УДК 004.042

ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДИКИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНЫХ ТЕХНОЛОГИЙ IOT УСТРОЙСТВ

Митрофанов Л.В.
Санкт-Петербург, Университет ИТМО
Научный руководитель – доцент, Донецкая Ю.В.
Санкт-Петербург, Университет ИТМО

В работе предложены методы модифицированной прямоугольной квадратурной амплитудной модуляции для уменьшения взаимного влияния беспроводных сетей, адаптивного подбора свободных каналов передачи данных в беспроводных сетях с использованием анализаторов спектра, повышения функциональной безопасности беспроводной инфраструктуры и комплексной оценки состояния систем ее защиты от воздействия техногенных и антропогенных угроз. Проведены экспериментальные исследования современного состояния беспроводных технологий IoT, взаимного влияния беспроводных сетей IoT, эффективности миниатюрных анализаторов спектра и работоспособности ускоряющей линзы для многолучевых систем, а также ее затмения и поляризационных свойств. Разработана методика обеспечения безопасности беспроводных технологий IoT устройств и описана эффективность данной методики.

Приведенные методы позволяют утверждать, что имеется потенциал для дальнейшего развития теоретических и практических методов и моделей обеспечения информационной и функциональной безопасности в беспроводных сетях на основе аппаратного разделения абонентов.

Введение. Актуальность темы данной работы обусловлена тем, что технология IoT позволяет с легкостью контролировать все аспекты нашей жизни. Нынешняя техническая революция и быстрое развитие мобильных технологий считается первой фазой Интернета вещей. Число физических объектов, подключенных к интернету растет с беспрецедентной скоростью, что реализует идею Интернета вещей. Уже сегодня практическое применение технологии IoT можно найти во многих отраслях промышленности, в том числе земледелии, строительстве, энергетике и транспорте.

Тема магистерской диссертации считается актуальной, так как архитектура интернета вещей имеет сложное строение и требует изучения. Цифровые двойники считаются неотъемлемой частью IoT. Представление любого объекта реального мира в виде информации находится в цифровом мире с возможностью идентификации этого объекта с конкретной записью. Предложенная методология защиты сети IoT позволяет выбрать лучший вариант средств и методов защиты для построения конкретной сети.

Известно, что решению проблемы информационной и функциональной безопасности в целом, и беспроводных сетей в частности, посвящены работы известных отечественных и

зарубежных ученых и их научных школ: Д. В. Агеева, В. М. Астапени, В. М. Богуша, В. Л . Бурячка, В. В. Домарев, А. Карлсона, А. Г. Корченко, Г. Т. Маркова, М. В. Степашкина, С. В. Толюпа, В. А. Хорошко и Я. С. Шифрина и многих др. Научно-прикладной задачей, которая решается в работе, считается обеспечение информационной и функциональной безопасности беспроводных сетей передачи данных, что, в свою очередь, требует создания научно-обоснованных методов повышения эффективности при передаче информации в беспроводных системах в условиях существующих объективных противоречий между динамическими изменениями современного мира при одновременном увеличении количества беспроводных технологий и сетей, и несовершенством, а иногда и отсутствием методологии построения информационно и функционально защищенных беспроводных систем с другого. Наличие данных противоречий и обусловливает актуальность темы работы, поэтому решение поставленной научно-прикладной задачи обеспечения информационной и функциональной безопасности беспроводных сетей имеет важное научное и практическое значение.

Основная часть. В работе решена научно-прикладная задача, которая заключается в обеспечении информационной и функциональной безопасности беспроводной инфраструктуры IOT-решений на основе аппаратного разделения абонентов.

Безопасность и устойчивость Интернета вещей - это эффективность оценки рисков и их устранение. Безопасность в IoT считается уникальной, поскольку люди должны доверять технологии. Уникальность заключается в том, что должна происходить идентификация, аутентификация, хранение и обработка информации, включая финансовую. Также должна обеспечиваться безопасность доставки товаров, мультифакторная аутентификация, автоматическая фиксация передачи прав от одного контрагента к другому.

Проведен анализ существующих угроз и атак на беспроводные технологии IOT-решений (передатчик, приемник и среду передачи информации). Для обеспечения содержательности анализа полученных результатов в процессе проведения выбора подходов к обеспечению информационной безопасности были проанализированы модели и критерии угроз в беспроводных технологиях и методы оценки угроз в беспроводных сетях IOT-решений.

Проведено сравнение моделей построения беспроводных сетей IOT-решений с помощью анализа спектра сигналов, исследование технологий построения (архитектуры) беспроводных сетей IOT-решений и моделирования беспроводных сетей IOT-решений с ортогональным частотным разделением каналов.

Предложены пути защиты беспроводных сетей IOT-решений на базе технологии обеспечения объективного контроля защищенности беспроводных сетей и повышение их защищенности (уровня функциональной безопасности).

Выводы. В работе рассмотрен комплекс проблем, связанных с обеспечением информационной безопасности беспроводных IOT-решений. Для их анализа, прежде всего,

необходимо было проанализировать возможности практического применения разработанной методологии в данной области. В частности, освещены следующие аспекты:

- архитектура, особенности, достоинства и недостатки беспроводных IOT-решений, затронуты вопросы работы стандартов в условиях городских и региональных сетей;

- спектр угроз и множество уязвимостей, классифицированные в соответствии с документами международных организаций по стандартизации, основные типы нарушителей, которые ввиду своей мотивации могут осуществить деструктивное воздействие на беспроводные IOT-решения, а также основные атаки на беспроводные IOT-решения;

- методология анализа рисков, основанная на оценке субъективной вероятности реализации угроз и применении аппарата теории нечетких множеств и теории нечеткой логики;

- ранжирование угроз по уровню риска, а также анализ комплексов контрмер, направленных на минимизацию рисков обеспечения информационной безопасности беспроводных IOT-решений;

- выбор оптимальной по соотношению цена-качество системы средств защиты на основании метода анализа иерархий;

- анализ существующих стандартов управления рисками и основных методик формирования политики безопасности.

Рассмотрены существующие методики и концепции управления рисками. Получены оценки уровня риска для всего спектра рассматриваемых угроз безопасности беспроводных сетей и проведено их ранжирование. Проанализирован комплекс контрмер, направленных на минимизацию рисков информационной безопасности беспроводных сетей. Рассмотрена задача обоснования выбора оптимальной системы средств защиты и предложен вариант ее решения на основании МАИ.

По итогам проведенного исследования оптимальной по соотношению стоимость (эффективность) защиты является система защиты №5, включающая в себя средства аутентификации по протоколу EAP, а также шифрование по протоколу AES (WPA2).

Митрофанов Л.В. (автор) Подпись

Донецкая Ю.В. (научный руководитель) Подпись