

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».

Актуальность темы исследования.

В настоящее время продолжается бурный рост объема и спектра предоставляемых услуг со стороны операторов компьютерных систем. К глобальным сетям подключаются как легитимные потребители, так и пользователи, преследующие деструктивные цели. Таких нелегально подключенных потребителей естественно назвать инсайдерами. Наиболее ярко этот процесс наблюдается в сети Интернет, где периодически возникают новейшие вирусные программы и организуются атаки типа «Отказ в обслуживании». Сложность защиты от подобных злоумышленников заключается в том, что им предоставляется определенные и подчас весьма существенные права и возможности. Эти возможности используются злоумышленниками в негативных целях.

Отличить действия злоумышленника от работы реального пользователя автоматической системы мониторинга и контроля весьма сложно. Поэтому разработке методов совершенствования обнаружения в автоматизированном режиме в настоящее время уделяется существенное внимание, что делает задачу исследования безусловно актуальной.

Развиваемое в рецензируемой диссертационной работе направление исследований посвящено вопросам выявления инцидентов информационной безопасности на основе статистического анализа и представляет большой интерес, поскольку не только принципиально позволяет определить наличие или отсутствие инцидентов информационной безопасности, но и снижает трудоемкость таких

исследований, а в целом создает основу для оценки защищенности информационных систем от потенциальных нарушителей, что и составляет основную цель настоящей работы.

Основные задачи исследования.

Предлагаемая диссертация направлена на развитие методов автоматизированной обработки и анализа данных, характеризующих состояние контролируемой компьютерной системы. Вопрос об оценке состояния компьютерной системы является принципиально важным при построении системы мониторинга информационной безопасности и выявления наступления инцидента информационной безопасности. В работе предлагается обобщенная модель взаимодействия пользователя с рабочим хранилищем данных, позволяющая отличить инсайдера по атрибутам посылаемого запроса. Предлагаемая диссертантом методика выявления инцидента информационной безопасности вследствие деятельности инсайдера в определенной степени универсальна по типам и видам систем, которые подвергаются мониторингу, хотя и предполагает наличие ограничений на механизмы работы инсайдера. Разработка автоматизированных систем контроля штатной работоспособности и выявление инцидентов информационной безопасности при реализации возникновении нештатного поведения пользователей является не только актуальной задачей, но и создает новый подход, обладающий определенной универсальностью.

Тема диссертации, направленность проведенных исследований и полученных результатов соответствуют п. 3, 7, 9 «Положения ВАК», по паспорту специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность». Теоретические и прикладные результаты ориентированы, в конечном счете, на повышение информационной безопасности вычислительных систем путем своевременного выявления инцидентов информационной безопасности, связанных с инсайдерскими атаками и оценке уровня безопасности в апостериорном режиме.

Характеристика содержания диссертационной работы

Диссертационная работа состоит введения, трех глав, заключения, списка сокращений, библиографии и одного приложения.

Во введении обоснована актуальность диссертационной работы, сформулированы цель и задачи, показана практическая значимость результатов, представлены выносимые на защиту научные положения.

В первой главе диссертационной работы произведен обзор методов и подходов, использованных при обнаружении инсайдера. В разделе 1.1 приведены основные причины инсайдерских атак и показана актуальность задачи защиты от них. В разделе 1.2 подробно рассмотрена программа CERT и предложенная в ней классификация угроз инсайдера, приведены выработанные в ней рекомендации по минимизации ущерба от успешных атак инсайдеров для каждой группы в отдельности, приведены основные результаты программы. В разделе 1.3 рассмотрен проект ADAMS от DARPA, кратко описаны используемые методики и алгоритмы поиска инсайдера, выделены их достоинства и недостатки в действующих информационных системах организаций. В разделе 1.4 приведены подходы к проверке разработанных методик и алгоритмов, выделены их сильные и слабые стороны.

Во второй главе автор излагает суть и обоснование предлагаемого подхода к обнаружению инсайдера основанного на определении атрибутов запроса пользователя, которые ведут к получению информации, не входящей в служебные полномочия пользователя. По мнению автора, такой подход обладает следующими преимуществами:

- независимость от количества пользователей, которых одновременно контролирует предлагаемая система;
- инвариантность к вероятностному распределению запросов;
- имеет приемлемую вычислительную мощность.

Для реализации этого подхода автор решает две задачи :

- разработка формальной модели работы пользователей в виде множества атрибутов его служебных запросов;

- математическое исследование сводимости алгоритма, поиск пользователя, запросы, которые не входят в множества разрешенных за конечное время.

Таким образом, производится обоснование предлагаемого подхода и его свойств, для чего используется математический аппарат вероятностных запретов, позволяющий подтверждать, что при принятых ограничениях на модель инсайдера, вероятность ошибки первого рода (ложная тревога обнаружения инсайдера среди правильных пользователей) равна нулю.

Изложенные модели составляют теоретическое обоснование подхода и подтверждают квалификацию автора.

К сожалению, в работе не рассмотрен более сложный сценарий действий инсайдера. Желательно было бы привести конкретный пример построения множества атрибутов запроса пользователя и его служебных обязанностей, хотя, в работе присутствует раздел, рассматривающий ограничения на работу пользователя не только по множеству запросов, но и по категории информации.

Дальнейшее развитие этих ограничений, видимо, позволит рассмотреть более сложные сценарии работы инсайдера, что подтверждает значимость предложенного подхода.

В третьей главе представлены результаты проведенного имитационного моделирования работы алгоритма. Разделы 3.1 и 3.2 посвящены вопросам применения имитационного моделирования в т.ч. к задаче проверки подходов к выявлению инсайдера. В разделе 3.3 описаны требования к разработанному программному обеспечению, его структура и алгоритмы работы в зависимости от настроек.

В главе описаны правила подготовки параметров модели, исходя из структуры информационной системы и организации работы пользователей.

Значимую часть этого раздела составляет решение вопроса об обработке данных большого объема возникающих в ходе моделирования и исследования возможностей применения предположения о нормальном распределении при описании работы инсайдера. Для преодоления проблем используется закон Ципфа,

позволяющий перейти от анализа атрибутов запросов к упорядочению по попаданию в выборку пользователей определенной группы.

Такое развитие метода с одной стороны расширяет рассматриваемые сценарии поведения инсайдера, с другой, не предполагает ограничений на закон вероятности запроса пользователей, т.е. решает задачи выполнения требований к методу, поставленных в гл. 2.

Также рассмотрен случай сокрытия накопленной избыточной информации инсайдера.

В целом, материал этой главы достаточно полно раскрывает правомерность и возможность предлагаемого подхода для обнаружения инсайдера на основе имитационного моделирования. Адекватность полученных при моделировании результатов фактическим процессам подтверждается актом о применении предлагаемого подхода при анализе работы конкретных информационных систем, по вероятности попадания атрибутов в выборку пользователей определенной группы, при этом конкретные значения атрибутов не раскрываются.

Кроме того, в этой же главе рассмотрена задача обнаружения инсайдера в случае накопления им избыточной информации, а также исследование времени работы алгоритма.

В целом, приведенные результаты составляют основу для практических рекомендаций при использовании разработанных методов.

Новизна исследования и полученных научных результатов.

Анализ содержания диссертации показывает, что автором:

- проведен анализ предметной области, включающий систематизацию инцидентов информационной безопасности и исследование деятельности инсайдера;

- построена универсальная математическая модель поведения пользователя при работе с хранилищем данных и предложены критерии обнаружения инсайдера на основе анализа вероятностных характеристик запросов;

- впервые предложено для обоснования свойств вероятностных методов обнаружения инсайдера применить метод вероятностных запретов, ранее для этих целей не использовавшийся;

- проведены исследования достоверности метода по выявлению инсайдера, при различных сценариях поведения инсайдера;

- разработана методика моделирования выявления инсайдеров, позволяющая получить рекомендации для сведения ошибок первого и второго рода к приемлемым значениям.

Выполненные исследования позволили соискателю выработать рекомендации по повышению информационной защищенности систем различного назначения, включая системы контроля доступа. Новизна и сущность полученных рекомендаций состоит в том, что они направлены на:

- определение неизвестного инсайдера с требуемой достоверностью, причем, при этом ошибки первого рода гарантированно равны нулю;

- определены объем и виды представления входных в систему данных, для выявления инсайдера;

- определены оптимальные значения параметров, алгоритмы, обеспечивающие эффективность методики как в смысле минимизации ошибок первого и второго рода, так и времени наблюдения.

Обоснованность и достоверность положений и выводов.

Анализ содержания работы позволяет судить о достаточно высокой степени обоснованности основных научных положений, выводов и практических рекомендаций, приведенных в диссертации. Это подтверждается использованием системного подхода к исследованию проблемы, логичностью промежуточных выводов, корректностью разработанных математических моделей и применением теоретически обоснованных методов математического моделирования.

Достоверность основных научных результатов обеспечивается:

- применением обоснованных научных методов исследования;

- обширным фактологическим и статистическим материалом, что подтверждается актами реализации;
- использованием на практике предлагаемой в работе методики обнаружения инсайдеров в системах мониторинга функционирования компьютерных систем, ее практической апробацией, что подтверждено соответствующими актами;
- непротиворечивостью экспериментально полученных количественных оценок теоретическим результатам.

Теоретическая значимость и практическая ценность работы.

Теоретическая значимость научных результатов определяется развитием основных положений теории защиты информации в части выявления инсайдеров по наблюдаемым данным о работе компьютерной системы, а также изучением неисследованных ранее свойств критериев, основанных на применении закона Ципфа и метода вероятностных запретов.

Практическая ценность состоит в апробации предложенного метода в 5 организациях.

Недостатки работы.

1. В главе 2 основным критерием наличия инсайдера является использование запрещенных атрибутов запросов. Однако, в 3 главе, для рассмотрения и моделирования различных сценариев нарушения, используются вероятностные критерии. В связи с чем, желательно было бы определить общий набор критериев, принципы задания пороговых значений.

2. При моделировании работы пользователя, автор использует множество атрибутов его запросов к БД в соответствии с его служебными обязанностями. Как это осуществляется на практике и сколько времени занимает ввод нового пользователя? Желательно было бы привести пример профиля пользователя для конкретной системы.

3. Как соотносится введение запрещенных запросов и задание политики безопасности? Причин нарушения ПБ много (ошибки, сбои, недочеты администратора). Любой нарушитель ПБ может быть интерпретирован как инсайдер. Рассматривались ли выборки запросов, содержащие работу инсайдера? Сколько его запросов необходимо найти для обнаружения?

4. На основе теории запретов показано, что вероятность ошибки I рода равна нулю, а ошибка II рода определяется числом шагов алгоритма. При переходе к вероятности попадания инсайдера в заданную группу, автор дает только оценки границ группы и не ограничивает время поиска и границы группы.

5. На стр. 49 работы декларируется построение решающей функции, не зависящей от ограничений на тип запросов, числа пользователей и т.д., однако, вид этой функции не приведен.

6. В диссертации не всегда соблюдена терминология. Иногда факт «утечки» путается с идентификацией инсайдера, есть неудачные стилистические обороты.

Указанные замечания не влияют на общую положительную оценку диссертации. Работа Мартянова Е.А. является законченной научно-квалификационной работой, содержащей существенные научные и практические результаты для развития отрасли защиты информации в информационных системах широкого назначения. Совокупность разработанных автором положений и их практическая реализация способствуют развитию общей теории информационной безопасности и могут квалифицироваться как новые технические решения важной задачи, способствующей повышению устойчивости функционирования компьютерных систем.

На основании изложенного можно заключить, что представленная диссертация удовлетворяет требованиям ВАК, предъявляемым к кандидатским диссертациям по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» в части пунктов 3,7,9.

Основные результаты работы достаточно полно освещены в 6 трудах автора, из них 4 статьи в изданиях, входящих в перечень рекомендуемых ВАК РФ. Содержимое автореферата правильно отражает основные положения и выводы работы. Автор диссертации Мартьянов Е.А. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент

директор Специализированного центра защиты информации Санкт-Петербургского политехнического университета Петра Великого, профессор кафедры Информационной безопасности компьютерных систем Института прикладной математики и механики Санкт-Петербургского политехнического университета Петра Великого, доктор технических наук (специальность 05.13.16 «Применение вычислительной техники, математического моделирования и математических методов в научных исследованиях (по отраслям наук)»), профессор, заслуженный деятель науки РФ; 195251, г. Санкт-Петербург, ул. Политехническая, д. 29, ауд. 173; Тел. +7 (812) 552-76-32. Адрес в сети Интернет: <http://ibks.ftk.spbstu.ru>, электронная почта kafedra@ibks.spbstu.ru.



 Зегжда Петр Дмитриевич
« 26 » февраля 2019 г.

Подпись Зегжды П.Д. удостоверяю

Начальник Управления персонала  Пахомова Мария Владимировна