изображения.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	102	121	120	101
72	92	95	98	112	100	103	99

Рис. 1. Коэффициенты матрицы квантования стандарта JPEG

При квантовании и последующем восстановлении коэффициенты матрицы ДКП изменяют свои значения. Такие изменения могут нарушить целостность встроенной информации.

Кодирование информации осуществляется созданием определенного неравенства между коэффициентами матрицы ДКП, в которые поизводиться встраивание. Нарушение этого неравентсва неизбежно приводит к безвозвратной потере информации. Неравенство может быть нарушено в двух случаях: неравенство превращается в равенство и знак неравенства изменяется. Превращение неравенства в равенство, в свою очередь, также возможно в двух случаях: когда коэффициент становяться равны друг другу и когда они обнуляются. При больших значениях коэффициента силы встраивания, модификация коэффициентов осуществляется путем их изменения на значительную величину, что уменьшает вероятность их равенства. Несмотря на то, что такой подход приводит к сильным искажениям изображения контейнера, он дает ощутимое увеличение устойчивости, что, как правило, используется в алгоритмах с качественным выбором областей встраивания. Следует так же отметить, что преимущество в устойчивости к JPEG имеют алгоритмы с 2-х коэффициентным кодированием, поскольку использование меньшего количества коэффициентов позволяет изменять их на большую величину без серьезных потерь качества изображения. Однако, предотвратить обнуление коэффициентов возможно только путем увеличения их значений, что имеет очень ограниченные возможности независимо от алгоритма встраивания. Изменение знака неравенства между коэффициентами обусловлено разностью значений между коэффициентами матрицы квантования. Если кодирующая разность между коэффициентами незначительна по отношению к величинам самих коэффициентов, а величины соответсвующих коэффициентов матрицы квантования значительны, то знак неравентсва может поменяться в случае, если неравенство между квантующими коэффициентами нарушает кодирующее неравенство.

Разработанный алгоритм повышенной устойчивости

Очевидный путь повышения устойчивости – это использование коэффициентов матрицы ДКП в областях назкочастотных компонент. Проведенные исследования показывают, что, несмотря, на изменение характера вносимых искажений, уровень этих самых искажений остается одинаковым [2]. Если искажения не достигают уровня визуализации, то встраивание в коэффициенты низкочастотных компонент вполне оправдано. Однако, использование для этих целей коэффициентов близких к DC коэффициенту все же не рекомендуется, поскольку это может приводить к серьезной деградации всего

пиксельного блока. Не целесообразно, также, ограничивать область допустимых коэффициентов исключительно их принадлежностью к определенной частотной группе компонент, как это делает большинство авторов. Если взглянуть на матрицу квантования JPEG, то можно заметить, что квантующие коэффициенты для коэффициентов матрицы ДКП одной частотной области могут отличаться более чем в два раза. При такой селекции, устойчивость внедренной информации будет зависеть лишь от псевдослучайного выбора конкретных коэффициентов. Таким образом, целесообразно определять рамки области коэффициентов матрицы ДКП, пригодных для встраивания информации, значениями соответствующих коэффициентов матрицы квантования JPEG.

При воздействии JPEG коэффициенты матрицы ДКП изменяют свои значения. Значения могут меняться, как в сторону увеличения кодирующего неравенства, так и в сторону его уменьшения. Зависит это от нескольких факторов, таких как, значения самих коэффициентов матрицы ДКП, величины разницы между кодирующими коэффициентами, значениями соответствующих коэффициентов квантования. Определить заранее поведение коэффициентов матрицы ДКП при JPEG сжатии достаточно сложно, поскольку коэффициент силы встраивания задается пользователем, а коэффициенты, в которые производиться встраивание, выбираются псевдослучайным образом. Для исключения такой неопределенности предлагается использовать один коэффициент матрицы ДКП и некоторое пороговое значения, для однозначного кодирования встраиваемого бита, как описано в формуле.

Кодирование:

$$\begin{cases} |\Omega_b(\upsilon,\nu)| < 0.5P, & при \quad m_b = 0; \\ |\Omega_b(\upsilon,\nu)| > 1.5P & при \quad m_b = 1. \end{cases}$$

Считывание:

$$\begin{cases} m_b = 0 & при \quad |\Omega_b(\upsilon,\nu)| < P; \\ m_b = 1 & при \quad |\Omega_b(\upsilon,\nu)| > P. \end{cases}$$

где $\Omega_b(\upsilon,\nu)$ – коэффициент матрицы ДКП с координатами υ,ν ; P – коэффициент силы встраивания; m_b – бит встраиваемой информации.

Здесь пороговое значение играет роль «виртуального коэффициента», который не подвержен влиянию JPEG сжатия, что позволяет исключить ситуацию, когда изменения коэффициентов направлены в сторону уменьшения кодирующего неравенства между ними. Выбор величины порогового значения определяется устойчивостью встроенной информации, чем больше величина, тем выше устойчивость. Стоит предостеречься от использования слишком больших значений порогового коэффициента, поскольку это может сильно сказаться на качестве изображения. Целесообразно выбирать значения порогового коэффициента близким к среднему значению соответствующих коэффициентов матрицы ДКП.

Результаты сравнительного анализа устойчивости разработанного алгоритма

Для сравнительного анализа был выбран алгоритм Кох, как наиболее устойчивый алгоритм со случайным выбором областей встраивания. Уровень вносимых искажений при встраивании устанавливался одинаковым по параметру пикового соотношения сигнал/шум (PSNR). Величина искажений выбиралась субъективно с условием отсутствия визуализации артефактов внедрения. В качестве изображений контейнеров были выбраны 10 полутоновых естественных изображений разрешением 512×512. Размер внедряемого ЦВЗ соответствовал максимальной пропускной способности контейнеров. Устойчивость измерялась параметром BER(Bit Error Rate) [3].

Результаты сравнительного анализа устойчивости алгоритма к JPEG сжатию с потерями представлены на рис. 2

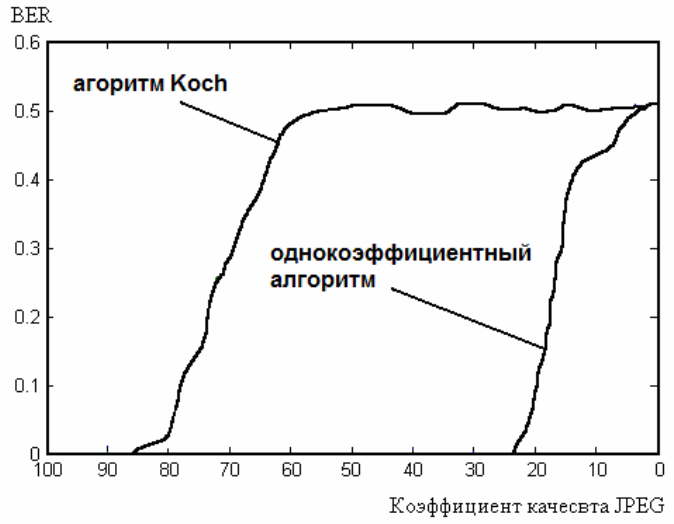


Рис. 2. Устойчивость алгоритмов к JPEG сжатию с потерями

Как и ожидалось, однокоэффициентный алгоритм демонстрирует хорошую устойчивость к JPEG сжатию, что обусловлено как использованием устойчивых коэффициентов матрицы ДКП, так и однокоэффициентной природой алгоритма

Устойчивость к фильтрации позволяет говорить об устойчивости данного алгоритма к этому виду воздействия, см. таблицу.

Фильтр	Koch, BER	Однокоэффициентный алгоритм, BER
Низкочастотный	0.008	0.018
Усредняющий	0.42	0.24
Контрастный	0	0.022

Таблица. Устойчивость встроенной информации к фильтрации

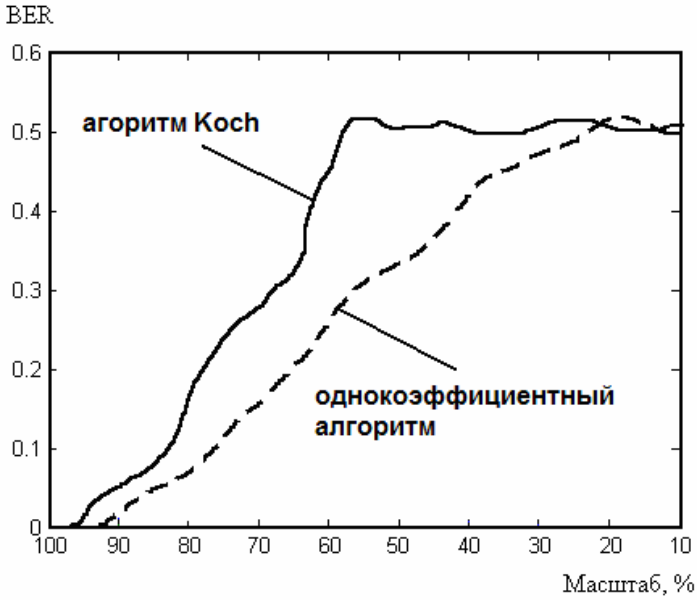


Рис. 3. Устойчивость алгоритмов к масштабированию

Наиболее опасная усредняющая фильтрация оказывает меньшее воздействие, чем на алгоритм Кох, в силу использования низкочастотных областей для встраивания.

Результаты устойчивости алгоритмов к масштабированию приведены на рис. 3.

Сильного выигрыша в устойчивости к масштабируемости у однокоэффициентного алгоритма не наблюдается, поскольку особенности масштабирования никак не учитывались при разработке данного алгоритма. Небольшое преимущество перед алгоритмом Кох можно также объяснить использованием низкочастотных областей для встраивания.

Выводы

Был создан алгоритм повышенной устойчивости к JPEG сжатию. Достигнутый уровень устойчивости позволяет противостоять этому воздействию во всем диапазоне качества JPEG сжатия в рамках коммерческого использования изображения-контейнера. Использование данного алгоритма, в качестве ядра устойчивой стеганосистемы, будет гарантировать сохранность внедренной информации, даже если изображение-контейнер подвергать сжатию с низким коэффициентами качества JPEG. При этом устойчивость к остальным внешним воздействиям будет на уровне современных стеганографических алгоритмов.

Литература

1. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – М: Издательство МК-Прес, 2006. – 288 с.
2. Прохожев Н.Н., Михайличенко О.В., Коробейников А.Г. Использование стеганографических алгоритмов частотной области в условиях атак на изображение-контейнер. – Дивноморск. САПР, 2008.
3. Коробейников А.Г., Прохожев Н.Н., Михайличенко О.В. Выбор коэффициентов матрицы дискретно-косинусного преобразования при построении стеганографических систем, основанных на алгоритмах частотной области. – М.: Вестник приборостроения, 2008. – №10.

УДК 681.2.001.5;681.2.007

ЗАДАЧА ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОЦЕССА МАССОПЕРЕНОСА ЖИДКИХ СРЕД С ГРАНИЦЕЙ РАЗДЕЛА

О.Л. Студеникин, О.В. Елисеев
Научный руководитель – к.т.н., доцент З.Г. Симоненко

Данная работа посвящена решению задачи имитационного моделирования процесса массопереноса жидких сред с границей раздела. По данным экспериментальных значений параметров массопереноса рассчитан ряд теоретических кривых для аналитического описания трехмерной диффузии
Ключевые слова: физическая модель, процесс массопереноса, трансцедентное уравнение, алгоритм, математическая модель, аналитическое описание

Введение

В современном приборостроении широко используются компьютерные технологии для имитации различных процессов, операций или их моделирования, выполняемых реальными устройствами, именуемыми системой. При этом приходится прибегать к допущениям, касающимся структурирования или функционирования системы, которые имеют вид математических или логических отношений, составляющих модель. Простые отношения описываются математическими методами, и для полученной математической модели решение является аналитическим. При рассмотрении сложных систем создается программно-аналитическая модель или имитационная модель, содержащая аналитические фрагменты.

Целью данной работы является необходимо создание программно-аналитической модели, имитирующей реальный эксперимент по определению параметров массопереноса.

Основная часть

Задача массопереноса в жидкой бинарной среде решается для стационарного случая в бесконечном вертикальном цилиндре относительно коэффициента массопереноса *D,* при условии зависимости концентрации *C* в любом горизонтальном сечении этого цилиндра от момента времени τ и расстояния *X* сечения *S* от поверхности раздела, то есть *C (X,*τ*),* с помощью уравнения Фика:

$$\mathbf{J} = grad(C * S) = -D\frac{\partial c}{\partial x}, \qquad (1)$$

где *D* – коэффициент переноса, зависящий от природы растворителя и растворенного вещества, равный количеству проходящего через единицу площади S вещества, нормальной к вектору направления диффузии в единицу времени t с размерностью $(м^2 * сек^{-1})$. Знак минус в формуле (1) характеризует направление потока в сторону, обратную градиенту от больших концентраций к меньшим.

При исследовании процесса массопереноса вектор *J* градиента концентрации бинарной жидкой среды является составляющей программно-аналитического подхода к созданию имитационной модели [1].

Важно учитывать, что в рабочем объеме этот градиент направлен вертикально вверх и равен 0 на концах рабочего объема, а коэффициент массопереноса в рабочем объеме – постоянная величина (рис. 1).

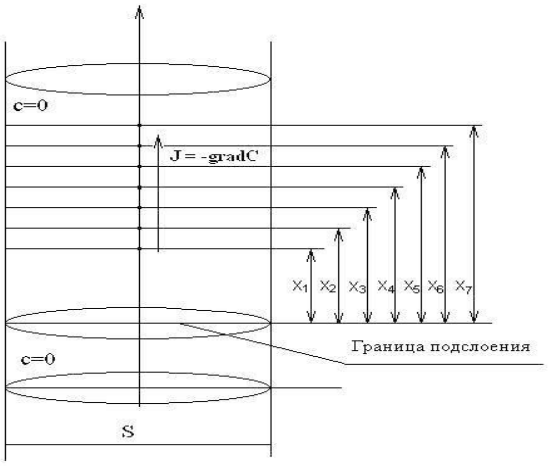


Рис. 1. Динамика переноса в диффузионном объеме

Физическая модель процесса массопереноса реализована с помощью метода и прибора лазерной поляризационной эллипсометрии [2]. В результате экспериментального определения параметров массопереноса (диффузии) были получены данные зависимостей $I = f(\tau)$ для случая двумерной диффузии. В работах [3, 4] показана принципиальная возможность аналитического описания двухмерной бинарной диффузии, в ней описана система уравнений, с помощью которых эта задача решается. В проводимом эксперименте необходимо получить величины зависимости $I = f(X)$, позволяющие получить аналитическое выражение для трехмерной диффузии.

Важным фактором является корректность используемой математической модели, которая обеспечивается, с одной стороны, высокой точностью экспериментально воспроизводимых величин коэффициента массопереноса, а с другой, точностью вычисления их с помощью созданных программ. Эти программы позволяют найти корни трансцендентного уравнения, связывающего между собой входные и выходные переменные исследуемого процесса массопереноса в жидкой бинарной среде с границей раздела, имеющего следующий вид:

$$\frac{erf\left[\frac{1}{\sqrt{4D\tau_3}}(X_0+\alpha/2)\right]-erf\left[\frac{1}{\sqrt{4D\tau_3}}(X_0-\alpha/2)\right]-erf\left[\frac{1}{\sqrt{4D\tau_2}}(X_0+\alpha/2)\right]+erf\left[\frac{1}{\sqrt{4D\tau_2}}(X_0-\alpha/2)\right]}{erf\left[\frac{1}{\sqrt{4D\tau_2}}(X_0+\alpha/2)\right]-erf\left[\frac{1}{\sqrt{4D\tau_2}}(X_0-\alpha/2)\right]-erf\left[\frac{1}{\sqrt{4D\tau_1}}(X_0+\alpha/2)\right]+erf\left[\frac{1}{\sqrt{4D\tau_1}}(X_0-\alpha/2)\right]}=1 \quad (2)$$

где τ_1, τ_2, τ_3 – измеряемые интервалы времени (с); D – коэффициент массопереноса ($м^2 * с^{-1}$); X_0 – расстояние от границы раздела двух жидких сред до прямой, равноудаленной от двух ортогонально поляризованных интерферирующих пучков (м); α – расстояние между двумя ортогонально поляризованными интерферирующими пучками (м). *erf (error function)* – функция ошибок Гаусса.

При решении уравнения (2) для получения численных значений, характеризующих соответствие вычисленных и экспериментально измеренных параметров массопереноса, выбраны заданные начальные и граничные условия, а также экспериментально полученные параметры:

$\alpha = 4 * 10^{-4}$ (м), $X_0 = 4{,}5 * 10^{-4}$ *(м),* $D = 1{,}88 * 10^{-9}$ $(м^2 * с^{-1})$, $\tau_1 = 470, \tau_2 = 1000, \tau_3 = 1436;$ (с).

Реализация алгоритма осуществлена с помощью программы, написанной на языке C/C++, в среде программирования MinGW, а также использования прикладного программного интерфейса Win32 API и средств графического пакета OpenGL), написанной в среде разработки Microsoft Visual Studio.NET 2003 на языке программирования C# [5].

В реальной физической модели величина *Xo* имеет фиксированное значение, т.е., лазерный пучок постоянно излучает на высоте, равной величине *Xo* от границы раздела двух сред. Для осуществления «виртуального» эксперимента переместим лазерный пучок на величину X_1 в вертикальном направлении – направлении градиента *J*, затем – на величину X_2, и так далее, каждый раз переходя от точки к точке объема вверх по искомому градиенту *J* (рис. 1).

Алгоритмическая последовательность выполняется в следующем порядке:

1. Строится огибающая *L* хода массопереноса для экспериментальной кривой (см. рис. 3).

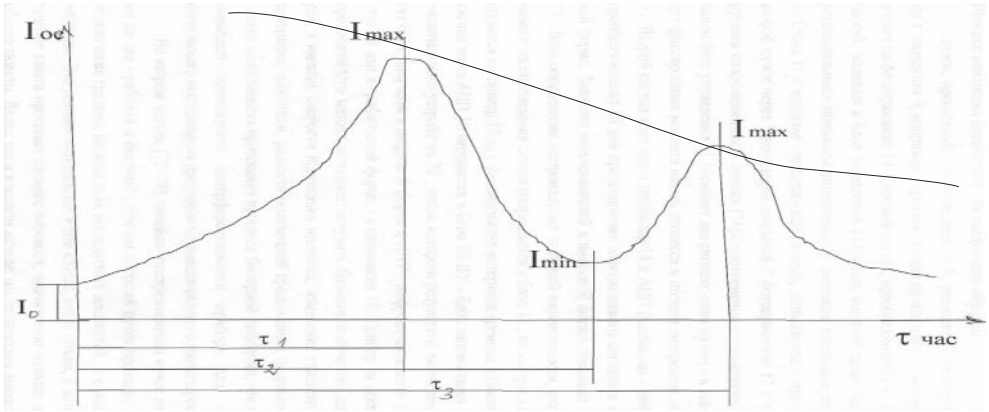


Рис. 2. Экспериментальная кривая изменения параметров массопереноса в бинарной с огибающей *L*

2. По программе рассчитываются мультипликативные коэффициенты k_1 и k_2, где $k_1 = \tau_2 / \tau_1$, $k_2 = \tau_3 / \tau_2$, где I_1, I_2, I_3 соответствуют трем экстремальным значениям величин составляющих интенсивности поляризованного излучения, прошедшего через диффундирующий слой.

3. С помощью этих коэффициентов осуществляется расчет величин триады (τ_1, τ_2, τ_3), который проводим с позиций единых требований, предъявляемых к математическим моделям, и с использованием научного логико-математического аппарата (прикладной «золотой» математики) из работы [6].

4. Для полученных величин триады (τ_1, τ_2, τ_3) рассчитываются искомые величины *X* семейства X_i, соответствующие виртуальному перемещению лазерного пучка в вертикальном направлении рабочего объема при при заданных граничных условиях и экспериментально полученном коэффициенте массопереноса.

В табл. 1 приведены вычисленные вычисления *Xi (*где *i* принимает значения от 1 до 12*)* с точностью $1 \cdot 10^{-6}$, данные уже осуществленного экспериментального измерения выделены курсивом.

5. На рис. 3 под огибающей *L* строим семейство графиков хода массопереноса для полученных величин триады (τ_1, τ_2, τ_3) (рис. 3).

6. Из полученных графиков находим экстремальные значения величин составляющих интенсивности ($I_{1,,}$ $I_{2,,}$ I_3) для полученных величин триады (τ_1, τ_2, τ_3) . Значения величин τ_i *и* I_i представлены в табл. 2.

τ_1, (сек)	τ_2, (сек)	τ_2, (сек)	Xi (м)
117,5	250,0	359,0	0,007898
141,0	300,0	430,9	0,008550
150,4	320,0	459,5	0,008775
173,9	370,0	531,3	0,002858
235,0	500,0	718,0	0,001069
300,8	640,0	919,0	0,003632
338,4	720,0	1033,9	0,003834
432,4	920,0	1321,1	0,004298
470,0	***1000,0***	***1436,0***	***0,004500***
705,0	1499,0	2154,0	0,005423
940,0	1999,0	2872,0	0,006233
1889,0	3998,0	5744,0	0,008753

Таблица 1. Результаты имитационного эксперимента для величин τ_1, τ_2, τ_3

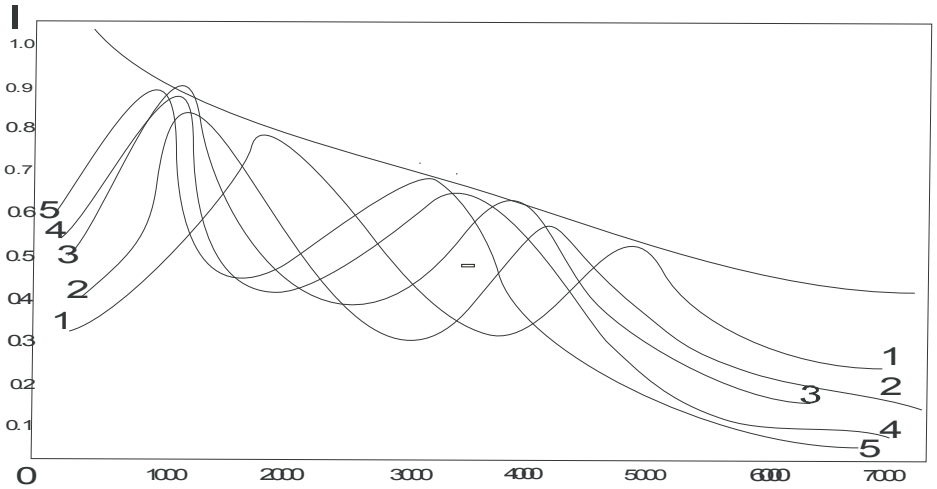


Рис. 3. Диаграмма семейства кривых $I = f(Xi)$

τ_1, (сек)	I_1	τ_2, (сек)	I_2	τ_3 (сек)	I_3
117,5	0,995	250,0	0,24	359,0	0,667
141,0	0,99	300,0	0.238	430,9	0,663
150,4	0,98	320,0	0,235	459,5	0,657
173,9	0,97	370,0	0,233	531,3	0,650
235,0	0,945	500,0	0,228	718,0	0,636
300,8	0,94	640,0	0,226	919,0	0,630
338,4	0,93	720,0	0,223	1033,9	0,623
432,4	0,90	920,0	0,216	1321,1	0,603
470,0	0,898	**1000,0**	0,21	**1436,0**	0,596
705,0	0,82	1499,0	0,197	2154,0	0,549
940,0	0,74	1999,0	0,178	2872,0	0,496
1889,0	0,71	3998,0	0,170	5744,0	0,476

Таблица 2. Результаты имитационного эксперимента для величин $I_{1,}$, $I_{2,}$, I_3

7. На рис. 4 выделим интегральную огибающую хода массопереноса.

8. Из данных диаграммы, представленной на рис. 4 и табл. 2 можно выявить данные зависимости величин X_i от I_i, которые представлены в табл. 3.

9. Полученная кривая зависимости величин интенсивностей $I=f(X)$ представлена на рис. 4.

Xi (м)	*Ii*
0,002858	0,97
0,010688	0,95
0,003632	0,94
0,016900	0,93
0,004298	0,90
0,004500	0,89
0,001200	0,82
0,005423	0,74
0,008753	0,71

Таблица 3. Данные зависимости величин X_i от I_i

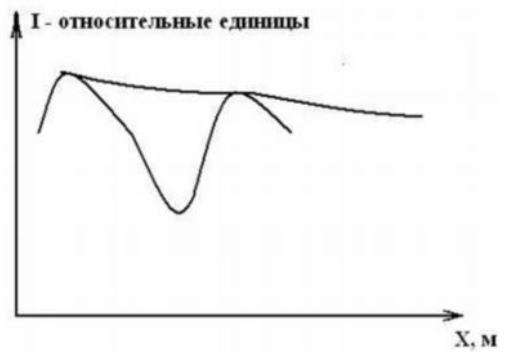


Рис. 4. График зависимости *I=f(x)*

Заключение

В данной работе осуществлен имитационный эксперимент ввиду большой сложности и трудоемкости реального измерительного процесса. Создание программно-аналитической модели позволяет получит как промежуточные параметры исследуемого процесса, но и получить необходимые данные для расчета коэффициентов при аналитическом описании трехмерной диффузии [7]. Результаты работы, полученные впервые, позволят получить семейство кривых для сплошных сред с заранее заданными свойствами.

Литература

1. Аверилл М. Лоу, В. Дэвид Кельтон. Имитационное моделирование. – 3-е издание: ПИТЕР. – Москва. – 2004.
2. Авторское свидетельство СССР № 976307. Бюллетень ОИ ПОТЗ / З.Г. Симоненко, А.А. Равдель, А.Б. Порай-Кошиц. Способ определения коэффициентов молекулярной диффузии в жидкостях и устройство для его реализации. – 1982.
3. Симоненко З.Г., Плотников В.В., Ильина Л.П., Мануйлов К.В., Федоров В.Н. Теорема Остроградского и решение параболических уравнений. – Научная конференция «Петербургская математическая школа в период XIX века» (24–28 сентября 2001г.) посвященная 200-летию со дня рождения М.В. Остроградского. – СПб.

4. Мануйлов К.В., Симоненко З.Г., Ильина Л.П., Плотников В.В. Экспериментальные и теоретические аспекты решения параболического уравнения для случая нетрансляционного массопереноса в жидкости. // Научно-технический вестник СПбГИТМО(ТУ), вып.3 «Физические процессы, системы и технологии точной механики». СПбГИТМО(ТУ). – 2002. – С. 188–191.
5. Симоненко З.Г., Лысак А.А., Якушенков М.В.Свидетельство о государственной регистрации программы для ЭВМ № 2009610784. Программа для вычисления параметров массопереноса в жидких средах с границей раздела. Зарегистрировано 4.02.2009 г.
6. Ясинский С.А. Прикладная «золотая» математика и ее приложения в электросвязи. Москва, Горячая линия – Телеком. – 2004. – 239 с.
7. Симоненко З.Г., Ильина Л.П., Мануйлов К.В., Несмачный Д.В. Аналитическое описание теплопроводности и диффузии в трехмерном пространстве. Научно-технический вестник СПбГУ ИТМО, вып.3 «Физические процессы, системы и технологии точной механики». – 2004.

УДК 004.421

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ РЕГИСТРАЦИИ МНОГОКАНАЛЬНОЙ ЭЛЕКТРОЭНЦЕФАЛОГРАММЫ

А.Г. Даурских, Н.В. Павлова
Научный руководитель – к.т.н., доцент Б.А. Крылов

Электроэнцефалография остается наиболее доступным методом оценки состояния головного мозга, который широко используется при неврологических исследованиях, в педиатрии, хирургии, анестезиологии, акушерстве, а также при научных исследованиях в области нейрофизиологии, психофизиологии, нейрокибернетике, инженерной психологии, и во многих смежных областях. Статья посвящена разработке программного комплекса регистрации многоканальной электроэнцефалограммы, предназначенного для научно-исследовательских целей. Комплекс должен осуществлять регистрацию и предварительную обработку многоканальной электроэнцефалограммы, усиление и цифровое преобразование ЭЭГ-сигналов и непосредственный ввод результатов обработки в ЭВМ с формированием на жёстком диске файла обследования пациента

Ключевые слова: электроэнцефалограмма, комплекс, регистрация, визуализация

Введение

По мере совершенствования компьютерной техники и программного обеспечения возможности автоматизированного анализа пространственно-временных отношений колебаний биопотенциалов мозга существенно расширились. Встала задача не только обрабатывать многоканальный (16–20 отведений) электроэнцефалографический сигнал в реальном времени, но и визуализировать результаты анализа в форме, приемлемой для научного исследования непосредственно в ходе наблюдения.

Для регистрации электроэнцефалографического сигнала был разработан программно-аппаратный комплекс, при создании которого были максимально учтены пожелания исследователей, осуществлена визуализация многоканальной электроэнцефалограммы в режиме реального времени.

Схема программно-аппаратного комплекса регистрации многоканальной электроэнцефалограммы

Аппаратный комплекс регистрации многоканальной электроэнцефалограммы представляет собой персональный компьютер с подключенным к нему посредством USB-кабеля электроэнцефалографом. На рис. 1 показана схема программно-аппаратного комплекса.

Электроэнцефалограф регистрирует с заданной частотой разность потенциалов (доли мВ) по каждому из каналов. Затем сигналы, полученные с электродов, усиливаются и осуществляется их аналого-цифровое преобразование.

Драйвер электороэнцефалографа, программа регистрации и программа чтения устанавливаются на персональный компьютер и образуют программный комплекс регистрации многоканальной электроэнцефалограммы.

Структура программного комплекса

Программный комплекс включает в себя:

- драйвер;
- программу регистрации;
- программу чтения.

Драйвер поставляется с прибором и предоставляет для работы с электроэнцефалографом набор функций. Все обращения программы регистрации к прибору производятся не напрямую, а через функции драйвера.

Структура и алгоритмы работы программы регистрации рассмотрены ниже.

При помощи функций драйвера программа регистрации получает массив, состоящий из заданного количества измерений по каждому из каналов. Структура внешних данных описана ниже. Полученный массив преобразуется в соответствие с алгоритмом преобразования входной информации во внутреннюю. Затем данные фильтруются.

Программа регистрации многоканальной электроэнцефалограммы также выполняет следующие функции:

- управление аппаратными функциями электроэнцефалографа: усилением, фотостимуляцией, измерением сопротивления, частотой приёма, закорачиванием разделительного конденсатора;
- визуализацию многоканальной электроэнцефалограммы;
- формирование файла обследования

Сформированный файл обследования сохраняется на жестком диске. Его можно открывать, используя программы чтения.

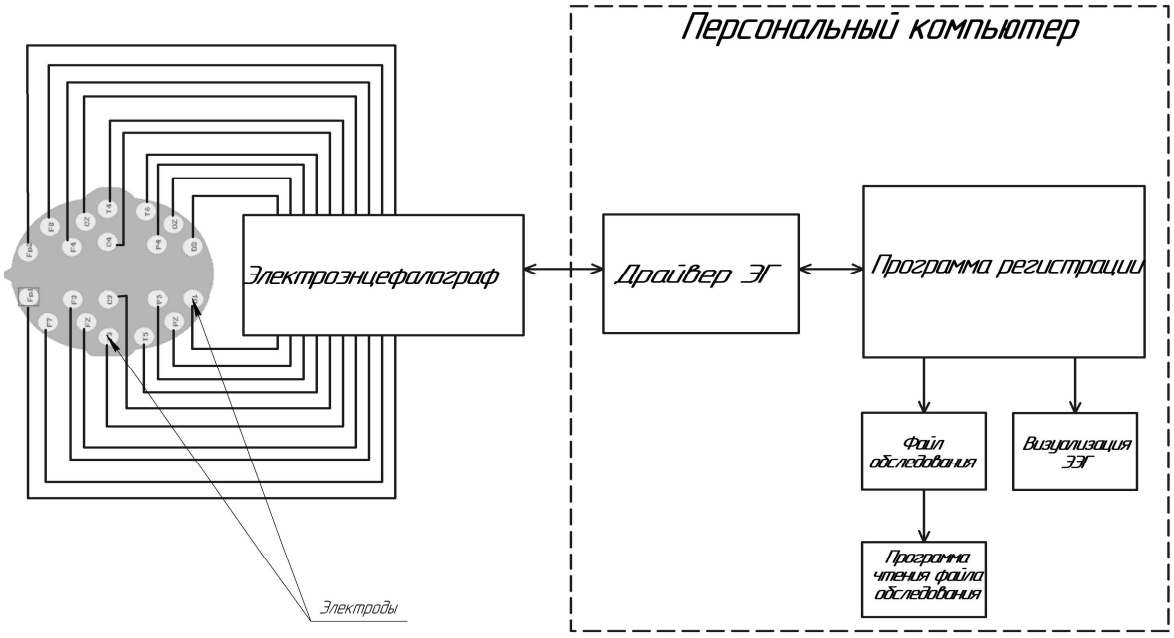


Рис. 1. Схема программно-аппаратного комплекса

Для реализации программы регистрации выбрана двупоточная структура, так как параллельно с выводом ЭЭГ на экран необходимо выполнять непрерывный опрос USB и получение массива измерений по каждому каналу.

При разработке программы в Borland Builder C++ мы используем объекты библиотеки VCL, их свойства и методы. Обращаясь к свойствам или выполняя методы этих объектов, могут выполняться некоторые действия, которые используют память, которая не защищена от действий других потоков. А значит, основной поток библиотеки VCL должен быть единственным потоком, управляющим этой библиотекой. Для того, чтобы безопасно из потока получить доступ к управлению свойствами и методами VCL-объектов (компонентов) необходимо использовать метод Synchronize().

Поток чтения USB организуем в виде бесконечного цикла, который непрерывно выполняет опрос USB. Опрос USB прекращается только при завершении работы приложения.

Поток чтения USB также осуществляет первичное преобразование полученного массива, а также изменение режима работы электроэнцефалографа (передача в устройство байта режимов).

Основной поток выполняет фильтрацию массива измерений, визуализацию многоканальной электроэнцефалограммы, формирование файла обследования, изменение байта режимов в зависимости от установок частоты, усиления, режима ЭЭГ/Калибровка и т.д.

Входными данными для программы регистрации многоканальной электроэнцефалограммы являются данные, возвращаемые функциями драйвера. Драйвер возвращает массив внешних данных, который физически является одномерным, а логически – двумерным. Этот массив состоит из заданного количества измерений по каждому каналу.

С помощью функций драйвера также получаем значение флага ошибки таймаута, он устанавливается в единицу, когда превышен допустимый интервал времени ожидания ответа от устройства.

Полученный по USB массив внешних данных преобразуем в соответствии с алгоритмом преобразования входной информации во внутреннюю во внутренний массив. Каждая строка этого массива состоит из заданного количества измерений по каждому из каналов.

Алгоритм преобразования входной информации во внутреннюю

Алгоритм преобразования входной информации во внутреннюю (рис. 2) является частью бесконечного цикла, расположенного в потоке чтения USB.

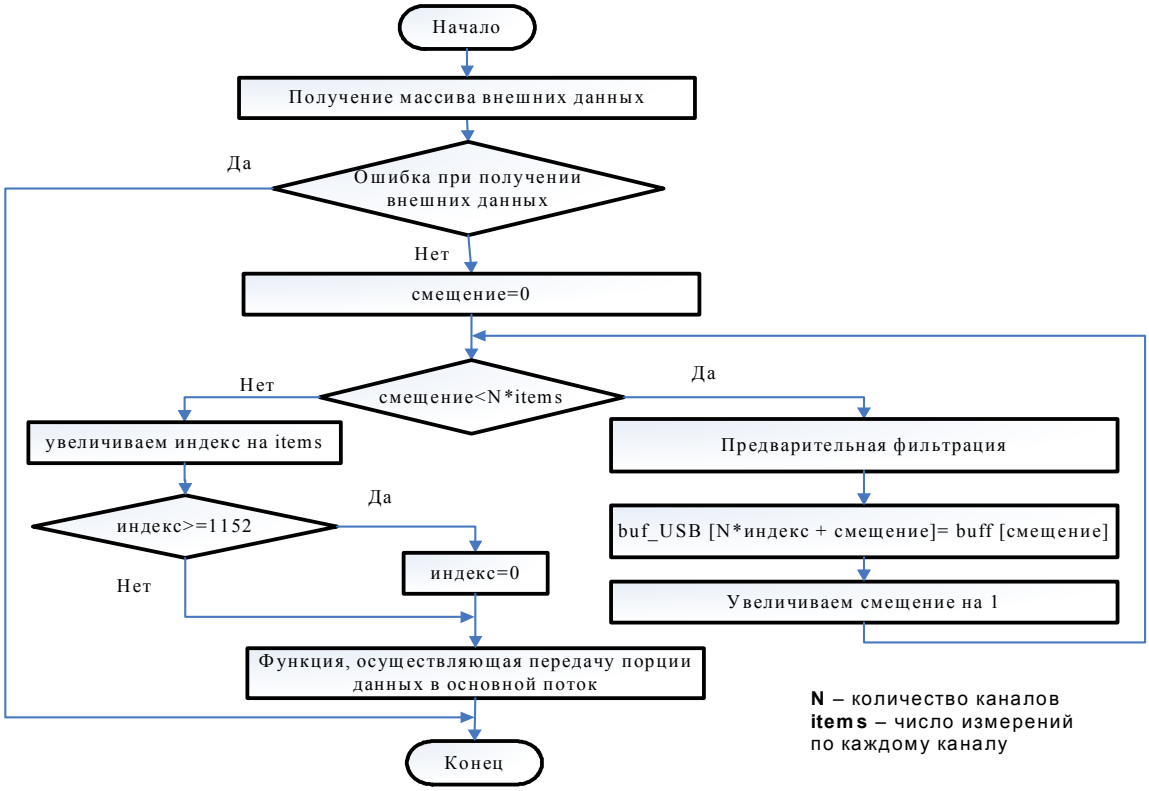


Рис. 2. Алгоритм преобразования входной информации во внутреннюю

При возникновении ошибки считывания информации по USB выдаётся сообщение об ошибке. Если ошибки не было, то переписываем все значения из полученного по USB массива внешних данных во внутренний массив, таким образом, формируется од-

на строка массива внутренних данных. После того как строка сформирована, к индексу прибавляем items (номер строки равен отношению индекса к числу каналов). Осуществляем проверку: если индекс больше или равен 1152, то обнуляем индекс. Далее вызываем функцию, осуществляющую передачу порции данных в основной поток.

Алгоритм фильтрации

Для осуществления фильтрации используется фильтр Чебышева. Достоинством фильтра Чебышева является крутизна нарастания затухания, особенно в районе частоты среза. На рис. 3 представлен алгоритм фильтрации.

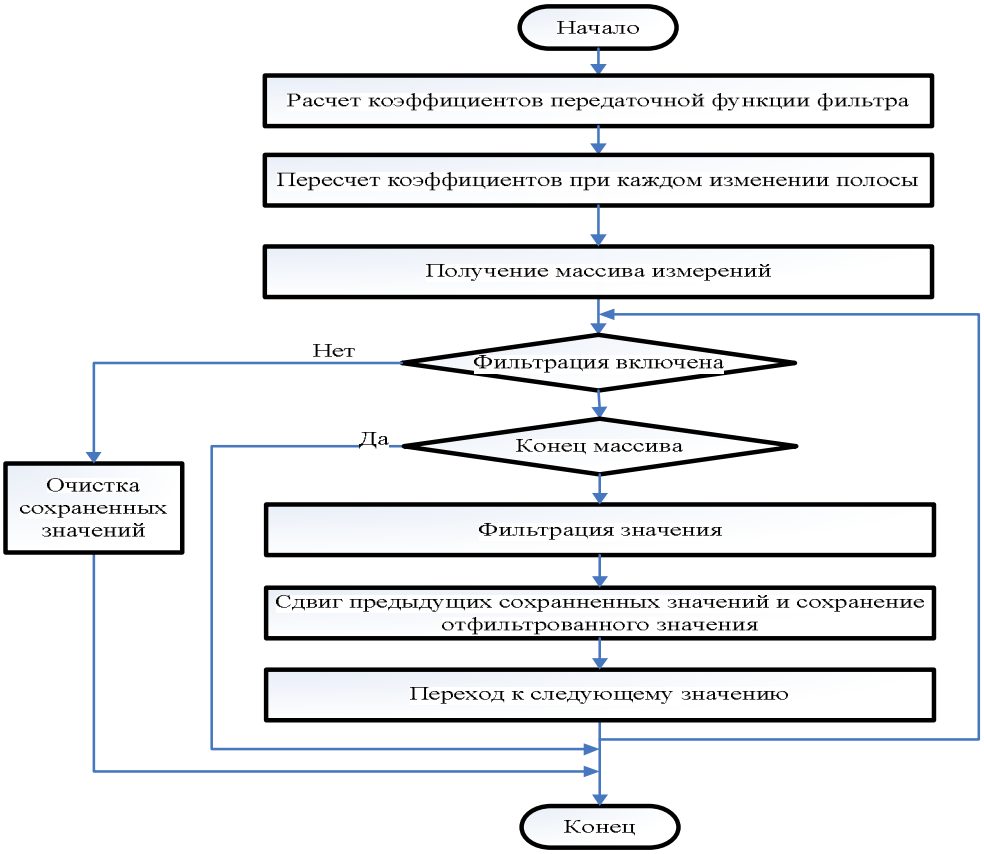


Рис. 3. Алгоритм фильтрации

Алгоритм визуализации регистрируемой ЭЭГ

Алгоритм визуализации изображен на рис. 4 и состоит из следующих шагов:

- создание области визуализации, установка размеров области визуализации (вызывается каждый раз при изменении размеров окна), вывод имён каналов;
- установка координаты X на начало области визуализации;
- если координата X больше ширины области визуализации, то возврат в пункт к предыдущему шагу;
- заполнение прямоугольной области цветом фона (очистка);
- прорисовка осей каналов на очищенной области, вывод времени;
- рисование линии;
- к текущей координате X прибавляем шаг.

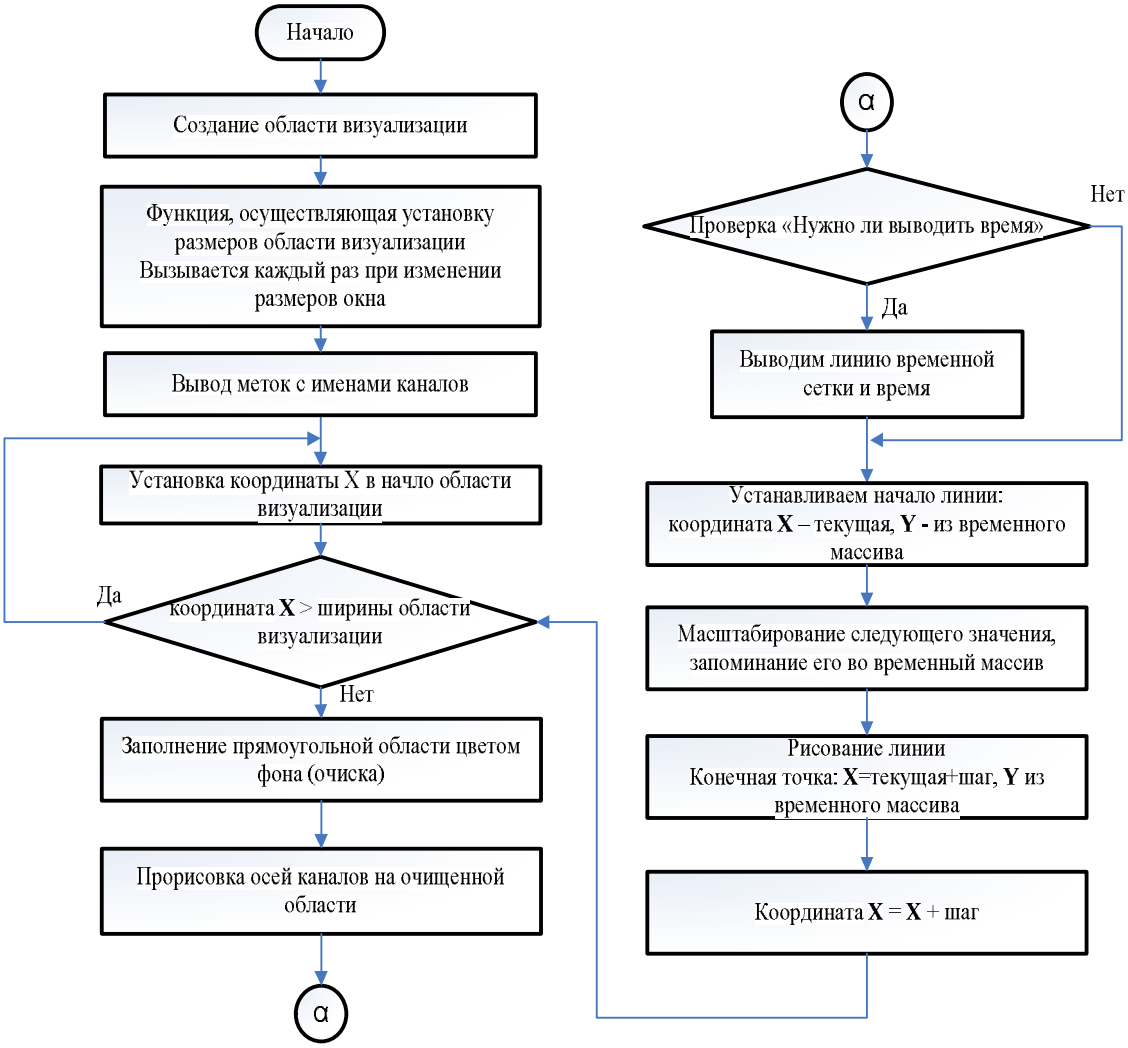


Рис. 4. Алгоритм визуализации

Структура файла обследования

Файл обследования предназначен для сохранения результатов и последующего воспроизведения зарегистрированной электроэнцефалограммы с помощью программы чтения.

Для реализации вышеуказанных требований файл обследования должен содержать следующую информацию:имя пациента, дату рождения пациента, дату обследования, пол пациента, комментарии специалиста, производящего регистрацию электроэнцефалограммы, количество используемых для регистрации каналов, частоту, на которой производиться запись, информацию об именах используемых для регистрации каналов, наборы значений, полученных с датчиков.

Алгоритм формирования файла обследования

Алгоритм формирования файла обследования начинается с нажатия на кнопку СОЗДАТЬ.

На экране появляется форма, куда необходимо внести данные о пациенте и имени файла, куда будут сохраняться результаты обследования.

Прибавляем к названию главной формы имя файла, введенное в поле “File Name” и расширение .eeg.

Создаем файл с именем, введенным в поле «File Name».

Теперь вызываем функцию, которая записывает в структуру имя пациента, дату рождения пациента, дату обследования, пол, комментарии, количество используемых для регистрации каналов, частоту, на которой производиться запись.

Вызываем функцию, которая записывает в заголовок файла ранее сформированную структуру и названия каналов. Если при записи произошла ошибка, то выводим сообщение «Ошибка при записи заголовка файла».

Далее, если нажата кнопка ЗАПИСЬ, записываем в файл по мере поступления массивы измерений до тех пор, пока не будет нажата кнопка ЗАКРЫТЬ.

Пока кнопка ЗАПИСЬ не нажата, происходит только визуализация электроэнцефалограммы.

Заключение

Была разработана структура программного комплекса регистрации многоканальной электроэнцефалорамы, а также разработана и реализована программа регистрации, выполняющая следующие функции:

- регистрацию электроэнцефалограммы;
- предварительную фильтрацию;
- управление аппаратными функциями (усилением, фотостимуляцией, частотой приема, закорачиванием разделительного конденсатора);
- визуализацию регистрируемой электроэнцефалограммы в режиме реального времени;
- формирование файла обследования;
- сохранение файла обследования на жестком диске.

Программа реализована на языке C++ в среде разработки Borland Builder 6.0 и имеет двупоточную структуру. Обращение к прибору происходит посредством функций драйвера.

Программный комплекс разрабатывался для научно-исследовательских целей и основным направление дальнейшей разработки является часть программного комплекса осуществляющая, машинный анализ зарегистрированной электроэнцефалограммы.

Литература

1. Егорова И.С. Электроэнцефалография. – М.: Медицина. – 1973. – 294 с.
2. Иванов Л.Б. Прикладная компьютерная электроэнцефалография: Моногр. – М.: Науч.-мед. фирма "МНБ", Антидор. – 2000. – 251 с.
3. Кратин Ю.Г., Гусельников В.И. Техника и методика электроэнцефалографии. – Л.: Медицина. – 1971. – 312 с.
4. Мошиц Г., Хорн П. Проектирование активных фильтров: Пер. с англ. – М.: Мир. – 1984. – 320 с.

УДК 004.89

ОБЗОР НАПРАВЛЕНИЙ МОДЕЛИРОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

А.Н. Носов
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

Рассмотрена задача моделирования различных вариантов создания искусственного интеллекта с теоретических точек зрения, а также на практике. Выделены основные принципы и представления концепций, возможные сферы применения искусственного интеллекта.
Ключевые слова: машинный интеллект, нейронные сети, инженерия знаний, экспертные системы

Введение

История искусственного интеллекта (ИИ) как нового научного направления начинается в 50х гг. XX века. К этому времени уже было сформировано множество предпосылок его зарождения: математики и экономисты задавались вопросами оптимальных расчётов и представления знаний о мире в структурном виде, нейрофизиологи и психологи разработали ряд теорий относительно работы человеческого мозга и мышления, а философы с давних времен вели споры о природе разума человека и процессе познания мира. Зародился фундамент математической теории вычислений – теории алгоритмов – и были созданы первые компьютеры. Возможности новых ЭВМ в плане скорости и количества вычислений оказались больше человеческих, поэтому в учёной среде закрался вопрос: существуют ли границы возможностей компьютеров и возможно ли в перспективе достижение машинами уровня развития человека?

Основная часть

Исторически сложились два основных подхода к моделированию ИИ: **машинный интеллект**, заключающийся в строгом задании алгоритма функционирования, и **искусственный разум**, направленный на моделирование внутренней структуры существования системы. Разделение работ по ИИ на два направления связано с существованием двух точек зрения на вопрос, каким образом строить системы ИИ [1].

Сторонники одной точки зрения убеждены, что совпадение поведения искусственно созданных и естественных интеллектуальных систем является наиболее приоритетным, и основной целью исследований является создание алгоритмического и программного обеспечения вычислительных машин, позволяющего решать интеллектуальные задачи не хуже человека. Другая точка зрения состоит в том, что непосредственное изучение механизмов естественного мышления органического происхождения и анализ данных о способах формирования разумного поведения человека могут создать основу для построения структур систем ИИ. Причем построение это должно осуществляться, как произведение техническими средствами принципов и конкретных особенностей функционирования биологических объектов. Моделирование систем машинного интеллекта, таким образом, рассматривает продукт интеллектуальной деятельности человека, изучает его структуру, и стремится воспроизвести этот продукт средствами современной техники. Оно достигается за счет использования логического подхода, теории множеств, фреймов, графов, семантических сетей и других достижений науки в области дискретных вычислений. Основные результаты заключаются в создании экспертных систем, систем разбора естественного языка и простейших систем управления вида «стимул-реакция». Ясно, что успехи этого направления ИИ тесно взаимосвязаны с раз-

витием возможностей ЭВМ и искусства программирования, то есть с тем комплексом научно-технических исследований, которые часто называют компьютерными науками.

Искусственный разум в перспективе рассматривает данные о нейрофизиологических и психологических механизмах интеллектуальной деятельности и, в более глобальном плане, разумного поведения человека. Эта технология стремится воспроизвести эти механизмы с помощью тех или иных технических устройств, с тем, чтобы алгоритмы таких устройств хорошо совпадали с поведением человека в определенных, заранее задаваемых пределах. Успехи в естественных науках предопределили развитие этого направления [2]. Для него характерно стремление к воспроизведению более широкого, чем в машинном интеллекте, спектра проявлений разумной деятельности человека. Системы искусственного разума базируются на математической интерпретации деятельности нервной системы, управляемой мозгом человека, и реализуются в виде нейронных сетей на базе нейроподобного элемента – аналога нейрона.

На сегодняшний день известно уже более 200 различных парадигм нейронных сетей (не только детерминированных, но и вероятностных), десятки НПС реализованы в специализированных кристаллах и платах, на их основе созданы мощные рабочие станции и даже суперкомпьютеры. Современные технологии достигли того рубежа, когда стало возможным изготовление технической системы из 3-4 млрд., как примерно и в человеческом мозге. Однако их соединение продолжает оставаться проблемой.

Также можно выделить еще одну концепцию, ориентированную на создание смешанных человеко-машинных, или интерактивных интеллектуальных систем, на симбиоз возможностей естественного и искусственного интеллекта. Важнейшими проблемами в этих исследованиях является оптимальное распределение функций и организация диалога между человеком и машиной. Но пока с уверенностью можно утверждать о несовершенстве и ненадежности получаемых результатов [3].

Методы и средства извлечения, структурирования, использования данных и метаданных изучает область ИИ, называемая инженерией знаний. Для типов знаний различного рода и для работы с ними должны использоваться конкретные методы и техника. Методы представления знаний получили особенно широкое распространение, начиная с 1970-х гг., когда весьма популярным направлением ИИ стали экспертные системы (ЭС) – интеллектуальные программы, основанные на использовании отдельно хранимой, пополняемой базы знаний о предметной области. ЭС выполняли в данной области роль эксперта, умеющего решать в ней, как правило, достаточно узкий, ограниченный применимостью конкретных, представленными в базе знаний, диапазон задач диагностики, планирования, прогнозирования и т.д.

Поскольку одним из важнейших свойств интеллекта является способность к обучению, то большое развитие получила такая подобласть инженерии знаний, как машинное обучение. Это самостоятельное получение знаний интеллектуальной системой в процессе её работы. Машинное обучение рассматривает большой класс задач на распознавание образов, а также биомоделирование [4].

Как выяснилось, знания, необходимые для решения многих нетривиальных практических задач с использованием компьютеров, носят гибридный характер, то есть, требуются не только процедурные, но также концептуальные и эвристические знания. Задумываясь о соотношении искусственного и естественного интеллекта, необходимо учитывать очевидное противоречие – то, что становится искусственным и передается машине, перестает быть интеллектом в буквальном смысле слова, а то, что подлинно разумно, остается вне функций компьютера.

Заключение

На сегодняшний день в создании ИИ наблюдается интенсивное слияние и переосмысление всех предметных областей имеющих хоть какое-то отношение к искусственному разуму в базы знаний. Практически все подходы были опробованы и изменены, но к возникновению ИИ ни одна исследовательская группа так и не подошла. Исследования ИИ влились в общий поток технологий сингулярности, таких как нанотехнология, актуарная математика, молекулярная биоэлектроника, теоретическая биология, квантовые теории, а также для обеспечения ряда других задач национальной безопасности. ИИ и его совершенствование превращают непреодолимые границы сложности в систематически преодолимые [5]. Это особенно важно в современном мире, в котором общество не может успешно развиваться без рационального управления сложными и сверхсложными системами. Разработка проблем ИИ является существенным вкладом в познание человеком закономерностей внешнего и внутреннего мира, в их использование в интересах общества и тем самым в развитие свободы человека.

Литература

1. Рассел С., Норвиг П. Искусственный интеллект: современный подход [Artificial Intelligence: a Modern Approach] / Пер. с англ. и ред. К.А. Птицына. – 2-е изд. – М.: Вильямс. – 2006.
2. Люгер Дж. Ф. Искусственный интеллект: стратегии и методы решения сложных проблем [Artificial Intelligence: Structures and Strategies for Complex Problem Solving] / Под ред. Н.Н. Куссуль. – 4-е изд. – М.: Вильямс. – 2005.
3. Горохов В.А. «Наука и жизнь», Инструмент интеллекта. – 1987. – №2.
4. Основы языка представления знаний Knowledge.NET, Научные работы Стэнфордского университета. – 1992.
5. Сирл Дж. «В мире науки». – 1990. – № 3. – с. 7–13.

УДК 004.056.55

ПРОГРАММНЫЙ КОМПЛЕКС ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ОСНОВЕ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В АУДИОСИГНАЛ МЕТОДОМ РАСШИРЕНИЯ СПЕКТРА

А.Г. Даурских, Н.В. Павлова
Научный руководитель – д.т.н., профессор А.Г. Коробейников

В работе рассмотрен стеганографический метод внедрения цифровых водяных знаков в аудиосигнал, а также шаги его практической реализации. Приведена структура работы алгоритма кодирования и декодирования сообщения.

Ключевые слова: стеганография, аудиосигнал, метод, цифровой водяной знак, расширение спектра

Введение

Повсеместное применение компьютерных технологий способствует активному использованию мультимедийной информации, т.е. информации, содержащей звуки, неподвижные изображения, текст, видеоизображения. Легкость распространения такой информации заставляет задумываться о защите авторских прав в каждом из названных видов мультимедийного контента. Из наиболее эффективных способов достичь этого стоит отметить использование методов стеганографии, т.е. встраивания в мультимедийные данные так называемых цифровых водяных знаков (ЦВЗ) – цифровых меток, невидимых без специального программного обеспечения и секретного ключа.

Для каждого вида данных существуют свои методы встраивания ЦВЗ, в которых используются определенные свойства этих данных. Так, для аудиосигналов применяются алгоритмы, основанные на особенностях самих сигналов и системы слуха человека (ССЧ).

ССЧ работает в сверхшироком динамическом диапазоне. Она воспринимает более чем миллиард к одному в диапазоне мощности, и более чем тысяча к одному в частотном диапазоне. Кроме этого, высокой является и чувствительность к аддитивному флуктуационному (белому) шуму. Отклонения в звуковом файле могут быть выявлены вплоть до одной десятимиллионной (на 70 дБ ниже уровня внешних шумов) [1].

Несмотря на это, существуют определенные возможности для скрытия информации в аудиосреде. Хотя ССЧ и имеет широкий динамический диапазон, она характеризуется достаточно малым разностным диапазоном. Как следствие, громкие звуки содействуют маскировке тихих звуков. Кроме того, ССЧ не способна различать абсолютную фазу, распознавая только относительную. Наконец, существуют некоторые виды искажений, вызванных окружающей средой, которые настолько обычны для слушателя, что в большинстве случаев им игнорируются [2].

В работе рассмотрена практическая реализация одного из таких методов, работающем во временно́й области – метод кодирования с расширением спектра.

Описание алгоритма

В стандартном канале связи нередко бывает желательным сосредоточить информацию в как можно более узком диапазоне частотного спектра, например, для того, чтобы сохранить имеющуюся полосу пропускания и уменьшить мощность сигнала. С другой стороны, основной метод расширения спектра предназначен для шифрования потока информации путем «рассеивания» кодированных данных по всему возможному

частотному спектру. Последнее делает возможным прием сигнала даже при наличии помех на определенных частотах.

В работе рассматривается алгоритм расширения спектра прямой последовательностью (РСПП). Методы РСПП расширяют сигнал данных (сообщения), умножая его на элементарную посылку – псевдослучайную последовательность максимальной длины, модулированную известной частотой.

Поскольку аудиосигналы, используемые в качестве контейнеров, имеют дискретный формат, то для кодирования в качестве элементарной посылки можно использовать частоту дискретизации. Как следствие, дискретный характер сигнала устраняет наиболее сложную проблему, которая возникает при получении сигнала с расширенным прямой последовательностью спектром, – корректное определение начала и конца составляющих элементарной посылки с целью фазовой синхронизации. Следовательно, возникает возможность использования намного более высокой частоты следования элементарных посылок, и, таким образом, получения значительной связанной с ней скоростью передачи данных. Кроме этого также могут применяться разнообразные алгоритмы блокирования сигнала, однако в вычислительном плане они являются достаточно сложными.

В РСПП для шифрования и дешифрования информации необходим один и тот же ключ – псевдослучайный шум, который в идеальном случае имеет плоскую частотную характеристику во всем диапазоне частот (так называемый белый шум). Ключ применяется к скрываемой информации и трансформирует ее последовательность в последовательность с расширенным спектром.

Метод РСПП по отношению к аудиосигналам заключается в следующем. Сигнал данных умножается на сигнал несущей и псевдослучайную шумовую последовательность, характеризующуюся широким частотным спектром. В результате этого спектр данных расширяется на всю доступную полосу. В дальнейшем последовательность расширенных данных ославляется и прибавляется к исходному сигналу как аддитивный случайный шум (рис. 1).

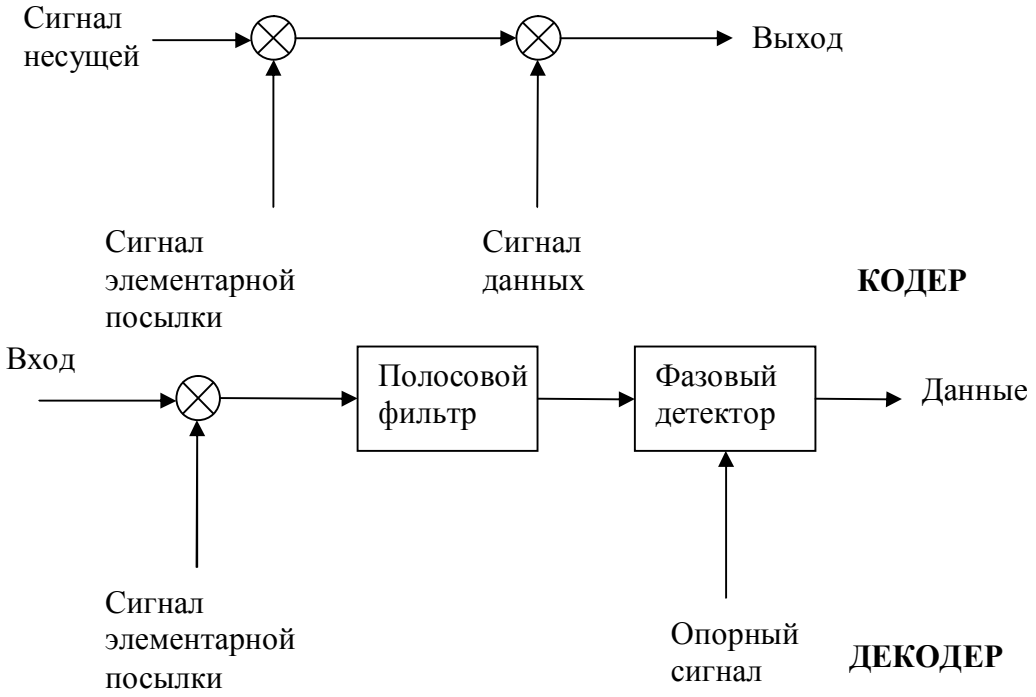


Рис. 1. Структурная схема кодека с расширением спектра

РСПП использует двоичную фазовую манипуляцию, поскольку фаза сигнала псевдослучайной последовательности поочередно чередуется с фазой, модулированной двоичной последовательностью сообщения (рис. 2).

На стадии извлечения фазовые значения φ_0 и $\varphi_0 + \pi$ интерпретируются, соответственно, как биты «1» и «0», которыми кодировалась двоичная последовательность данных. При этом предусматривается следующее:

- псевдослучайный ключ представляет собой *M*-последовательность (т.е. он имеет максимально возможное количество комбинаций, которые равномерно распределены в заданном диапазоне, и максимально долго не повторяются). Следовательно, он имеет относительно плоский частотный спектр;
- принимающей стороне известен поток ключей для шифрования, выполнена синхронизация сигнала, а также известны точки начала и конца расширенных данных;
- принимающей стороне также известны следующие параметры: частота следования элементарных посылок, скорость передачи данных и частота (вид) несущей.

Объединение несложной техники повторения и кодирования с исправлением ошибок позволяет гарантировать целостность двоичной последовательности. Короткие сегменты двоичной кодовой комбинации объединяются и складываются с сигналом аудиоконтейнера таким образом, чтобы уменьшить шумы переходных процессов. Для этого в процессе декодирования проводится усреднение по всему сегменту.

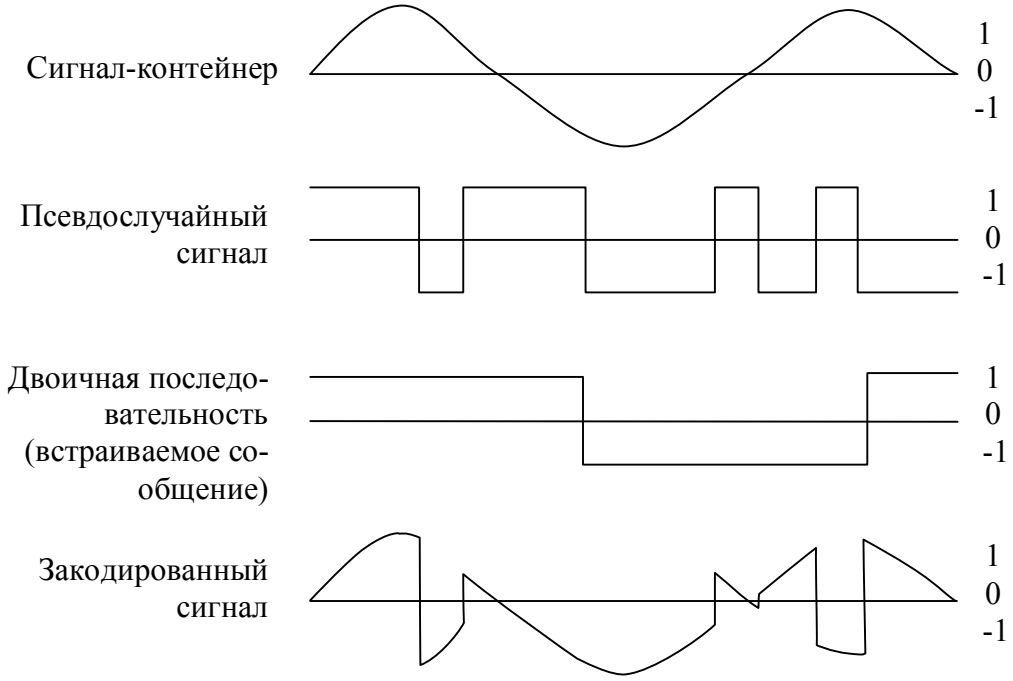


Рис. 2. Информация, синтезированная расширением спектра и шифрованная методом прямой последовательности

Реализация алгоритма

Реализация представленного метода кодирования расширением спектра с помощью прямой последовательности имеет следующие этапы.

Шаг 1

Начальные данные:

- считанные и подготовленные аудиоданные из звукового файла, выбираемого пользователем. Длина данных *I*. (В качестве контейнера выберем левый канал стереофайла);

- введенное пользователем сообщение M длиной L_M бит.

Для встраивания L_M битового сообщения в контейнер, имеющий I дискретных отсчетов, последний разобьем на L_M сегментов длиной

$$SegLen = \mathrm{Math.Floor}(I),$$

где *Math.Floor()* – функция отсечения дробной части (округление до целого числа в меньшую сторону).

Каждый сегмент будет предназначен для встраивания одного бита сообщения.

Шаг 2

Для каждого бита сообщения необходимо сгенерировать псевдослучайную последовательность в виде последовательности ± 1 длиной, как минимум, *SegLen* элементов. За основу генератора псевдослучайных чисел можно взять регистр сдвига с линейной обратной связью (РСЛОС).

Как известно, РСЛОС состоит из двух частей: собственно регистра сдвига и функции обратной связи (рис. 3). Регистр сдвига представляет собой последовательность битов (разрядов) R, количество которых d определяется длиной регистра сдвига. Обратная связь представляет собой сумму по модулю 2 определенных битов регистра (эти биты называются отводной последовательностью) [3].

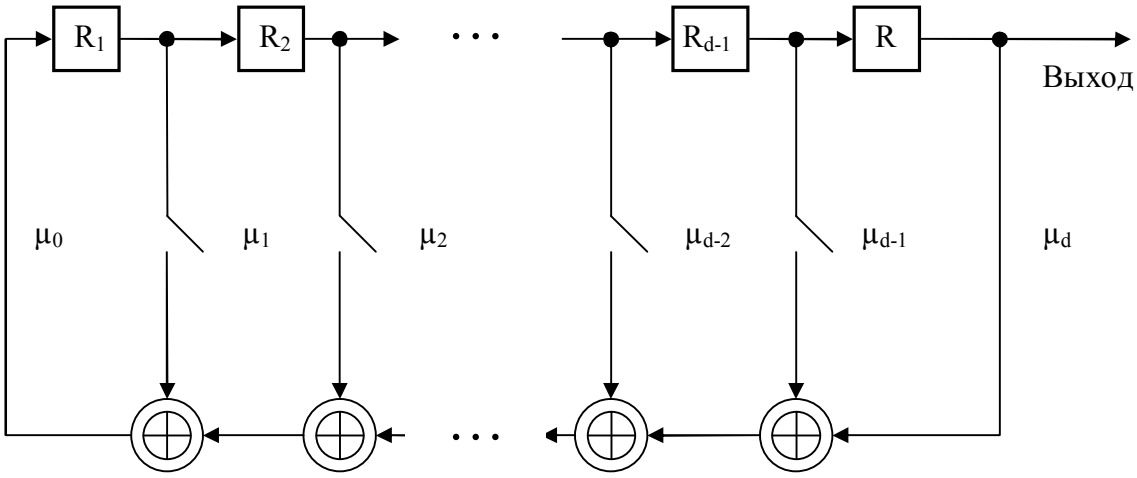


Рис. 3. Обобщенная схема работы регистра сдвига с линейной обратной связью

Теоретически, d-битовый РСЛОС может пребывать в одном из $2^d - 1$ внутренних состояний, то есть может генерировать псевдослучайную последовательность с периодом в $T = 2^d - 1$ бит. Все T внутренних состояний регистр пройдет только при определенных отводных последовательностях. Такие РСЛОС имеют максимальный период, а полученный при этом результат называют M-последовательностью**.**

На рис. 3 значения μ_i (i = 0, 1, …, d) являются весовыми коэффициентами полинома степени d, ассоциированного с последовательностью:

$$\rho(x) = \mu_0 \cdot x^0 + \mu_1 \cdot x^1 + \mu_2 \cdot x^2 + \ldots + \mu_{d-2} \cdot x^{d-2} + \mu_{d-1} \cdot x^{d-1} + \mu .$$

Если $\mu_i = 1$, то соответствующий ключ замкнут. В случае $\mu_i = 0$ – разомкнут.

Неудачное включение сумматоров в цепь обратной связи может привести к получению псевдослучайной последовательности, период повторения которой будет меньше максимально возможного при имеющейся разрядности регистра. Для того, чтобы конкретный РСЛОС имел максимальный период, полином $\rho(x)$ должен быть примитивным по модулю 2 (т.е. не раскладываться на произведение двоичных полиномов меньшей степени). При этом коэффициенты μ_0 и μ_d всегда равняются 1, поскольку, в случае $\mu_0 = 0$, полином $\rho(x)$ делится на x и не является примитивным; в

случае $\mu_0 = 0$, даже если полином и примитивный, его степень меньше *d*. Другие коэффициенты выбранного полинома и будут определять схему формирования псевдослучайной последовательности.

В нашем случае достаточное количество разрядов регистра:

$$d = \text{Math.Ceiling}(\log_2(SegLen)),$$

где *Math.Ceiling()* – функция округления до целого числа в бóльшую сторону.

При этом период генерируемой псевдослучайной последовательности составит $2^d - 1 > SegLen$.

Результирующая последовательность определяется наименьшим значащим битом состояния регистра. Руководствуясь достаточностью, процесс генерации длится до получения *SegLen* битов псевдослучайной последовательности. На выходе модуля мы получаем последовательность {0, 1}, преобразованную в последовательность {−1, 1}.

Шаг 3

На этом этапе выполняется непосредственно встраивание битов сообщения в контейнер.

Вначале строка символов сообщения преобразовывается в вектор значений {−1, 1}. На этом этапе можно также применить какой-либо криптографический метод для шифрования встраиваемого сообщения.

Далее весь контейнер делится на количество сегментов равной длины, соответствующее количеству битов во встраиваемом сообщении, то есть для одного бита сообщения отводится один сегмент. Каждый полученный бит накладывается с помощью соответствующей сгенерированной псевдослучайной последовательности на один сегмент исходного контейнера путем модификации каждого 16-битного отсчета внутри сегмента. При этом энергию ЦВЗ задает параметр *alpha*. Он выбирается исходя из требований стойкости встраиваемого ЦВЗ и незаметности модификации носителя. Этот параметр можно рассматривать как уровень шума (в процентах), вносимого при встраивании сообщения, по отношению к исходному сигналу. Рекомендуемое значение порядка одной сотой (что соответствует примерно 1 % искажения исходного контейнера).

Модифицированные сегменты далее объединяются в общий вектор. После встраивания последнего бита сообщения это вектор удлиняется до длины исходного сигнала конечными, не претерпевшими модификации элементами начального контейнера.

При большом значении параметра *alpha* увеличивается вносимый в исходный контейнер аддитивный шум, что приводит к ощутимым на слух искажениям, которые также можно наблюдать на временных диаграммах.

После встраивания ЦВЗ измененный контейнер объединяется со вторым немодифицированным каналом и записывается в WAV-файл.

Шаг 4

Процесс извлечения заключается в следующем. После открытия файла, содержащего ЦВЗ, из массива данных выделяется левый (первый) канал, в который было произведено встраивание.

Принимающая сторона должна иметь оригинальный аудиофайл, из которого тоже извлекается соответствующий аудиоканал. Известным также должно быть число *SegLen*, представляющее количество 16-битных отсчетов в одном сегменте.

Считывание ЦВЗ производится также с использованием той же самой псевдослучайной последовательности, которая использовалась при встраивании сообщения в сигнал. Определение закодированного значения «0» или «1» происходит на основе анализа разницы между исходным и модифицированным сигналами. Поочередно анализируются все сегменты. В качестве определяющего фактора выступает знак разницы сигналов – если отрицательный, то встроено значение «0», если положительный – значе-

ние «1». Сравнение производится по усредненным значениям всего сегмента, что повышает стойкость к помехам, которые могут возникнуть при передаче сигнала.

В случае применения криптографической защиты при встраивании сообщения, извлеченные данные расшифровываются.

Заключение

В работе рассмотрены основные шаги практической реализации алгоритма встраивания ЦВЗ в аудиосигнал методом расширения спектра прямой последовательностью. Выбранный алгоритм имеет отличные показатели скрытности и устойчивости к преобразованиям.

Стоит отметить, что применение комбинированных методов защиты – криптографических и стеганографических – является удачным решением, повышающим стойкость встроенных данных к обнаружению, модификации, уничтожению, обеспечивая защиту данных одновременно на нескольких уровнях.

Перспективы развития стеганографических методов защиты авторских прав предполагают их дальнейшее изучение с целью увеличения скрытности и стойкости встраиваемой информации, в то время, как развитие стегоанализа направлено на поиски новых методик детектирования скрытой информации, ее извлечения и удаления.

Литература

1. W. Bender, D. Gruhl, N. Morimoto, A. Lu. Techniques for Data Hiding // IBM Systems Journal. – 1996. – №35 (3 & 4). – С. 313–336.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика. – Киев: МК-Пресс, 2006. – 288 с., ил.
3. Скляр Б. Цифровая связь: Теоретические основы и практическое применение. – 2-е изд., исправл. – М.: Вильямс, 2003. – 1104 с.

УДК 681.4

УЧЕБНЫЙ КОМПЛЕКС «DES-CRYPT» КАК ПОСОБИЕ ДЛЯ ИЗУЧЕНИЯ БЛОЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ СЕТИ ФАЙСТЕЛЯ И РЕЖИМОВ ШИФРОВАНИЯ НА ПРИМЕРЕ АЛГОРИТМА DES

Р.А. Саврулин, Н.В. Благодарный, А.В. Горбачев, И.С. Панов
Научный руководитель – О.В. Михайличенко

«DES-crypt» – интерактивный учебный комплекс для дистанционного изучения студентами в рамках предмета «Криптографические методы и средства обеспечения информационной безопасности» темы «Блочные шифры и режимы шифрования». «DES-crypt» демонстрирует работу блочных алгоритмов на примере алгоритма DES в различных режимах шифрования, сопровождая работу методическим материалом.

Ключевые слова: шифрование, учебный комплекс, блочные алгоритмы

Введение

Большое количество учебных пособий и справочной литературы по криптографии зачастую являют собой текстовые материалы. С целью облегчения изучения темы «Блочные шифры и режимы шифрования» в рамках предмета «Криптографические методы и средства обеспечения информационной безопасности» необходимо использовать не только справочную литературу, но и интерактивные программные комплексы визуализирующие процесс работы алгоритмов шифрования.

В основу учебного комплекса был взят алгоритм DES, поскольку подробное изучение DES позволит понять принципы, заложенные в структуру других алгоритмов традиционной схемы шифрования. В сравнении со схемами на основании открытого ключа, структура DES, равно как и большинства других алгоритмов традиционной схемы, очень сложна и поэтому не может быть описана так просто, как структура RSA.

Исходя из вышесказанного, был разработан интерактивный учебный комплекс «DES-crypt», детально демонстрирующий работу блочного алгоритма в разных режимах шифрования, визуализируя процесс шифрования и дешифрования сообщений в различных режимах шифрования.

Постановка задачи

Целью данной работы является разработка веб-приложения с возможностью дистанционного изучения блочных алгоритмов и режимов шифрования.

Разработка учебного комплекса

«DES-crypt» разработан в виде web-приложения, включающим в себя серверную и клиентскую часть. Серверная часть приложения может функционировать под управлением любой современной операционной системой, способной обеспечить корректную работу web-сервера и модуля исполнения скриптов PHP [1]. Для работы клиентской части необходимо использовать web-браузер с поддержкой Javascript.

Результаты моделирования

В ходе моделирования целесообразным было признано разбиение приложения (сайта) на четыре модуля (страницы), исходя из их функционального назначения:

(1) Главная страница – ссылки на изучение теоретических данных, режимов шифрования, дешифрования.

(2) Модуль «Методичка» – теоретический материал по теме «Блочные шифры и режимы шифрования».
(3) Модуль «Шифрование данных» – ввод сообщения, ключа, выбор и описание режима шифрования, выбор файла для шифрования [2].
(4) Модуль «Дешифрование данных» – ввод шифротекста, ключа, выбор режима и файла дешифрования.
(5) Модуль «About» – информация о разработчиках.

Основной результат

В результате написания и отладки программного кода, согласно разработанной модели, был получен продукт (сайт) следующей структуры и функциональности:

Модуль «Методичка»

В модуле представлена необходимая теоретическая информация о блочных алгоритмах и режимах шифрования. Максимально полно рассмотрены основные термины и понятия необходимые для выполнения практической работы, а так же представлен графический материал (схемы, алгоритмы), рис. 1.

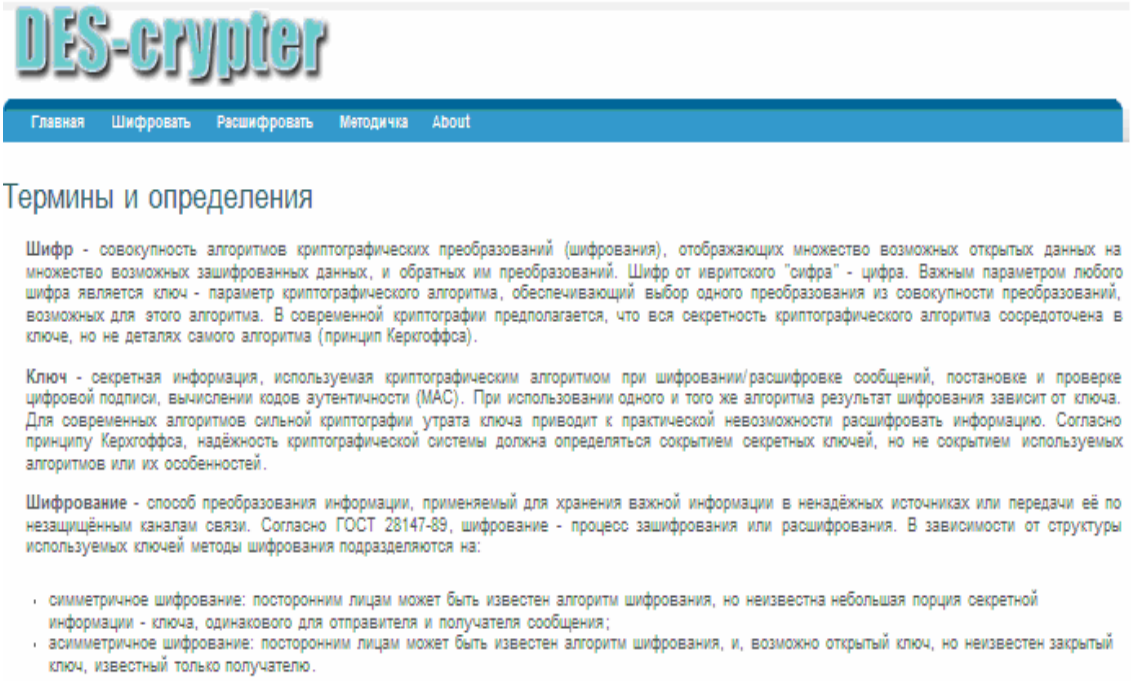


Рис. 1. Теоретические данные модуля «Методичка»

Модуль «Шифрование данных»

Модуль «Шифрование данных» представляет возможность шифровать файлы и введенные сообщения в поле для ввода с последующим выбором режима шифрования, см рис. 2.

Для шифрования файлов необходимо выбрать файл произвольного размера, ввести ключ, выбрать режим шифрования и нажать клавишу «Зашифровать файл». Модуль позволяет сохранить зашифрованный файл на жестком диске, с возможностью его последующего использования.

Процесс работы с модулем также содержит ссылки на теоретический материал по теме «Режимы шифрования блочных шифров».

Учебный комплекс «DES-crypt» детально иллюстрирует каждый этап шифрования открытого текста, рис. 3.

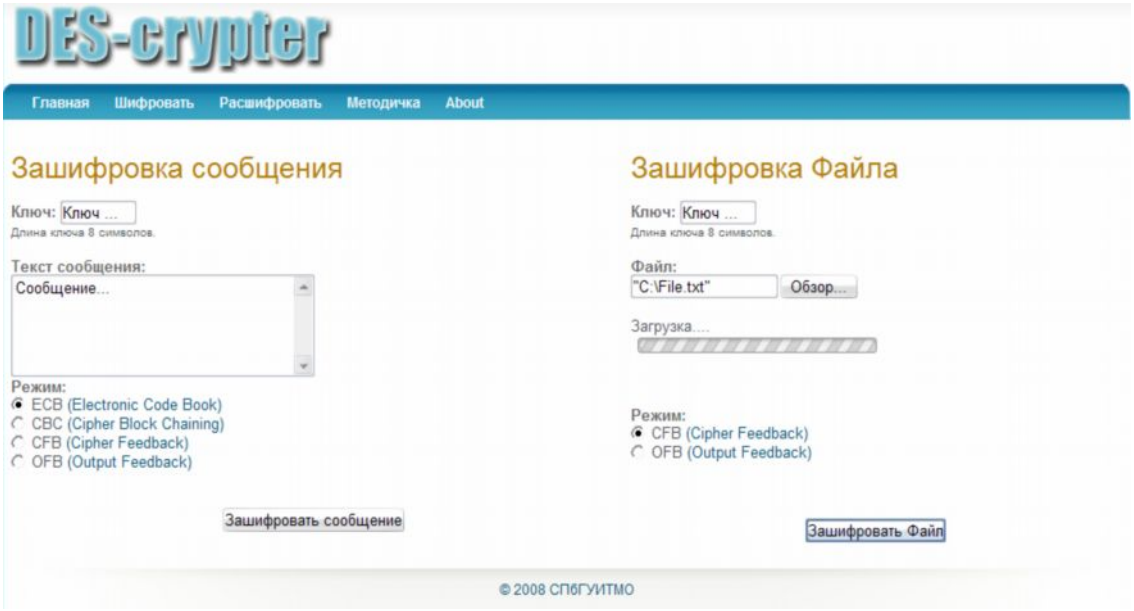


Рис. 2. Модуль «Шифрования данных»

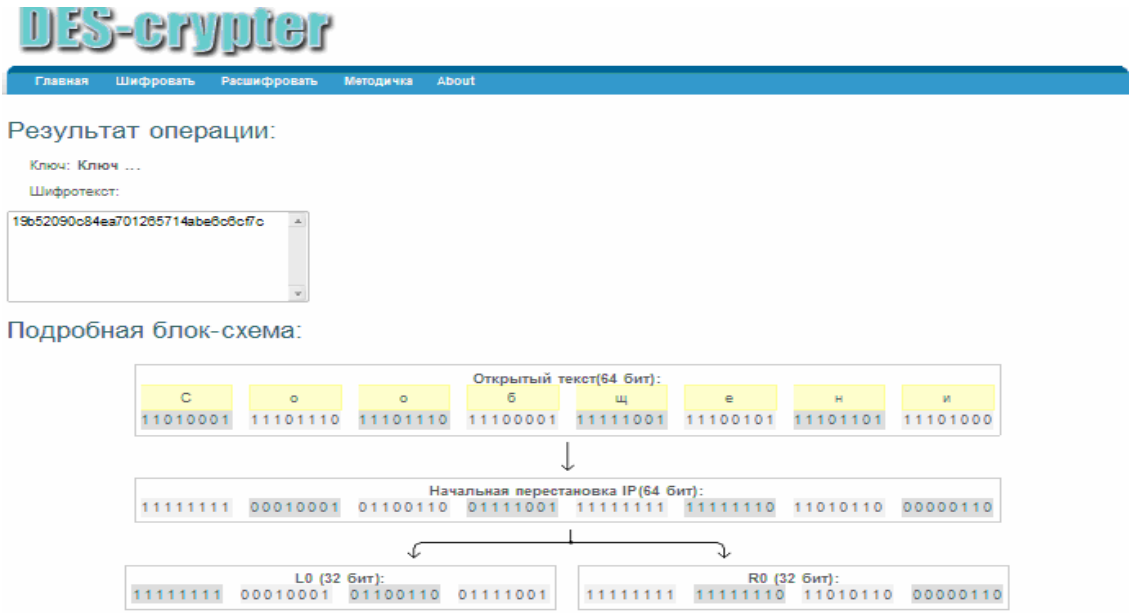


Рис. 3. Результат операции шифрования данных

Модуль «Дешифрование данных»

«Модуль дешифрования» позволяет дешифровать данные зашифрованные в «Модуле шифрования». Интерфейс взаимодействия абсолютно аналогичен интерфейсу модуля шифрования.

Для дешифрования зашифрованного текста необходимо ввести шифротекст в форму для ввода, ввести ключ, выбрать соответствующий режим шифрования и нажать «Расшифровать сообщение», рис. 4.

Для дешифрования шифрованных файлов необходимо выбрать файл произвольного размера в форму для ввода файла, ввести ключ, выбрать режим шифрования и нажать «Расшифровать Файл». После нажатия появляется диалоговое окно, предлагающее сохранить или открыть уже дешифрованный файл, рис. 4.

После дешифрования появляется схема алгоритма, детально иллюстрирующая каждый этап дешифрования шифротекста, рис. 5.

Рис. 4. Модуль дешифрование данных

Модуль «About»

В модуле «About» представлена информация о разработчиках модуля и номер версии и сборки.

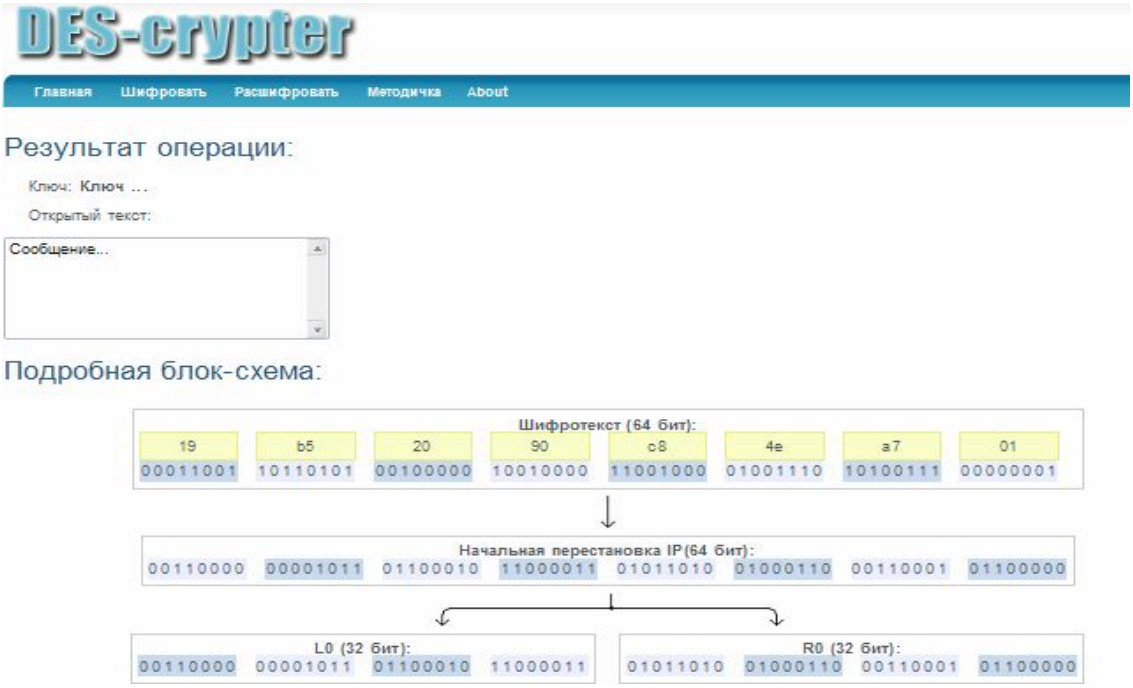


Рис. 5. Результат операции дешифрования данных

Заключение

При использовании интерактивной формы организации образовательной деятельности, обучающийся оказывается вовлеченным в процесс обучения, что способствует детальному усвоению изучаемого материала.

Интерактивный учебный комплекс «DES-crypt» можно использовать в качестве обучающе-ознакомительного комплекса, как для выполнения практических работ, так и для дистанционного обучения студентов.

В дальнейшем для развития комплекса планируется ввести другие алгоритмы шифрования для их детального изучения. Также планируется расширение методического и справочного материала, разработка режима пошагового выполнения практических работ.

Литература

1. Кузнецов М., Симдянов И., Голышев С. PHP 5 на примерах. – Изд. БХВ-Петербург. – 2005. – 576 с.
2. Дейв Крейн, Эрик Паскарелло, Даррен Джеймс Ajax в действии. – Изд. Диалектика. – 2006. – 640 с.

УДК 004.413.4

МЕТОДЫ ИНТЕРВАЛЬНОГО ОЦЕНИВАНИЯ В СИСТЕМАХ АНАЛИЗА РИСКОВ

С.В. Савков
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

В работе проводится анализ существующих систем анализа рисков и предлагаются методы интервального оценивания, позволяющие повысить доверие к получаемым оценкам. В качестве базовой модели для использования предлагаемого в работе алгоритма принята почти произвольная по структуре модель факторов риска, которая обеспечивала лишь точечную оценку значимости факторов. А источником идеи для алгоритма послужил способ арифметизации ординальных отношений в методе анализа и синтеза показателей при информационном дефиците.

Ключевые слова: анализ, риски, уязвимость, оценка, информационный дефицит

Введение

Анализ рисков – составная часть управления информационными рисками, в процессе которого оцениваются уязвимости информационной системы к угрозам безопасности, их критичность и вероятность ущерба для анализируемой системы, вырабатываются контрмеры по уменьшению рисков до приемлемого уровня и обеспечивается контроль защиты информационной системы. Важность этого этапа управления обусловлена тем, что, во-первых, анализ уязвимости сети необходим при создании комплексной системы информационной безопасности (ИБ), а во-вторых, необходимостью вложения средств в ИБ [1].

Обзор используемых на практике методик

Наиболее известными российскими программными продуктами в области анализа информационных рисков являются программный комплекс «Гриф», разработанный санкт-петербургской компанией Digital Security, и серия продуктов «АванГард» Института системного анализа РАН.

Построение «модели угроз», наряду с инвентаризацией информационных активов, – один из наиболее важных этапов анализа рисков. Алгоритмы построения таких моделей предлагают многие разработчики программного обеспечения анализа рисков. Например, классификация угроз DSECCT, входящая в состав программного продукта «Гриф», описывает существующие угрозы информационной безопасности и их признаки, позволяет строить модели угроз для условий конкретной информационной системы компании. В качестве инструментов для построения модели можно предложить также методики OWASP (Open Web Application Security Project), DREAD Threat Model, бесплатный программный продукт Microsoft threat modelling tool [2].

Структурная модель

В реальных условиях исходная информация, используемая при анализе рисков, плохо структурирована, неполна, неточна, часто имеет нечисловой характер, все первичные данные, по сути, являются случайными величинами. Следовательно, чтобы повысить адекватность оценок необходимо предусмотреть, во-первых, возможность обработки именно таких, плохо определенных и разнообразных, данных и, во-вторых, обеспечить расчет хотя бы дисперсии используемых для принятия решений показателей. В рассмотренных системах такая возможность не предусматривается, в результате

чего снижается достоверность получаемых оценок и доверие к результатам оценивания.

В основу модели положены 3 множества факторов, описываемых взаимнонепересекающимися множествами:

- множество источников угроз (M_u);
- множество угроз (M_y);
- множество компонентов объекта ($M_к$);

Также рассматривается сводный показатель защищенности (или уязвимости) объекта $z_0 \in Z$, где Z – множество состояний защищенности объекта, характеризуемое измеримыми показателями безопасности.

Угрозы могут индуцироваться не только объектами множества источников. Они могут возникать как следствие других угроз, либо порождаться компонентами самого объекта.

Каждый компонент вносит свой вклад в защищенность всего объекта.

Таким образом можно выделить 5 видов отношений, каждое из которых задается соответствующим отображением между множествами:

- Источники –> Угрозы $(M_u \to M_y)$;
- Угрозы –> Угрозы $(M_y \to M_y)$;
- Угрозы –>Компоненты $(M_y \to M_к)$;
- Компоненты –> Угрозы $(M_к \to M_y)$;
- Компоненты –> Защищенность $(M_к \to Z)$.

Описанную модель можно изобразить в виде графа (точнее взвешенного орграфа), вершинами которого являются элементы модели (факторы риска – источники угроз, угрозы безопасности, компоненты защищаемого объекта), а дуги представляют отношения между ними. На рис. 1 представлена упрощенная модель взаимодействия среды и защищаемого объекта. В действительности, структурная схема зачастую гораздо более сложная, но в общем случае допустимо работать на рассмотренной трехслойной модели.

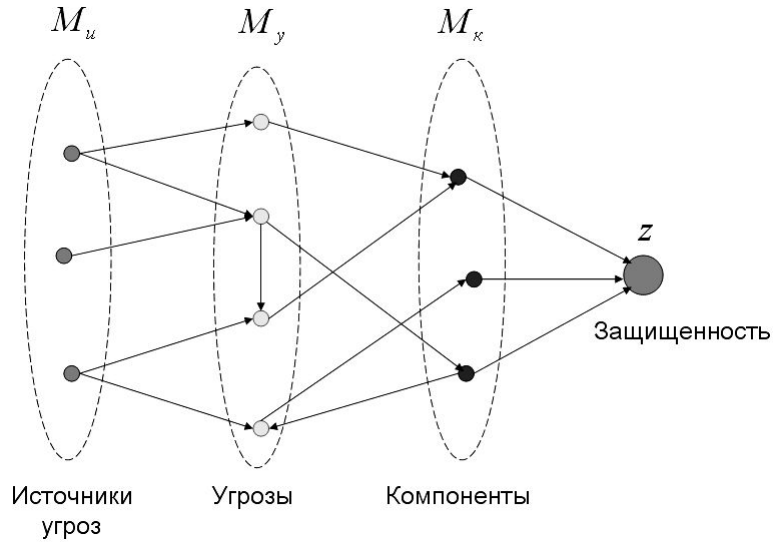


Рис. 1. Структурная модель факторов риска

Веса дуг w_{ij} показывают степень влияния элементов модели друг на друга. Они обладают следующими свойствами: $0 \le w_{ij} \le 1$ и $\sum_i w_{ij} = 1$ (условие нормировки).

В итоге имеет место граф со взвешенными дугами $G(X,U,W)$, где X – множество вершин, U – множество ребер, а $W=\{w_{ij}\}$ – множество весовых коэффициентов.

В рассмотренном графе можно ввести аналогичную по смыслу w_{ij} метрику

$$v_{ij}=\sum_{s}\prod_{t} w^{s}_{t^s}\ , \qquad (1)$$

где t^s – пары индексов всех дуг множества $U_{ij}^{\ s}$ дуг s-го пути из x_i в x_j, $u_{t^s}\in U_{ij}^{\ s}\subset U$; s – индексы путей множества T_{ij} всех путей из x_i в x_j.

Описанную модель можно представить, используя матрицу смежности W графа $G(X,U,W)$, элементами которой будут являться весовые коэффициенты, сопоставленные дугам графа. В блочном виде матрица W выглядит, как показано на рис. 2.

W		1	2	3	4
1	Источники угроз	0	$W_{ИУ}$	0	0
2	Угрозы	0	$W_{УУ}$	$W_{УК}$	0
3	Объект (компоненты)	0	$W_{КУ}$	0	W_{Kz}
4	Состояние объекта	0	0	0	0

Рис. 2. Матрица смежности W

Суммируя степени W по всем значениям i от 1 до такого m≤n, что $W^{m+1}=0$, определяется транзитивная матрица V, содержащая показатели v_{ij} (рис. 3).

$$V=\sum_{i} W^{i}\ . \qquad (2)$$

V		1	2	3	4
1	Источники угроз	0	$V_{ИУ}$	$V_{ИК}$	$V_{Иz}$
2	Угрозы	0	$V_{УУ}$	$V_{УК}$	$V_{Уz}$
3	Объект (компоненты)	0	$V_{КУ}$	$V_{КК}$	V_{Kz}
4	Состояние объекта	0	0	0	0

Рис. 3. Транзитивная матрица

На практике, транзитивная матрица вычисляется по формуле

$$V=(I-W)^{-1}-I\ , \qquad (3)$$

где I – единичная матрица.

Данная формула получается из (2) при условии, что матрица $(I-W)$ – неособенная, то есть для нее существует обратная матрица [3].

Алгоритм интервального оценивания

Источником идеи для алгоритма интервального оценивания послужил способ арифметизации ординальных отношений в методе анализа и синтеза показателей при информационном дефиците (АСПИД) [4], но применяемый ранее только для простых расслоенных или древовидных структур.

Метод позволяет, имея нечисловую либо неполную информацию об отношениях, получить значения их математических ожиданий и дисперсий для использования в расчете.

Предполагается, что компоненты вектора весовых коэффициентов $w=(w_1,...,w_m)$ отсчитываются дискретно с шагом $h=1/n$, где n – число градаций значимости отдельных показателей, измеряемой весовыми коэффициентами. То есть весовые коэффициенты принимают значения из множества $\{0,1/n,2/n,...,(n-2)/n,(n-1)/n,1\}$.

Таким образом, множество $W(m,n)$ всех возможных векторов весовых коэффициентов конечно и имеет конечное число $N(m,n)$ различных элементов, определяемое формулой

$$N(m,n)=\frac{(n+m-1)!}{(m-1)!n!}.$$

Наиболее устойчивой и простой для восприятия является нечисловая ординальная (порядковая) информация, формализуемая при помощи системы равенств и неравенств вида $w_i=w_j$, $w_r>w_s$, $i,j,r,s\in\{1,...,m\}$, для весовых коэффициентов $w_1,...,w_m$.

Другой вид информации, доступной исследователю, есть неточная (интервальная) информация, формализуемая при помощи неравенств вида $a_i\le w_i\le b_i$, $i=1,...,m$, где $0\le a_i\le b_i\le 1$. Интервальная информация указывает диапазоны $[a_i,b_i]$ для допустимых значений весовых коэффициентов.

Учет описанной нечисловой (порядковой), неточной (интервальной) и неполной информации I о весовых коэффициентах $w_1,...,w_m$ позволяет, обычно, существенно сократить множество $W(m,n)$ всех возможных векторов весовых коэффициентов до некоторого непустого множества $W(m,n;I)$ всех допустимых (с точки зрения информации I) весовых векторов [4].

Для случая m=3, получение множества $W(m,n;I)$ можно наглядно изобразить на пространственном графике (рис. 4). Условие нормировки $w_1+w_2+w_3=1$ задает в координатах (w_1,w_2,w_3) – плоскость, на которой расположены элементы исходного множества $W(m,n)$.

При задании различного вида исходной информации, получаем часть плоскости, содержащую элементы множества $W(m,n;I)$.

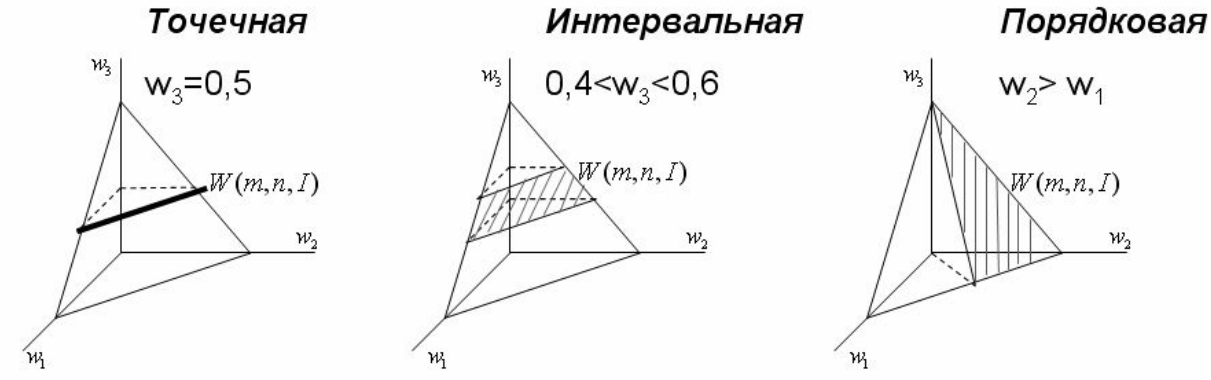


Рис. 4. Выбор множества векторов с учетом исходной информации

Преимущество описанного метода в том, что таким способом можно задать любые исходные данные, в том числе и в лингвистическом представлении. От способа задания исходной информации будет зависеть форма геометрической фигуры – части плоскости, содержащей множество $W(m,n;I)$.

Неопределенность выбора вектора $w=(w_1,...,w_m)$ из множества $W(m,n;I)$ моделируется путем рандомизации этого выбора, в результате которой весовые коэффициенты превращаются в случайные величины $\tilde{w}_1(I),...,\tilde{w}_m(I)$, имеющие совместное равномерное распределение на множестве $W(m,n;I)$.

Теперь в качестве числовых оценок $\overline{w}_i(I)$ весовых коэффициентов, удовлетворяющих равенствам и неравенствам системы I, можно использовать, например, математические ожидания $M\tilde{w}_i(I)$ рандомизированных весовых коэффициентов $\tilde{w}_i(I)$, $i=1,...,m$, образующих случайный весовой вектор $\tilde{w}(I)=(\tilde{w}_1(I),...,\tilde{w}_m(I))$. Точность таких оценок естественно определить при помощи дисперсий $D\tilde{w}_i(I)$ и стандартных отклонений $s_1(I),...,s_m(I)$ соответствующих случайных «весов».

Далее, используется матричный алгоритм расчета показателей на базовой модели, но вместо арифметических операций над числами при точечном задании исходных данных применяются соответствующие стандартные интегральные операторы над случайными величинами.

Ранее, для транзитивных показателей v_{ij} мы приводили формулу (1). Теперь вместо чисел w_i мы имеем случайные величины $\tilde{w}_i$. Пусть w_1 и w_2 – две случайные величины из этого набора, имеющие функции распределения $f(w_1)$ и $g(w_2)$ соответственно. Тогда для их суммы $w=w_1+w_2$ справедливо выражение:

$$p(w)=\int f(z)g(w-z)dz=\int f(w-z)g(z)dz. \qquad (4)$$

Для произведения $w=w_1\cdot w_2$

$$p(w)=\int\left|\frac{1}{z}\right|f(z)g(\frac{w}{z})dz=\int\left|\frac{1}{z}\right|f(\frac{w}{z})g(z)dz. \qquad (5)$$

Приведенные выражения (4) и (5), доказанные в [5] позволяют найти распределения для показателей удаленного влияния v_{ij}, пользуясь формулой (1). А зная функции распределения искомых показателей, можно найти их характеристики (например, моменты распределений) [6].

Заключение

Рассмотренный в работе метод, в отличие от применяемых на практике в экспертных системах, позволяет получать интервальную оценку информационных рисков. Преимущество метода в том, что исходные данные могут быть представлены различным образом, как в числовом (точечном, интервальном), так и в нечисловом (лингвистическом, ординальном) виде. По сравнению с методиками, применяемыми в других экспертных системах, повышается достоверность оценок и доверие к результатам оценивания.

Литература

1. Хохлов Н.В. Управление риском. – М.: Юнити-дана. – 1999. – 239 с.
2. Медведовский И.Д. Современные методы и средства анализа и контроля рисков информационных систем компаний, 2004. [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/analytics/216326.php
3. Шишкин В.М. Метамодель анализа, оценки и управления безопасностью информационных систем // Проблемы управления информационной безопасностью: Сбор-

ник трудов Института системного анализа Российской академии наук / под ред. Д.С. Черешкина. – М.: Едиториал УРСС, 2002. – С. 92–105.
4. Хованов Н.В. Анализ и синтез показателей при информационном дефиците. – СПб: Издательство СПбГУ. – 1996. – 204 с.
5. Хан Г., Шапиро С. Статистические модели в инженерных задачах / пер. с англ. Е.Г.Коваленко. Под ред. В.В. Налимова. – М.: Мир. – 1969. – 396 с.
6. Савков С.В., Шишкин В.М. Исследование возможностей и разработка алгоритма интервального оценивания в системах анализа рисков // XI Санкт-Петербургская международная конференция «Региональная информатика-2008», Санкт-Петербург, 22–24 октября 2008г.: Труды, СПб. – 2009. – С. 135–141.

УДК 535.5

ОПТИМИЗАЦИЯ ЗАДАЧИ ВЫЧИСЛЕНИЯ ПАРАМЕТРОВ МАССОПЕРЕНОСА ЖИДКОЙ БИНАРНОЙ СРЕДЫ С ГРАНИЦЕЙ РАЗДЕЛА

А.А. Лысак, М.В. Якушенков
Научный руководитель – к.т.н., доцент З.Г. Симоненко

Данная работа посвящена вопросам оптимизации задачи вычисления процесса измерения параметров массопереноса жидкой бинарной среды с границей раздела, востребованных при разработке пакета программ для автоматизации мониторинга массопереноса сплошных сред.

Ключевые слова: оптимизация, информационно-измерительная система, процесс массопереноса, математическое описание, алгоритм, математическая модель, программа вычисления

Введение

В современном приборостроении в центре внимания инженеров-системотехников оказываются все более сложные системы, что затрудняет использование физических моделей, но повышает значимость математических моделей и имитационного моделирования систем.

В математической физике задача массопереноса в жидкой бинарной среде рассматривается для стационарного случая в бесконечном вертикальном цилиндре при условии, что концентрация C в любом горизонтальном сечении этого цилиндра зависит от момента времени τ и расстояния X сечения от поверхности раздела двух сред. Решается она с помощью второго уравнения Фика [1] в частных производных с заданными коэффициентами:

$$\frac{\partial}{\partial}\frac{C}{\tau} = D\frac{\partial^2 c}{\partial x^2}. \qquad (1)$$

При постановке задачи массопереноса для оптических методов градиент концентрации заменяется на градиент показателя преломления (или изменение разности фаз).

В настоящее время в механике сплошных сред (МСС) феноменология процесса массопереноса жидких бинарных сред изучается с помощью информационно-измерительной системы (ИИС), созданной на использовании методов и приборов поляризационной интерферометрии с элементами нуль-эллипсометрии [2]. ИИС позволяет наиболее точно исследовать изменение разности фаз между двумя ортогонально поляризованными интерферирующими пучками, пропорциональную переносу масс жидкой бинарной среды.

Целью данной работы является поиск оптимального решения задачи вычисления параметров массопереноса, получаемого с помощью быстродействующих программ для обеспечения целей мониторинга реального процесса массопереноса.

Основная часть

При системном подходе к выявлению путей решения сформулированой задачи предлагается следующая последовательность действий:

МО – РА – ММ – ПВ,

где МО – математическое описание; РА – реализация алгоритма; ММ – математическая модель; ПВ – программа вычисления.

Выбор того или иного метода в значительной степени определяется постановкой оптимальной задачи, а также используемой математической моделью объекта оптимизации.

Рассмотрим математическое описание (МО), связывающее между собой входные и выходные переменные исследуемого процесса массопереноса в жидкой бинарной среде с границей раздела, приведенное в работах [3].

Такая связь зачастую выражается системами дифференциальных уравнений в частных производных (например, в задачах механики твердого тела, жидкости и газа

На основании этого описания используем трансцендентное уравнение, которое имеет следующий вид:

$$\frac{erf\left[\frac{1}{\sqrt{4D\tau_3}}(X_0+\alpha/2)\right]-erf\left[\frac{1}{\sqrt{4D\tau_3}}(X_0-\alpha/2)\right]-erf\left[\frac{1}{\sqrt{4D\tau_2}}(X_0+\alpha/2)\right]+erf\left[\frac{1}{\sqrt{4D\tau_2}}(X_0-\alpha/2)\right]}{erf\left[\frac{1}{\sqrt{4D\tau_2}}(X_0+\alpha/2)\right]-erf\left[\frac{1}{\sqrt{4D\tau_2}}(X_0-\alpha/2)\right]-erf\left[\frac{1}{\sqrt{4D\tau_1}}(X_0+\alpha/2)\right]+erf\left[\frac{1}{\sqrt{4D\tau_1}}(X_0-\alpha/2)\right]}=1, \quad (2)$$

где параметры имеют следующий физический смысл: τ_1, τ_2, τ_3 – измеряемые интервалы времени (с); D – коэффициент массопереноса ($м^2 \cdot с^{-1}$); X_0 – расстояние от границы раздела двух жидких сред до прямой, равноудаленной от двух ортогонально поляризованных интерферирующих пучков(м), α – расстояние между 1 и 2 ортогонально поляризованными интерферирующими пучками (м). *erf (error function)* – функция ошибок Гаусса, которая изменяется от 0 до 1.

При решении уравнения (2) для получения численных значений, характеризующих соответствие вычисленных и экспериментально измеренных параметров массопереноса, выбраны заданные начальные и граничные условия, а также экспериментально полученные параметры:

$\alpha = 4*10^{-4}$ (м), $X_0 = 4{,}5 * 10^{-4}$*(м),* $D = 1{,}88*10^{-9}$ ($м^2*с^{-1}$),

а также $\tau_1 = 470$, $\tau_2 = 1000$, $\tau_3 = 1436$ (с).

Реализация алгоритма (РА) осуществлена с помощью программы, написанной в среде разработки Microsoft Visual Studio.NET 2003 на языке программирования C#. Математически такая задача сводится к выполнению условия уравнения в окрестностях значений рассматриваемых параметров с учетом наложенных ограничений. Для этих целей рассчитывается функция *erf()* с использованием метода аппроксимации гамма-функции по шести параметрам, описанного Виктором Точ (Viktor Toch) [4]. Общая точность аппроксимированной функции составляет $3 \cdot 10^{-7}$ при 100 итерациях с использованием чисел с плавающей запятой двойной точности) [5–6].

Программа позволяет интерактивно изменять параметры интерполяции переменных для немедленного отображения результата на графике. Основное окно программы представлено на рис. 1.

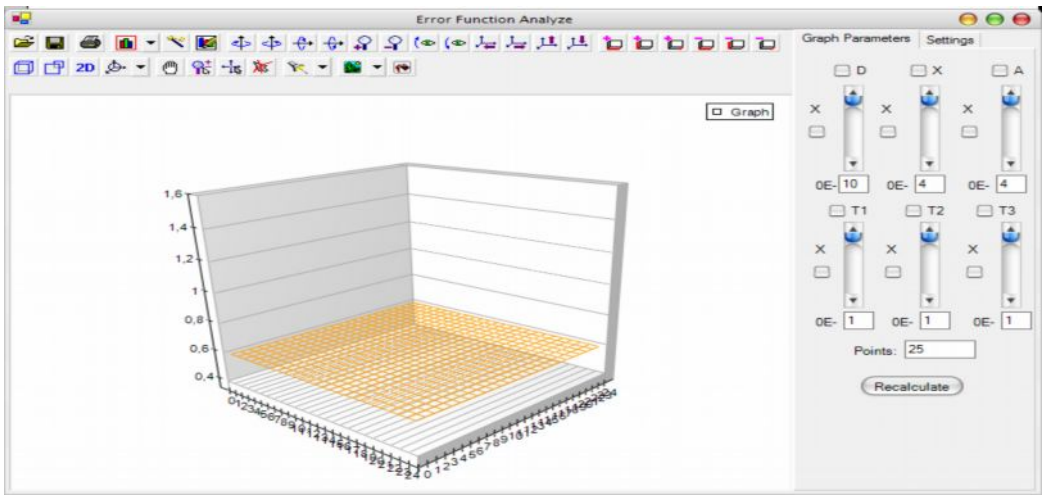


Рис. 1. Основное окно программы

На верхней панели находятся элементы управления отображением графика.

График можно приближать, удалять, вращать вокруг различных осей, изменять способы заливки и отрисовки. На правой панели находится 6 элементов управления 6-и различных параметров графика (рис. 2). Графа Points позволяет задать размер стороны квадратной матрицы графика.

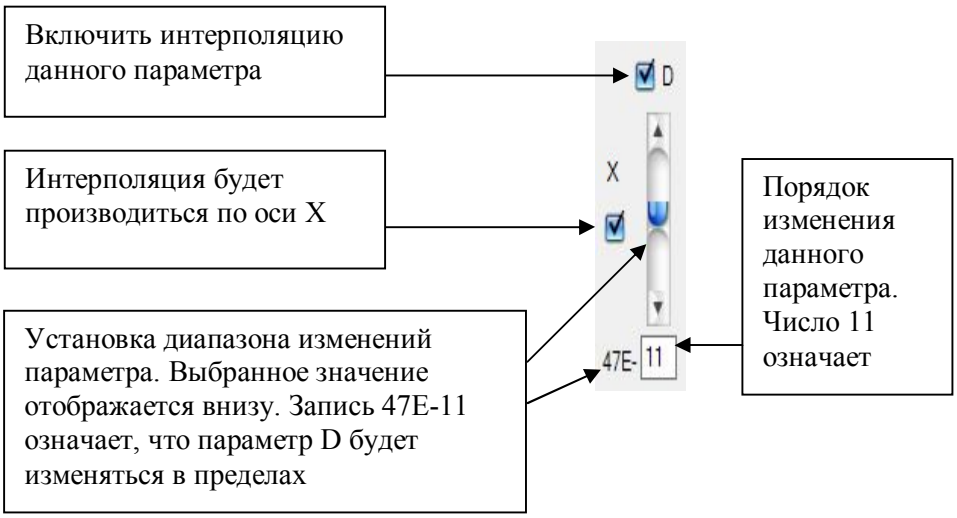


Рис. 2. Панель управления параметрами

На рис. 3 представлен график функциональной зависимости функции *erf()* от изменения параметров D и X_0 по осям X и Y соответственно.

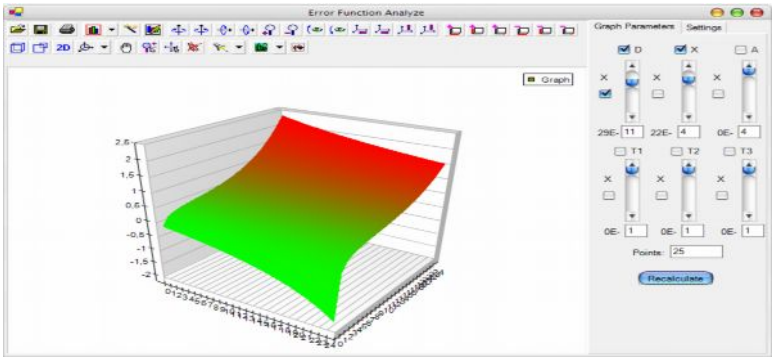


Рис. 3. График функциональной зависимости функции *erf()* от изменения параметров D и X_0 по осям X и Y

Результаты расчетов показали, что созданная программа позволяет проверить выполнение условия уравнения в окрестностях значений параметров, однако точности значений рассматриваемых параметров X_0, α, τ неудовлетворительны.

Это потребовало создания более совершенной программы, написанной на языке C/C++, в среде программирования MinGW. В основе приложения – шаблон диалогового окна, функциональность которого обеспечивается с помощью непосредственного использования прикладного программного интерфейса Win32 API и средствами графического пакета OpenGL) [7].

Программа разработана без применения скриптовых языков программирования, что позволило создать приложение, способствующее более быстрым вычислениям.

Программа содержит шесть подпрограмм, состоящих из шести файлов (файл Diffan.dev, файл main.cpp, файл RenderWindow2D.hpp, файл Diffusion Analyser.rc, файл Erf Analyzer.cpp).

Подпрограмма Diffusion Analyser способна посчитать десятки неизвестных значений меньше чем за минуту, что значительно сокращает время вычисления, при этом выводимый результат имеет точность вычислений порядка девятого знака после запятой. В главное окно Diffusion Analyser выводятся, окна ввода параметров, управляющих кнопок и шкалы прогресса, график исследуемой функции (рис. 4).

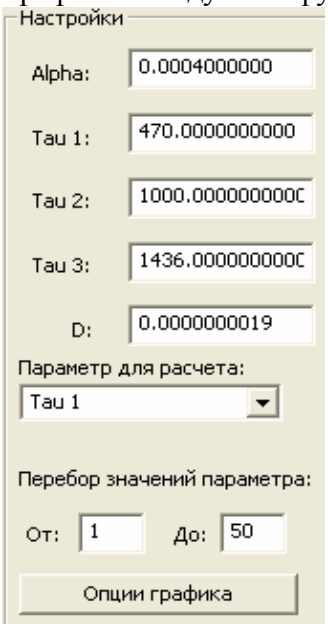


Рис. 4. Интерфейс главного окна

В окне с интерактивным управлением по сравнению с рассмотренной выше программой реализованы следующие возможности графика функции:

1. Перемещение по области графика в любом направлении.
2. Масштабирование графика как по обеим функциональным осям, так и отдельно по оси абсцисс.
3. Вывод с помощью различных режимов отображения.

Для расчета значений трансцендентного уравнения в программе создается отдельный системный поток, т.е. процесс вычислений происходит параллельно работе программы, имеет больший приоритет, и не создает эффекта «временного зависания».

Поток расчета значений выводит части графика «на лету», кроме того, предусмотрено прерывание вычисления в любой момент времени.

В главном окне присутствует блок установки постоянных для изменения значения каждой переменной в трансцендентном уравнении. Отличием от предыдущей программы является предусмотренная возможность выбора временной переменной ($\tau_{1,2,3}$) и требуемая область расчета.

В программе реализована возможность быстрого подсчета одного точного значения, определяемого пользователем (рис. 5). Аргументы для быстрого подсчета можно также ввести вручную, запустив операцию кнопкой «Быстрый подсчет».

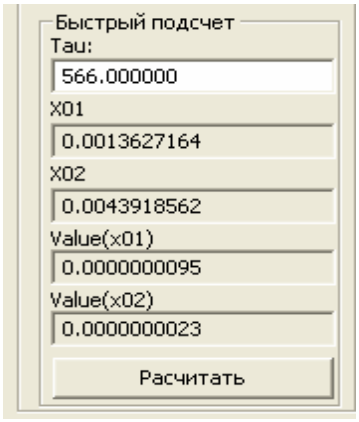


Рис. 5. Интерфейс окна быстрого подсчета

Исследования графика трансцендентной функции позволили сделать необходимые для инициализации начальных значений вычисляемых величин выводы: чем ближе значения функции к нулю, тем выше точность вычислений.

Текущая версия программы пригодна для целей вычисления X_0 и исследования поведения зависимости X_0 от интервалов времени $\tau_{1,2,3}$. Diffusion Analyser находит искомый параметр X_0 с максимальной точностью до 10^{-10}.

Основным достоинством данной программы является скорость, точность вычислений и удобство интерфейса по сравнению с созданной ранее.

Созданные программы позволяют как мгновенные значения параметров так и значения параметров в реальном масштабе времени исследуемого процесса.

Заключение

Решение задачи вычисления параметров массопереноса для обеспечения целей мониторинга процесса массопереноса получено с помощью двух созданных программ, которые могут работать в автономном режиме или дополняют друг друга в зависимости от типа выполняемого задания заказчика.

Для наиболее полного обеспечения целей мониторинга можно рассмотреть возможности дальнейшей доработки программ в следующих направлениях:

1. Возможность решения трансцендентного уравнения не только для X_0, но и для остальных переменных.
2. Возможность совершенствования метода по отбору несуществующих решений, возможность перемещения видимой области увеличенного графика, облегчение масштабирования.
3. Возможность аналитического отсева некорректных решений, что позволит сократить время вычислений еще на порядок.

Литература

1. Симоненко З.Г., Ткалич В.Л. Разработка информационно-измерительной системы неразрушающего контроля параметров массопереноса в жидкой бинарной среде с границей раздела. Учебное пособие. – СПб: СПбГУ ИТМО. – 2006. – 120 с.
2. Маслов В.П., Данилов В.Г., Волосов К.Л. Математическое моделирование процессов массопереноса, Наука. – 1987. – 90 с.

3. Симоненко З.Г. Математическое представление процесса измерения параметров массопереноса в жидкой бинарной среде с границей раздела.// Научно технический вестник. СПб: СПбГУ ИТМО. – Выпуск 23. – 2005. – С. 90–95.
4. Erf calculation using 6 parameter Lanczos approximation http://www.rskey.org/gamma.htm
5. Симоненко З.Г. Использование программ численного решения задач интерференции поляризованного излучения в учебном процессе. Тезисы XXIII научной и учебно-методической конференции СПбГУ ИТМО. 3–6 февраля 2006 года. – СПб. – 2004.
6. Симоненко З.Г., Уваров Д.Л. Программа для расчета параметров массопереноса бинарной жидкой среды с границей раздела. // XXXIV неделя науки СПбГПУ, Материалы Всероссийской межвузовской научно-технической конференции студентов и аспирантов, 28 ноября–3 декабря 2005, Радиофизический факультет, ч. VI. – С. 143–145.
7. Симоненко З.Г., Лысак А.А., Якушенков М.В. Свидетельство о государственной регистрации программы для ЭВМ № 2009610784. Программа для вычисления параметров массопереноса в жидких средах с границей раздела. Зарегистрировано 4.02.2009 г.

УДК 004.4

КОМПЛЕКС ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ НЕЗРЯЧИХ И СЛАБОВИДЯЩИХ ЛЮДЕЙ

С.А. Сергеев, А.Р. Орлов
Научный руководитель – д.т.н., профессор Ю.А. Гатчин

В данной работе рассматривается концепция создания программного комплекса для работы незрячих пользователей с ПК. Цель работы показать высокую необходимость и актуальность подобного программного обеспечения и рассмотреть предлагаемый вариант его создания.
Ключевые слова: инвалид по зрению, незрячие, программное обеспечение

Введение

Известно, что жизнь незрячего человека очень сложна. По данным Всемирной организации здравоохранения, в мире насчитывается 45 миллионов слепых людей и 136 миллионов слабовидящих (с остаточным зрением до пяти процентов). В год слепыми становятся около семи миллионов человек [1]. Осуществление даже простых действий для здорового человека, у человека незрячего может вызывать существенные трудности. Таким людям необходимы помощники, которые, к сожалению, есть не всегда. Таким помощником, расширяющим возможности слепого и способствующим его социальной интеграции, может стать предлагаемый программный комплекс. При помощи современных информационных технологий, например, позволяющих читать электронный текст или понимать человеческую речь, дается возможность более полноценной работы с персональным компьютером.

Адаптация инвалидов с нарушениями зрения является актуальной проблемой не только для государственной службы реабилитации инвалидов и Всероссийского общества слепых, но и для органов здравоохранения и социальной защиты всех регионов РФ [2].

Цель нашего комплекса – обеспечит возможность удобного и вместе с тем максимально полного использование функций ПК для слепых и слабовидящих людей без посторонней помощи.

Не малый упор будет сделан на развитие межпользовательских отношений, на основе раздела связи, который в свою очередь предоставит возможность общения в формате форума, мгновенных сообщений (на подобии icq, magent, Miranda и др.) формата skype связи.

Структура программного комплекса

Комплекс представляет собой систему управления ПК, посредством необходимых приложений, адаптирующих все основные функции и инструменты под незрячего или слабовидящего человека. Оболочка комплекса, встраиваемая вместо стандартного графического интерфейса обеспечивает быструю навигацию по всем разделам, как с помощью мыши, так и помощью клавиатуры, используя 4 клавиши перемещения.

Оболочка – это платформа, скрепляющая воедино все самые необходимые инструменты управления компьютером, поддерживая обновления, она сможет также поставить инвалида в центр развития новых технологий, отодвинув края цивилизации в прошлое.

В комплекс будут входить как самописные программы, так и программы других производителей. Так же возможна установка других программ. Оболочка не только

представляет собой более простой доступ к работе с ПК, но и значительно расширяет возможности его использования незрячим человеком.

Для удобства все программы и функции разбиты на тематические разделы и подразделы (рисунок) как в меню сотовых телефонов, что позволяет осуществлять навигацию по ним, запускать, а также настраивать под индивидуальные потребности каждого пользователя, любого приложения при помощи клавиш навигации.

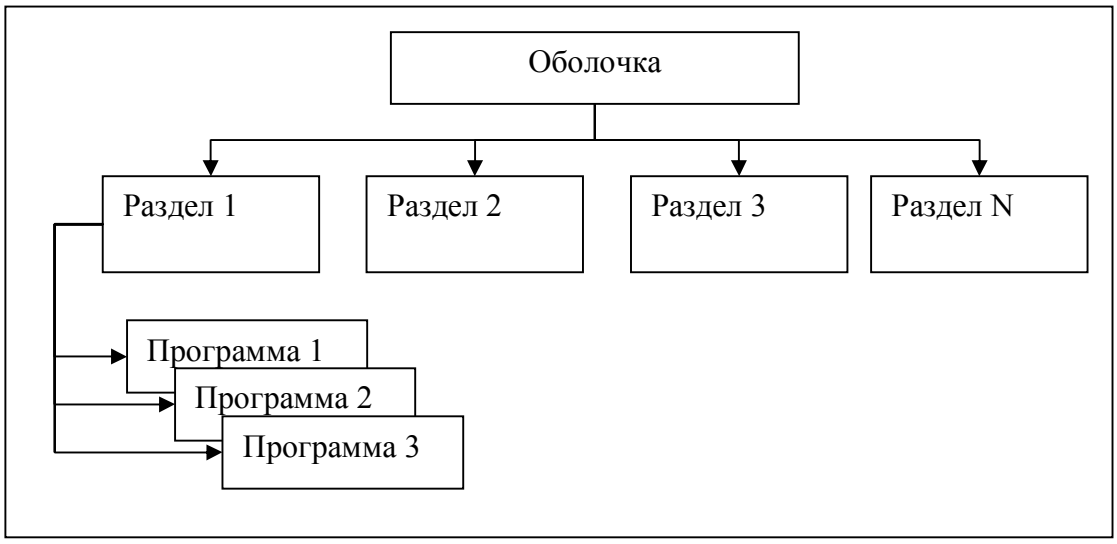


Рисунок. Структура оболочки

Как и любой другой пользователь ПК, незрячий или слабовидящий сможет коротать время, используя приложения раздела «развлечения» и «обучение».

Разделы:

1. Связь.
   - Программы записи звуковых сообщений в аудиофайл и отправка его по емейлу, Она же может получать и воспроизводить такие файлы, а так же читать вслух текстовое содержимое писем.
   - Интерактивный форум на основе функций таких приложений как skype, icq, M/agent и др.
   - Почтовая служба, поддерживающая получение, хранение и отправление звуковых форматов файлов участвующих в первых двух пунктах.
   - Каталог специализированных Интернет ресурсов.
   - Программа поиска в сети Интернет.
2. Домашний офис.
   - Файловый менеджер.
   - Редактирование документов и вывод на печать.
   - Перевод текстов.
3. Обучение.
   - Программа, читающая электронные книги и осуществляющая навигацию по ним.
   - Архив аудио книги лекций как научно образовательного, так и художественного формата.
4. Развлечение.
   - Аудио плеер.
   - Простые звуковые игры.
   - Программы для работы с музыкой и создание мелодий.
5. Настройки и обновление.
   - Настройка работы оболочки.
   - Обновление баз программ и архивов.

- Антивирус и защита.

6. Помощь.
   - Справка по работе с оболочкой.
   - Удаленный помощник.

Вывод

Рассмотренная концепция программного комплекса является актуальной и в достаточной мере доступной для реализации по средствам коллектива молодых разработчиков.

Литература

1. Лисина А. Трогательный взгляд. http://www.subbota.com/2007/10/18/ob008.html [Электронный ресурс].
2. Момот В.А. Медико-психологическая реабилитация инвалидов по зрению. Автореферат.

УДК 004.65:004.91

ЭЛЕКТРОННАЯ СИСТЕМА МОНИТОРИНГА КАРЬЕРНОГО РОСТА СТУДЕНТОВ

А.О. Гречишкин
Научный руководитель – д.т.н., профессор С.А. Арустамов

В статье говорится о системе, направленной на изучение карьеры студента. Система задумывалась как инструмент для сбора статистики по предыстории карьеры студента, а так же по ее развитию. Задачами системы являются автоматизация сбора информации по целому ряду вопросов от карьерного планирования до практических навыков, организация доступа к просмотру и анализу этой информации, стимулирование общения между студентами и выпускниками и помощь в формировании отчетности по учебному курсу в целом.

Ключевые слова: карьерные рост, профессиональный рост, система мониторинга

Введение

Последний век мир переживает настоящий технологический бум: никогда еще научный прогресс не развивался так стремительно. Это не могло не повлиять и на систему образования. В определенные моменты наступала такая ситуация, вузы порой не успевали за новыми стандартами. Конечно же, это затрагивало далеко не все сферы, но определенные проблемы в системе подготовки кадров этот эффект выявил.

С другой стороны ситуация, которая сложилась в современной системе высшего образования в России, тоже имеет свои перекосы. Одним из таких перекосов является политика набора в университеты. При этом сильное влияние оказывает и демографическая ситуация. В настоящее время высшее образование становится более доступным из-за того, что количество абитуриентов идет на спад по сравнению с прошлым десятилетием [5]. Отсюда не возникало проблем с поступлением ни у кого, даже у тех, кто не всегда дотягивал до уровня высшего образования. В общем, благодаря различным причинам, очень часто возникала ситуация, когда на определенную специальность поступали люди, которым она не была интересна, т.е. определенный процент людей заведомо не планировал работать по специальности.

Третьим аспектом можно назвать смещение акцента на формирование междисциплинарных связей в системе высшей школы, что вызывает дефицит практической подготовки. Как следствие, зачастую только маленькая группа способных выпускников, могла работать по специальности [4]. Свой профессиональный выбор оставшаяся большая часть выпустившихся из высших учебных заведений делала не пользу работы по специальности.

Взяв во внимание три вышеназванные причины: бурный прогресс и, как следствие, быстрая изменчивость рынка труда, специфическая ситуация с набором в вузы и разрыв между теоретической и практической подготовкой – университеты получали очень пеструю картину мест работы их выпускников. Как итог, в таких условиях очень трудно корректировать учебные планы, для достижения большей эффективности образования. А то, что большая часть студентов не работает по специальности, является скорее негативным следствием (хотя, конечно, зависящим и от внешних факторов).

Для вузов дело осложнялось еще и тем, что этот процесс (выхода студентов на рынок труда) не был прозрачным. Многие вузы не утруждали себя сбором статистики, следовательно не получали обратной связи от своих студентов, о том, какие знания пригодилось им в большей или меньшей степени. Ситуацию можно было бы значительно улучшить, если бы сбором статистики по профессиональным планам занимались бы начиная с момента начала обучения студента в вузе, тогда можно проследить как меняются предпочтения студента в зависимости от суммы внешних факторов.

Постановка задачи

Итак, обозначенная проблема – *непрозрачность процесса выхода студентов на рынок труда и карьерного планирования студентов*. Это касается в равной степени, как предыстории, так и непосредственно развития карьеры студента.

Негативное явление заключается в том, что сотрудники кафедры не всегда могут ответить на вопрос о том, где работают их студенты, как долго, как они туда попали, чем они занимаются на своей работе. А это, в свою очередь, – проблема, т.к. возникает закономерный вопрос: «А как кафедра получает обратную связь»?

Вуз должен готовить студента к выходу на работу, т.е. давать ему образование, обладая которым студент уже идет работать. При этом, в случае получения качественного образования, студент не должен испытывать серьезных трудностей с поиском работы, т.к. он устраивается на профильную позицию, а приобретенный багаж знаний позволяет ему достаточно легко это сделать. Плохое образование обернется возникновением известного рода трудности с поиском работы, которые зачастую заканчиваются поиском случайных, непрофилирующих вакансий, что в последствии может навсегда перечеркнуть возможность работы по специальности. Как происходит процесс сбора информации обычно? Как правило, кафедра в курсе мест работ студентов, «вхожих» на кафедру. Они охотно рассказывают об этом, да и это часто выясняется само собой в процессе общения. По целому ряду других студентов кафедра имеет определенные догадки, судя по уровню знаний. Догадки эти могут касаться, к примеру, сферы деятельности. По остальным часто отсутствует какая-либо информация, либо это сведения обрывочного характера. О ком-то знают по слухам, есть такие, кто сам говорит, есть такие, о которых вообще ничего не известно. Распространенной практикой в вузах является краткое анкетирование при получении диплома. Но это анкетирование является разовым и не позволяет отследить причины имеющейся на данный момент карьеры.

Незнание того, что происходить со студентами на рынке труда чревато тем, что кафедра не всегда сможет уследить за тем, как меняются предпочтения студента относительно сферы его деятельности в процессе обучения, что кафедра не всегда сможет увидеть, как изменяется сам студент по ходу его учебы, что кафедра не всегда сможет отследить карьерный рост и узнать чем еще занимается студент и планирует ли он вообще работать по специальности. Чревато это еще и тем, что можно не уследить за тем, как меняется рынок труда, вовремя не скорректировать программу обучения на кафедре т.к. обратная связь от студентов не достаточно сильна.

Решению этих проблем посвящена работа. Необходимо создать некий инструмент для мониторинга ситуации. Нужна система, которая будет работать не с оценками (за что отвечает внутренняя ИС университета), а с опытом и предпочтениями студента. Задача системы состоит в том, чтобы дать подробную информацию по каждому студенту относительно его успехов на рынке труда.

Значимость работы заключается в возможности получения обратной связи от студентов для корректировки учебного процесса и понимания желаний студентов и выпускников по поиску работы.

Структура системы

Рассмотрим требования к такой информационной системе.

Цель – *создать систему для сбора и хранения информации о достижениях студентов в их профессиональной деятельности*.

Самая важная часть – это опросник. Все строится на его основе. Собранная информацию в последствии будет обрабатываться для получения той или иной статистики.

Так как система должна работать не только с фактологической частью трудовой истории студента, но и с его предпочтениями, а так же, по возможности, объять всю сферу профессиональных знаний [1], то опросник было решено разбить на шесть частей:

1. **учеба** – в этом разделе студенту предлагается дать оценку учебному процессу, проецируя его на свой опыт работы: какие из изучаемых предметов помогли, какие не очень, чего не хватало, какие предметы давались плохо и т.п. Это позволит дать прямую обратную связь по непосредственно учебному процессу.
2. **работа** – этот раздел разбит на два подраздела: знания и опыт. В знаниях студент должен указать те дисциплины и области, в которых он силен, которые, по его мнению, пригодятся ему в работе. В опыте он должен описать свои предыдущие места работы и дать оценку. В частности, его попросят указать была эта работа временной или постоянной, случайной или целенаправленно искавшейся, попросят рассказать о причинах ухода.
3. **карьерное планирование** – один из самых важных разделов. Студента попросят поделиться его карьерными планами на ближайший семестр и вообще на будущее, вплоть до окончания университета. Это поможет выяснить что происходит «в головах» у студентов, какие настроения, к чему он больше стремится в профессиональном плане.
4. **языки** – этот раздел нужен для сбора информации по уровню владения языками, а так же преследует цель выяснения потребности студента в изучении языка на будущее.
5. **студенческая активность** – собирает информацию по студенческой и социальной активности студентов. Как правило, весьма небольшое количество студентов занимается внеучебной деятельностью в вузе, состоит в различных студенческих сообществах и организация. Но для многих из них это оказывает решающее значение в выборе дальнейшего пути.
6. **творчество** – в этом разделе студент указывает информацию о своих творческих интересах (музыка, спорт и т.п.) в том случае, если они оказывают влияние на его карьеру, подчас фатальное. Эти люди должны быть выключены из общей статистики по трудоустройству, т.к. работа по специальности становится неактуальной для них.

Заполнение анкет предлагается сделать регулярным – раз в семестр.

Вторым по важности элементом системы является возможность просмотра ответов студентов другими студентами. Это позволит скорректировать свой путь более молодым студентам, посмотрев на то, где и кем работают старшие. Так появится возможность общения между студентами разных курсов, а результаты такого межличностного общения очень трудно переоценить.

Следующий, не менее важный модуль – статистика. Статистика нужна в первую очередь для кафедры. Зная ее, можно легко корректировать учебные курсы с учетом изменения рынка труда. Она, по сути, должна давать основную отчетность: процентное распределение трудоустроенных студентов по сферам деятельности, среднее время начала работы и т.п. Она окажет неоценимую помощь при формировании отчетности.

В системе так же предусмотрена возможность дать рекомендации студентам. Зачастую, рекомендации оказывают эффект и могут служить хорошим подспорьем при устройстве на работу. Преподаватель может сам дать рекомендацию понравившемуся студенту, либо студент может попросить об этом преподавателя. Рекомендации будут отображаться в личной страничке студента.

Система позволяет формировать на основе собранной информации онлайн-резюме. Это может оказаться очень полезным для студентов на начальном этапе трудоустройства. На него формируется перманентная ссылка, которую можно рассылать работодателям и резюме будет доступно им в любое время через Интернет.

Заключение

В целом система организованна так, что должна в первую очередь дать полную информацию по студентам в плане их карьеры. При этом она будет полезна и для самих студентов, т.к. на ее основе можно собирать информацию по студентам старших курсов и выпускникам, что в последствии поможет им в определении их карьерного пути.

Литература

1. Аверьянов Л.Я. Социология: искусство задавать вопросы. – 2-е изд., перераб. и доп. – М.: Высш. шк., 1998. – 188 с.
2. Шлосснейгл Дж. Профессиональное программирование на PHP. – СПб: Вильямс, 2005. – 624 с.
3. Веллинг Л., Томсон Л. MySQL. Учебное пособие. – Спб.: Вильямс, 2005. – 304 с.
4. Волков К. Выпускники легкомысленны // Ведомости. – 2007. – 3 авг.
5. Молодежь о карьере: амбиции и реальность (Пресс-выпуск ВЦИОМ) wciom.ru/novosti/press-vypuski/press-vypusk/single/9503.html

УДК 519.688

ПРОГРАММНАЯ СИСТЕМА СЕГМЕНТАЦИИ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ВЫЧИСЛЕНИЯ ОПТИЧЕСКОГО ПОТОКА

Б.Б. Казаков
(Санкт-Петербургский государственный электротехнический университет, ЛЭТИ)
Научный руководитель – к.т.н., доцент С.А. Ивановский
(Санкт-Петербургский государственный электротехнический университет, ЛЭТИ)

В работе сравниваются дифференциальный и тензорный методы вычисления оптического потока. Анализируется основное преимущество тензорного метода. Проводится экспериментальное сравнение тензорного и дифференциального методов с использованием специально разработанной системы визуального программирования.

Ключевые слова: оптический поток, тензоры, МНК, визуальное программирование

Введение

В последнее время в измерительной технике на смену системам регистрации статических изображений всё чаще приходят системы наблюдения, регистрирующие последовательности кадров (изображений). Во многих случаях сегментация изображений и выделение движущихся объектов невозможна или неэффективна, если анализировать кадры по отдельности. Поэтому, для анализа последовательностей изображений вводится понятие оптического потока.

Вычисление оптического потока

Оптический поток есть векторное поле, элементы которого определяют движение конкретных пикселей при переходе от предыдущего изображения к последующему. Для определения оптического потока вводится понятие пространственно-временного изображения. Пусть отдельное изображение определяется как:

$$g_S = F(\bar{x}). \qquad (1)$$

Функция F опредедяет интенсивность светового потока в точке плоскости с координатами $\bar{x}$. Чтобы перейти к описанию видеофрагментов, к параметрам функции F добавляется дополнительная координата t. Пространственно-временное изображение g определяется функцией:

$$g = F(\bar{x}, t), \qquad (2)$$

в которой координата t определяет момент съемки видеокадра.

Существуют различные методы вычисления оптического потока. Дифференциальный метод вычисления оптического потока основывается на анализе основного уравнения неразрывности оптического потока:

$$\frac{\partial g}{\partial t} + f^T \nabla g = 0.$$

Считая, что в локальной окрестности оптический поток является постоянным, и решая уравнение МНК первого порядка, переходим к системе уравнений [1]:

$$\begin{bmatrix} \overline{g_x g_x} & \overline{g_x g_y} \\ \overline{g_x g_y} & \overline{g_y g_y} \end{bmatrix} \begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = -\begin{bmatrix} \overline{g_x g_t} \\ \overline{g_y g_t} \end{bmatrix}, \qquad (3)$$

где $g_x = \frac{\partial g}{\partial x}$, $g_y = \frac{\partial g}{\partial y}$, $g_t = \frac{\partial g}{\partial t}$, f_1, f_2 – компоненты оптического потока по осям x и y.

В качестве альтернативы дифференциальному методу может рассматриваться тензорный метод вычисления оптического потока.

Для определения оптического потока в пространственно-временном изображении необходимо определить ориентацию в каждой точке [1]. Ориентация – это направление постоянства уровней яркости. Для определения ориентации в тензорном методе используется матрица структурного тензора:

$$D = \begin{bmatrix} \overline{g_x g_x} & \overline{g_x g_y} & \overline{g_x g_t} \\ \overline{g_x g_y} & \overline{g_y g_y} & \overline{g_y g_t} \\ \overline{g_x g_z} & \overline{g_y g_z} & \overline{g_t g_t} \end{bmatrix}. \quad (4)$$

Найдя собственные числа матрицы D, и собственный вектор, соответствующий минимальному собственному числу, можно определить оптический поток:

$$\begin{bmatrix} f_1 \\ f_2 \end{bmatrix} = \frac{1}{e_{33}} \begin{bmatrix} e_{31} \\ e_{32} \end{bmatrix}.$$

где $\overrightarrow{e_3}$ – собственный вектор, соответствующий минимальному собственному числу.

Для сравнения дифференциальных и тензорных методов необходимо учесть, что оба метода основаны на анализе матриц производных для нахождения оптимального вектора ОП (3), (4).

Существенным отличием тензорного метода является наличие элемента $\overline{g_t g_t}$ в матрице производных, что позволяет отличить локально-постоянное движение от локально-непостоянного. Это особенно важно, потому что в областях с локально-непостоянным движением корректно вычислить оптический поток невозможно.

Чтобы отделить локально-постоянные области от локально-непостоянных вводится понятие доверительной маски, которая делит плоскость изображения на область доверия (значение равно 1) и область недоверия (значение равно 0):

$$m(x,y) = \begin{cases} 1 & \text{при } \lambda_3 /(\lambda_1 + \lambda_2 + \lambda_3) < c, \\ 0 & \text{иначе}, \end{cases}$$

где λ_1, λ_3 – максимальное и минимальное собственное число матрицы (4). Значение c должно быть мало, например, $c = 1 \times 10^{-4}$.

Аналитическое сравнение двух методов определения оптического потока затруднено тем, что на результаты вычислений оказывают большое влияние ошибки, связанные с дискретным представлением изображений, и использование аппроксимаций. Например, один и тот же метод может давать различные результаты при использовании различных методов вычисления градиента.

Поэтому целесообразно экспериментальное сравнение поведения двух методов на различных моделях изображений.

ПК визуального исследования алгоритмов

Необходимость проведения большего количества экспериментов привела к созданию программного комплекса экспериментального исследования алгоритмов. Основной целью данного ПК является возможность визуального проектирования, исследования и модификации алгоритмов в интерактивном режиме.

Алгоритм описывается в виде направленного графа. Для построения графа программа, реализующая алгоритм, разбивается на смысловые блоки. Отдельный блок представляется в виде черного ящика с набором входных и выходных данных. Блоки соответствуют узлам графа. Поток данных между блоками определяет ребра графа. Для определения семантики ребер каждому из них приписывается имя выходного и входного параметра. Два узла графа могут соединяться больше чем одним ребром при условии, что они (ребра) соответствуют разным входным параметры. Естественным ограничением является то, что к одному узлу не могут присоединяться два ребра с

одинаковым входным параметром. Значение входных параметров блока может задаваться или с помощью ребер (в этом случае значение входного параметра равно значению соответствующего выходного параметра связанного блока и может изменяться при перевычислении блока), или в виде константных значений. Для задания константных значений в ПК существуют стандартные элементы пользовательского интерфейса, позволяющие задавать атомарные значения (числа, строки, булевские значения), списки, массивы произвольной структуры.

Для задания семантики блоков выбран язык python. Перечислим его основные достоинства:

(а) python – интерпретируемый язык; это позволяет менять семантику блоков «на лету» без необходимости перекомпиляции;

(б) наличие обширной библиотеки функций (для языка python существуют библиотеки математических функций, отображения произвольных графиков, пользовательского интерфейса, работы с графами и т.д.) [3];

(в) язык python имеет привычный синтаксис и допускает использование нетипизируемых переменных (нетипизируемые переменные облегчают передачу данных между блоками; синтаксис языка напоминает синтаксис C++, однако имеются существенные отличия).

Любое изменение описания алгоритма или тестовых данных приводит к моментальному перевычислению выходных данных без необходимости перекомпиляции, перезапуска, переконфигурации программы. Результаты промежуточных вычислений буферизуются, что позволяет сократить количество вычислений. При изменении блока анализ графа позволяет выполнять не всю программу целиком, а только последовательность зависимых операторов (подграф графа).

Экспериментальное сравнение тензорного и дифференциального методов

Приведем пример графа алгоритма для сравнения двух методов вычисления оптического потока. В задачу данного сравнения входит определение принципиальных отличий и сравнение точности вычислений оптического потока для двух методов на модельных сигналах. В данном эксперименте основной интерес представляет зависимость точности определения потока от распределения градиента в локальной окрестности.

Выделим основные смысловые блоки программы сравнения:

(а) генерирование модельной последовательности изображений $g(x,y,t)$;

(б) формирование градиента ∇g_a, вычисленного аналитически;

(в) вычисление градиента ∇g_n численными методами;

(г) сравнение двух градиентов (угловая ошибка, ошибка модуля);

(д) вычисление усредненных значений производных $\overline{g_x g_x}$, $\overline{g_y g_y}$, $\overline{g_t g_t}$, $\overline{g_x g_y}$, $\overline{g_x g_t}$, $\overline{g_y g_t}$;

(д) вычисление оптического потока дифференциальным методом;

(е) вычисление оптического потока тензорным методом;

(ж) вычисление доверительной маски;

(з) сравнение двух методов вычисления оптического потока.

Граф программы представлен на рис. 1.

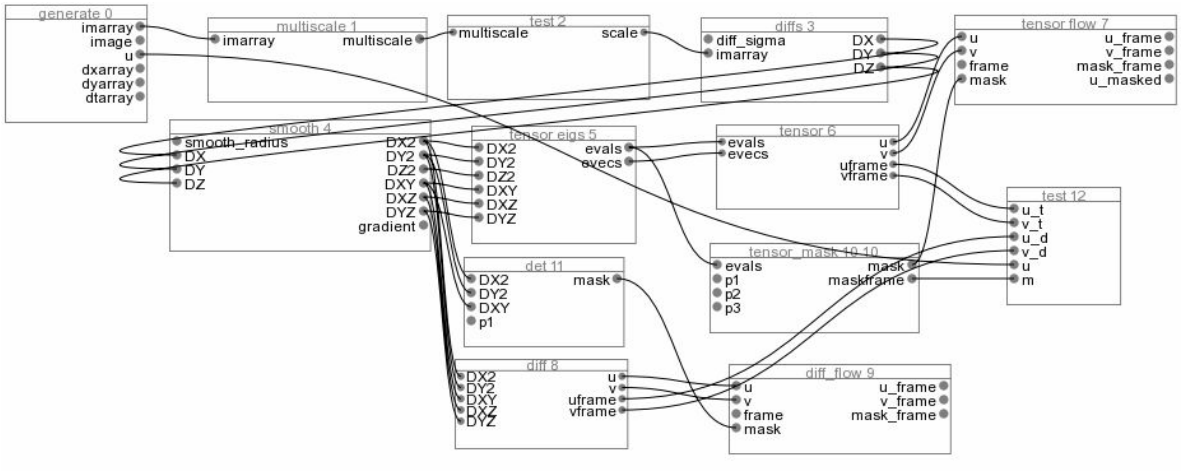


Рис. 1. Граф программы

Были проведены эксперименты с пятью моделями изображений. В табл. 1 представлены модели, описывающие экспериментальные последовательности изображений. Основным предметом исследования была зависимость ошибки определения оптического потока от направления градиента и от периодичности сигнала в этом направлении. Все исследуемые модели сигналов имеют круговую симметрию, т.е рассматривается зависимость от аргумента $R = \sqrt{(x-(u_1 t))^2 + (y-(u_2 t))^2}$. Величина r в таблице является параметром модели, величины u_1, u_2 – компонентами вектора перемещения [1].

Таблица 1. Математические модели последовательностей изображений

N	модель	N	модель
(1)	$g(x,y,t) = \sin\left(\frac{R}{r}\right)$	(2)	$g(x,y,t) = \cos\left(\frac{R}{r}\right)$
(3)	$g(x,y,t) = \left(\frac{R}{r}\right)$	(4)	$g(x,y,t) = \left(\frac{R^2}{r^2}\right)$
(5)	$g(x,y,t) = cos\left(\frac{R^2}{r^2}\right)$		

Для примера, изображение, полученное с помощью модели (2), показано на рис. 2.

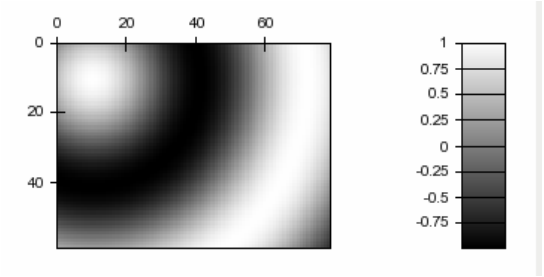


Рис. 2. Одно из модельных изображений, используемых для сравнения методов вычисления оптического потока

Результаты экспериментального сравнения

Рассматривается видеоряд из 10 кадров. Результаты проведенных экспериментов для вычисления оптического потока в отдельном, например, 5-м кадре, представлены в

табл. 2. Столбцы в таблице: m – номер модели; r – значение параметра r; σ_t – СКО тензорного метода; σ_d – СКО дифференциального метода; σ_{tm} – СКО тензорного метода с учетом доверительной маски; σ_{dm} – СКО дифференциального метода с учетом доверительной маски; $\sigma_{t(1-m)}$ – СКО тензорного метода внутри области недоверия; $\sigma_{d(1-m)}$ – СКО дифференциального метода внутри области недоверия; S_m / S_F – отношение площади области недоверия к полной площади изображения.

Таблица 2. Результаты экспериментов

m	r	σ_t	σ_d	σ_{tm}	σ_{dm}	$\sigma_{t(1-m)}$	$\sigma_{d(1-m)}$	$\frac{S_m}{S_F}$
1	$r=50$	0,024	0,022	0,015	0,015	0.048	0.043	0.144
	$r=10$	0,035	0,033	0,022	0,022	0.055	0.049	0.239
	$r=5$	0,058	0,056	0,034	0,035	0.069	0.063	0.477
2	$r=50$	4.6×10^{-5}	4.6×10^{-5}	4.6×10^{-5}	4.6×10^{-5}	-	-	0
	$r=10$	0,041	0,039	0,032	0,032	0.101	0.088	0.066
	$r=5$	0,083	0,084	0,070	0,072	0.091	0.090	0.235
3	$r=50$	0,038	0,032	0,014	0,014	0.120	0.101	0.083
	$r=5$	0,038	0,032	0,014	0,014	0.120	0.101	0.083
	$r=-5$	0,038	0,032	0,014	0,014	0.120	0.101	0.083
4	$r=50$	$3,8\times10^{-5}$	$3,8\times10^{-5}$	$3,8\times10^{-5}$	$3,8\times10^{-5}$	-	-	0
	$r=1$	4×10^{-5}	3.94×10^{05}	4×10^{-5}	3.94×10^{05}	-	-	0
	$r=-1$	4×10^{-5}	3.94×10^{05}	4×10^{-5}	3.94×10^{05}	-	-	0
5	$r=500$	0,447	0,285	0,073	0,074	0.583	0.357	0.657
	$r=300$	0,560	0,525	0,018	0,018	0.674	0.599	0.897143
	$r=100$	1,006	1,60	-	-	1,006	1,60	1

Анализ полученных данных показывает:

(а) максимальное СКО σ_t, σ_d (без учета маски) равно 80% (0,56) от номинального значения угла вектора перемещения $\left(\frac{\pi}{4}\right)$;

(б) при использовании доверительной маски максимальное СКО σ_{tm}, σ_{dm} снизилось до 10 % (0,073) в точках области доверия;

(в) основные ошибки в вычислениях $\sigma_{t(1-m)}, \sigma_{d(1-m)}$ находятся в точках внутри области недоверия;

(г) наименьшее СКО получается при использовании сигналов вида 4 и 3;

(д) области недоверия образуются вокруг точек с разрывами первой производной.

Вторая группа экспериментов была проведена с использованием значений градиента, найденных аналитически. Во всех случаях СКО не превышал 0,5 % от уровня сигнала. Здесь ОП оценивается практически безошибочно каждым методом.

Заключение

В работе приведены результаты экспериментов, проведенных с целью сравнения дифференциального и тензорного методов нахождения оптического потока на модельных последовательностях. Результаты экспериментов показали, что основная причина ошибки при нахождении оптического потока обоими методами - неточность в определении направления градиента, которая в основном проявляется вокруг точек с разрывами первой производной. При использовании тензорного метода существует возможность вычисления доверительной маски, локализующей области с ошибками в вычислении оптического потока.

Для того, чтобы иметь возможность исследовать методы вычисления оптического потока в интерактивном режиме, разработана специальная программная система. К основным её достоинствам можно отнести наглядное представление алгоритма, простоту изменения алгоритма, простоту задания и изменения входных данных алгоритма, удобные средства визуализации выходных данных (графики, таблицы), поддержка модели «ленивых» вычислений (отложенных вычислений) и автоматического хранения промежуточных данных.

Литература

1. Яне Б. Цифровая обработка изображений; – Москва; Техносфера 2007. – 584 с.
2. Гонсалес Р., Вудс Р., Эддинс С. Цифровая обработка изображений в среде MATLAB. – Москва: Техносфера. – 2006.
3. Hans Petter Langtangen. Python scripting for computational science. – Springer; 3rd edition (February 1, 2009). – 717 с.

СОДЕРЖАНИЕ

Сборник трудов конференции молодых ученых, Выпуск 6. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ / Главный редактор д.т.н., проф. В.Л. Ткалич. - СПб: СПбГУ ИТМО, 2009. - 707 с.

СБОРНИК ТРУДОВ КОНФЕРЕНЦИИ МОЛОДЫХ УЧЕНЫХ
Выпуск 6

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Главный редактор доктор технических наук,
профессор В.Л. Ткалич Дизайн обложки Т.В.
Точилина Редакционно-издательский отдел СПбГУ
ИТМО Зав. РИО Н.Ф. Гусарова Лицензия ИД №
00408 от 05.11.99. Подписано в печать 31.03.09.
Заказ 2101. Тираж 100 экз.