

ОТЗЫВ

официального оппонента на диссертационную работу Мартьянова Евгения Александровича на тему «Исследование и разработка методик оценки защищенности информационных объектов от потенциальных нарушителей», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Практическая значимость и актуальность работы

В диссертационной работе Мартьянова Е.А. решена актуальная научная задача, связанная с обеспечением информационной безопасности. Постоянно в мире значительное число организаций подвергается угрозам, исходящими от собственных сотрудников (инсайдеров). Инсайдеры имеют право доступа к конфиденциальной информации и используют его в личных интересах или в интересах третьих лиц. Как правило, организация, опасаясь репутационных потерь, не придаёт огласке факт инсайдерских атак, тем не менее, можно с уверенностью говорить о росте их количества, что в значительной степени определяется возрастающей ролью информационных систем. С учётом значительной трудности их обнаружения и предотвращения, можно считать, что инсайдеры представляют весьма серьёзную угрозу безопасности.

Цель работы, обозначенная автором, – найти решение технической задачи идентификации как инсайдера пользователя определённого типа. Существенная сложность работы определяется ограниченностью количества доступной для исследования информации. Однако подход, предлагаемый автором, позволяет решить эту проблему. Кроме того, можно говорить о возможности его широкого практического применения. Таким образом, в работе Е.А. Мартьянова решается **актуальная и важная** задача, связанная с точным выявлением инсайдера среди пользователей информационной системы.

Характеристика содержания диссертационной работы

Диссертация Мартьянова Е.А. состоит из введения, трех глав, заключения, списка сокращений, приложения и библиографического списка, включающего 109 наименований. Объем диссертации составляет 136 страниц.

Во введении аргументируется актуальность исследований, перечисляются используемые методы исследования, формулируются цель и задачи работы, обосновывается научная новизна, теоретическая и практическая значимость полученных результатов, приводятся сведения о результатах использования.

В первой главе автор приводит аналитический обзор исследований в области защиты организаций от инсайдеров, описывает и анализирует используемые методы их обнаружения. В разделе 1.1 обосновывается необходимость своевременного и точного обнаружения инсайдера. В разделе 1.2 автор подробно рассматривает программу CERT и результаты работы центра изучения угроз инсайдера, обращая особое внимание на причины появления угроз инсайдерских атак и способы минимизации возможного ущерба от них по трем группам угроз: саботаж и шпионаж, воровство интеллектуальной собственности и мошенничество. Раздел 1.3 полностью посвящен проекту ADAMS. В нем проведен анализ методов и подходов к обнаружению аномалий в больших объемах данных, которые применяются в задаче выявления инсайдера. В разделе 1.4 затронут вопрос проверки методов обнаружения инсайдера, выделены применяемые исследователям подходы к верификации, сформулированы их достоинства и недостатки. Раздел 1.5 содержит выводы к первой главе диссертационной работы.

Во второй главе диссертации автором предложена формальная модель работы пользователей с информационной системой, описан и обоснован метод выявления потенциальных инсайдеров, основанный на определении факта сбора избыточной информации. В разделе 2.1 проведён анализ недостатков рассмотренных в главе 1 подходов и обоснована необходимость разработки нового метода обнаружения инсайдера. В разделах 2.2-2.3 подробно описаны формальная модель информационной системы организации и ее пользователей и алгоритм обнаружения действий инсайдера. Раздел 2.4 посвящен исследованию свойств описанного метода для одного работающего пользователя. В частности, доказываемое утверждение, что в описанной модели можно за конечное число шагов гарантированно выявить инсайдера. В разделе 2.5 доказательство данного утверждения распространяется на случай произвольного множества пользователей.

Раздел 2.6 содержит интересное расширение модели, в которой, помимо ограничения на атрибуты, для пользователя вводится ограничение на множество разрешенных строк данных. При этом описание возможностей пользователя заметно усложняется, но, как показано автором, заявленные свойства метода сохраняются. Раздел 2.7 содержит выводы ко второй главе диссертационной работы.

В третьей главе рассматривается разработанное автором программное средство для имитационного моделирования действий пользователя в информационной системе для их анализа по методике, описанной в главе 2. В разделах 3.1-3.2 обоснована эффективность применения имитационного моделирования в сложных задачах. Раздел 3.3 полностью посвящен указанному программному средству: приведены требования, представлены разработанные автором и реализованные им же алгоритмы работы. В разделах 3.4 – 3.8 поставлены и на основе имитационного моделирования решены задачи изучения работы описанного в главе 2 метода. В разделе 3.4 рассматривается случай выборки пользователем большого объема данных из хранилища и построена соответствующая модель. В разделах 3.5 и 3.6 рассмотрен оригинальный сценарий работы пользователя с хранилищем данных. Сценарий, представленный в разделе 3.7, рассматривает действия инсайдера, который маскирует свою деятельность за легальной активностью. В разделе 3.8 исследована динамика времени работы метода в зависимости от количества пользователей и размеров хранилища данных. Раздел 3.9 содержит основные сведения о внедрении разработанного метода и программного средства. Раздел 3.10 содержит выводы к третьей главе диссертационной работы.

В Заключении сформулированы основные научные и практические результаты, представленные в диссертации.

Научная новизна и практическая значимость результатов

В диссертационной работе предложен новый метод идентификации действий инсайдера в информационной системе, который обладает следующими характерными свойствами:

- 1) не зависит от характеристик случайных процессов, таких, как работа пользователей;

- 2) гарантирует отсутствие ложных определений честных пользователей как нарушителей;
- 3) дает теоретическое обоснование возможности достоверной селекции инсайдеров и честных пользователей за конечное число шагов.

Разработанное программное средство позволяет анализировать содержание запросов пользователей к хранилищу данных с целью обнаружить потенциального инсайдера на основании выхода его за разрешенное множество атрибутов. Модуль имитационного моделирования, в свою очередь, позволяет создавать синтетические данные для изучения деталей работы алгоритма и его проверки на различных сценариях. Применение его в условиях действующих информационных систем подтверждает высокую практическую значимость проведенной работы. Подход может быть применен и для других случайных процессов, связанных с защитой информационного объекта.

Достоверность основных положений и результатов работы

Достоверность основных положений обеспечивается прикладными результатами применения предложенной методики, реализованной в программном средстве. Результаты диссертации получены автором лично, представлены в шести публикациях, четыре из которых опубликованы в научных изданиях, рекомендуемых ВАК РФ. Результаты работы обсуждались на конференциях и научных семинарах. В опубликованных автором трудах отражены основные положения его диссертации. Диссертационная работа оформлена качественно и соответствует требованиям, установленным Министерством образования и науки Российской Федерации. Автореферат полностью отражает содержание диссертационной работы. Изложенные в работе материалы обладают внутренним единством и непротиворечивостью.

Необходимо отметить следующие недостатки представленной работы:

- 1) в тексте работы в явном виде не описано, как связана задача обнаружения выхода за разрешенное множество атрибутов с политикой безопасности. Пользователи могут обращаться к запрещенным атрибутам по разным

причинам (случайно, в результате сбоя или ошибки в задании, и т.д.), а не только в случае, когда они инсайдеры.

- 2) материал раздела 3.1, в котором приведены особенности применения имитационного моделирования к задаче выявления инсайдера, возможно, лучше отнести к разделу 1.4;
- 3) в разделе 3.6 автором были получены граничные значения только для одной пары параметров, в то время, как в разделе 3.5 и приложении А приведены расчетные значения всех параметров из полуинтервала $(0;4]$ с шагом 0,1. Было бы интересно получить подобные экспериментальные граничные значения и для других пар параметров;
- 4) в разделе 3.8 на стр. 111-112 рис. 3.11 и 3.12 диссертационной работы (и автореферата – стр. 17 рис. 4 и 5) автором продемонстрирован характер роста времени проверки действий пользователей в зависимости от их количества и мощности разрешенного множества. Однако не отмечено, сохранится ли та же тенденция при увеличении числа пользователей;
- 5) в тексте диссертации встречаются опечатки.

Указанные недостатки не снижают значимости полученных автором результатов. Представленная диссертационная работа, несомненно, свидетельствует о высокой научной квалификации автора. Показана возможность практического приложения полученных результатов для решения задачи обнаружения инсайдера при работе с информационной системой организации. Поставленная цель диссертационного исследования достигнута и, несмотря на замечания, заслуживает положительной оценки.

Автореферат соответствует основному содержанию диссертации и отвечает требованиям ВАК РФ.

На основании анализа содержания диссертации и опубликованных автором работ можно сделать заключение, что диссертация Мартянова Евгения Александровича является законченной научно-квалификационной работой и соответствует требованиям ВАК РФ, предъявляемых к диссертациям на соискание кандидата технических наук. Новые научные результаты, полученные диссертантом,