УДК 004.056

РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВНУТРЕННЕГО НАРУШИТЕЛЯ НА ОСНОВЕ ДЕВИАНТНОГО ПОВЕДЕНИЯ В СОЦИАЛЬНОЙ ГРУППЕ

Меренков Д.Н. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – преподаватель практики Ищенко А.П.
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

В данной работе рассматривается модель системы выявления внутренних нарушителей организации, основывающаяся на оценке степени отклонения поведения человека от общепринятого в пределах замкнутой социальной группы. Предложенная модель направлена на уменьшение времени реагирования на инциденты информационной безопасности и снижение финансовых издержек на их устранение.

Введение.

Под внутренним нарушителем понимают действующего или бывшего сотрудника организации, контрагента или бизнес-партнера, который имеет или имел авторизованный доступ к внутренним сетям, системам или данным организации и, вследствие намеренных или ошибочных действий, создал инцидент информационной безопасности.

Наиболее распространенным способом получения внутренним нарушителем защищаемой информации является доступ к информационным системам организации, где осуществляется хранение и обработка информации. Нарушитель может, как скомпрометировать аутентификационную пару логин-пароль для несанкционированного доступа к стороннему компьютеру организации, так и совершить некоторый набор действий на своем рабочем компьютере, ведущий к утечке данных. В обоих рассматриваемых случаях, нарушитель, с точки зрения системы, имеет к ней легитимный доступ, и действия, совершаемые им, так же могут расцениваться, как легитимные.

Существующие системы выявления внутреннего нарушителя направлены на сравнение действий пользователя с заданными специалистами информационной безопасности шаблонами типовых действий, которые не всегда отражают все аспекты деятельности подразделений и выполняемые пользователями функции. В результате подобные системы безопасности зачастую ведут либо к снижению эффективности работы подразделений за счет избыточных или некорректных реакций на потенциальные инциденты ИБ, либо к низкой эффективности работы самой системы обнаружения инцидентов ИБ.

Целью работы является разработка модели системы обнаружения внутреннего нарушителя, которая улучшает существующие методы выявления аномалий в анализируемых действиях за счет:

1) дополнительной оценки степени влияния на совершенные действия внешних факторов, поддающихся сбору и метрической оценке, с целью последующей автоматизированной корректировки критериев
2) сравнение действий не только с заданным шаблоном действий конкретного пользователя, но и со стандартными действиями социальной группы, к которой относится потенциальный нарушитель, на основании предварительно обученной или периодически обучаемой системы

Основная часть.

Для решения поставленной проблемы предлагается использовать разработанную автором модель. Модель может являться частью системы помощи принятия решения.

Работу модели можно разделить на два этапа: обучение и анализ. В процессе обучения производится разделение людей на внутрикорпоративные социальные группы и сбор данных для последующего анализа. Отнесение человека к той или иной социальной группе происходит с помощью применения методов кластеризации, основывающихся на выявленных характеристиках человека Сбор данных включает в себя фиксацию времени каждого совершенного сотрудником действия, самих действий, внешних обстоятельств, при которых были совершены действия, идентификационного номера сотрудника и занесение этой информации в базу данных. В период сбора данных, все детектируемые действия считаются «нормальными» для каждой из социальных групп.

В процессе второго этапа модель анализирует совершаемые всеми сотрудниками действия на предмет аномальности. При похожих внешних факторах аномальными считаются такие действия, которые отклоняются от «нормальных» действий исследуемого человека или являются девиантными по отношению к социальной группе, в которой он состоит.

Действие считается аномальным, если в множестве собранных данных не найдено ни одного элемента множества, удовлетворяющего предъявляемым к нему требованиям. В число таких требований входит схожесть внешних факторов, попадание текущего времени в некоторый заданный интервал времени элемента множества и совпадения анализируемого действия с действием, уже совершенным социальной группой, в которую входит рассматриваемый человек. Схожесть внешних факторов рассчитывается на основе заданной метрики. Сравнение текущих действий не только с действиями самого человека, но и с действиями социальной группы, в которой он состоит, способствует снижению ложноположительных срабатываний системы.

Выводы.

Представленная в докладе модель системы тестировалась на данных, полученных в процессе проведения эксперимента в действующей организации со количеством пользователей информационных систем не менее 1000 человек. По результатам обучения модели, была произведена проверка ее работоспособности на предмет выявления внутреннего нарушителя. Модель системы успешно справилась в поставленной перед ней задачей и смогла обнаружить не менее 80 % пользователей, характеризуемых на время тестирование системы как внутренние нарушители.

Таким образом, разработанная модель системы обнаружения внутреннего нарушителя на основе девиантного поведения в социальной группе, за счет комплексного анализа поведения человека, может применяться в организациях, работающих с защищаемой информацией, где требуется принимать меры по ее защите от несанкционированного доступа.

Меренков Д.Н. (автор)

Ищенко А.П. (научный руководитель)