АКЦИОНЕРНОЕ ОБЩЕСТВО
"НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
"РУБИН"

194100, Санкт-Петербург, ул. Кантемировская, д. 5, тел. (812) 670-89-89, факс: (812) 596-35-81, e-mail: inforubin@rubin-spb.ru
ИНН/КПП 7802776390/780201001, ОГРН 1127847043720, ОКПО 07542394

27.03.2020 № К-419 Экз. 1

УТВЕРЖДАЮ
Генеральный директор

С.С. Степанов

«26» марта 2020 г.

ОТЗЫВ

ведущей организации на диссертационную работу Ушакова Игоря Александровича на тему: «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность»

АКТУАЛЬНОСТЬ ТЕМЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

Современный опыт использования компьютерных сетей на различных предприятиях показывает, что необходимость организации совместного использования информационных и технических ресурсов работниками разных компетенций приводит к таким негативным последствиям, как утечка информации, нарушение функций сети связи, искажение ценной информации и др.

Известными способами борьбы с этими последствиями являются различные способы разграничения доступа работников к совместно используемым ресурсам, аудит их действий, периодическая проверка целостности этих ресурсов, анализ происходящих событий, аномалий и моделирование возможных действий, которые могут указывать на наличие нарушителей.

В качестве превентивных способов борьбы при этом используются предсказание возможных действий работников, установка «ловушек», срабатывание которых может указывать на нелегальную деятельность.

Все эти способы и связанные с ними методы борьбы не совершенны и их эффективность ослабевает одновременно с совершенствованием подходов в реализации инсайдерской деятельности.

В рамках данной области востребованы и в ближайшем будущем будут востребованными и актуальными задачи обнаружения инсайдеров на ранних этапах их активности. Возможность идентификации нарушителя до того, как он осуществил свои намерения, позволяет избежать убытков, которые при его успехе будут понесены.

По этой причине актуальность темы диссертационных исследований не вызывает сомнений.

НОВИЗНА И ДОСТОВЕРНОСТЬ НАУЧНЫХ РЕЗУЛЬТАТОВ

Научные результаты, полученные в диссертационной работе:

модель представления больших данных об инсайдерских атаках в формате NoSQL, обеспечивающая хранение и анализ признаков пользователей в компьютерных сетях в различные моменты времени, отличается возможностью обеспечения хранения и анализа признаков пользователей, полученных на базе UBA/UEBA-аналитики и характеризующих потенциальную инсайдерскую деятельность в компьютерных сетях, а также возможностью учета динамики изменения этих признаков;

модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак отличаются применением комплексного подхода к решению задачи обнаружения инсайдеров с учетом признаков и свойств пользователей, устройств, приложений, сервисов, включая параметр времени;

методика обнаружения инсайдеров в компьютерных сетях с использованием комбинированных экспертных правил, методов машинного обучения и обработки больших данных отличаются использованием предложенной модели представления больших данных об инсайдерских атаках, а также предложенных модели и алгоритмов комбинированного применения экспертных правил, методов машинного обучения и обработки больших данных;

архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных отличаются использованием предложенной методики обнаружения инсайдеров, обеспечивающей комбинированное применение технологий обработки больших данных, экспертных правил и методов машинного обучения.

Отличительной особенностью разработанных автором предложений является строго аргументированное обоснование системотехнических решений, направленных на повышение информационной безопасности компьютерных сетей. Достоверность полученных научных результатов подтверждается наличием трех свидетельств о регистрации программ для ЭВМ.

ЗНАЧИМОСТЬ ВЫВОДОВ И РЕКОМЕНДАЦИЙ СОИСКАТЕЛЯ ДЛЯ НАУКИ И ПРАКТИКИ И ВОЗМОЖНЫЕ ПУТИ ИХ ИСПОЛЬЗОВАНИЯ

Практическая значимость результатов исследования состоит в том, что разработанные методика, модели и алгоритмы могут быть использованы при создании эффективной системы обеспечения информационной безопасности, в которой для анализа деятельности работников используются концепция больших данных совместно с экспертными правилами и методами машинного обучения, которые позволяют достигнуть наилучших показателей эффективности обнаружения инсайдеров.

Теоретическая значимость диссертационной работы определяется ее вкладом в дальнейшее развитие теории и методов информационной безопасности, что проявляется в следующих аспектах: расширены классы атрибутов, необходимых для обнаружения инсайдеров; предложен новый подход к комбинированию двух классов алгоритмов, основанных на экспертных правилах и методах машинного обучения, для решения задачи обнаружения инсайдеров в компьютерной сети; методика реализует последовательность операций, необходимых для решения задачи обнаружения инсайдеров, основывается на модели в формате NoSQL, алгоритмах, основанных на экспертных правилах, а также алгоритмах, основанных на методах машинного обучения; архитектура реализует совокупность компонентов, их взаимосвязь, процедуру их выполнения и программую реализацию для решения задачи обнаружения инсайдеров в компьютерной сети; архитектура основана на модели NoSQL, ал-

горитмах, основанных на экспертных правилах и методах машинного обучения, предложенных в диссертации.

Личный вклад определяется в осуществлении самостоятельного научно-теоретического анализа исследуемой области знаний о информационной безопасности; разработке и обосновании основных положений, которые вынесены им на защиту.

Отраженные в диссертационной работе исследования проведены в рамках ФЦП 2019-2020 гг. в соответствии с соглашением № 05.607.21.0322 (идентификатор RFMEFI60719X0322) с Минобрнауки России по теме: «Разработка методов, моделей, алгоритмов и программных средств, основанных на выявлении отклонений в эвристиках трафика сверхвысоких объемов, для обнаружения сетевых атак и защиты от них». Полученные результаты внедрены в учебный процесс СПбГУТ (учебные курсы: «Безопасность компьютерных сетей», «Безопасность беспроводных локальных сетей») и СПбГУТПД (учебные курсы «Комплексная защита информации на предприятии», «Технологии и методы программирования»), применяются в рабочем процессе Роскомнадзора по Северо-Западному федеральному округу, компании ООО «Фаст Лейн». Результаты диссертационного исследования также представлены в заявке, победившей в конкурсе субсидий молодым ученым, молодым кандидатам наук вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга, в 2019 г.

Полученные соискателем результаты целесообразно использовать в специальных службах органов внутренних дел, осуществляющих специальные технические мероприятия по противодействию преступлениям в сфере инфотелекоммуникаций (например, Управление специальными техническими мероприятиями ГУВД г. Санкт-Петербург), а также подразделениях защиты от иностранных технических разведок предприятий оборонно-промышленного комплекса Санкт-Петербурга (например, АО «НИИ «Рубин», АО «НИИ «Масштаб», ПАО «Интелтех», АО «НИИ «Вектор»).

СОДЕРЖАНИЕ И ОФОРМЛЕНИЕ ДИССЕРТАЦИИ

Диссертационная работа представлена в виде завершенной научно-квалификационной работы, которая включает в себя введение, три раздела, заключение, список источников литературы (190 наименований) и 2

приложения. Объем работы 206 станиц машинописного текста, в том числе 35 рисунка и 13 таблиц. Распределение материала по разделам последовательное и логичное, а стиль его изложения достаточно ясный и технически грамотный.

Автореферат в целом правильно отражает основные результаты диссертационной работы, которые опубликованы в 40 научных трудах, в том числе — 9 в рецензируемых изданиях из перечня ВАК, 2 — в изданиях, индексируемых в международных базах данных Scopus и Web of Science, также получено 3 свидетельства о государственной регистрации программ для ЭВМ. Содержание публикаций соответствует научным положениям, выносимым автором на защиту.

Вместе с тем в диссертационной работе необходимо отметить наличие недостатков.

Во-первых, имеют место недостатки формального характера: отдельные рисунки (например, рисунок 1.10) плохо напечатаны или неоднозначны, присутствуют грамматические ошибки, постановка задачи недостаточно формализована.

Во-вторых, ключевое понятие работы «инсайдер» четко не определено, а при попытке понять заложенный автором в это понятие смысл из текста возникает следующая ситуация: термин «инсайдер» используется и для обозначения внутреннего нарушителя, и для обозначения внешнего нарушителя (например, при приведении результатов анализа деятельности пациентов), а также для обозначения потенциального нарушителя обоих типов. Это обстоятельство существенно усложняет процесс оценки размера области исследования и сферы применения полученных результатов.

В-третьих, в работе достаточно часто упоминается, что для формирования моделей поведения «инсайдеров» должно выполняться и при подтверждении полученных результатов выполнялось привлечение экспертов. Однако, в работе не представлена информация о том, какой должна быть квалификация эксперта и по какой методике этот эксперт должен формировать модель. Это обстоятельство препятствует возможности проверить достоверность приведенных моделей.

В-четвертых, из текста третьего раздела вытекает, что автор использовал комплект общеизвестного программного обеспечения (ПО) и

разработал методику его конфигурирования, которая, по нашему мнению, уже должна быть заложена в этот комплект ПО. Из чего следует, что предложенные ранее модели — это просто входные данные для настройки выбранного комплекта ПО. Приведенные же в приложениях к работе свидетельства о регистрации программ для ЭВМ подтверждают, что архитектура разработана автором лично и совместно с разработанными моделями обладает общностью и может быть использована, например, для создания другого отечественного аналога. Однако в работе новизна самой программной реализации доказана неубедительно.

Ввиду этих соображений считаем целесообразным изменить формулировку последнего научного результата на «архитектура системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных». В этом случае содержание результата будет в большей степени соответствовать его названию.

В-пятых, и в автореферате, и в диссертации недостаточно подробно описан физический смысл приведенных формул.

Однако отмеченные недостатки имеют частный характер, принципиально не влияя на полученные в диссертационной работе научные результаты.

ВЫВОДЫ ПО РАБОТЕ

Диссертационная работа Ушакова И.А. является законченной научно-квалификационной работой, в которой решена актуальная задача исследования актуальная задача исследования, заключающаяся в разработке модельно-методического аппарата для обнаружения инсайдеров в сети на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных, и имеющая существенное значение для построения устойчивых сетей связи ведомственного назначения. Диссертация характеризует автора как сформированного специалиста, способного самостоятельно исследовать широкий круг теоретических и практических вопросов, получать обоснованные выводы и рекомендации. Содержание диссертации соответствует паспорту специальности 05.13.19 — «Методы и системы защиты информации, информационная безопасность». В целом дис-

сертационная работа Ушакова И.А. соответствует требованиям п.п. 9, 10, 11 и 14 «Положения о порядке присуждения ученых степеней» и предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук.

Отзыв обсужден и одобрен на заседании секции № 2 научно-технического совета АО «НИИ «Рубин», по которому оформлен протокол № 9о от 17 марта 2020 года.

Отзыв составили:
Главный научный сотрудник НИО
доктор технических наук, доце

Юрий Михайлович Шерстюк

Инженер отдела РКД
кандидат технических наук

Алексей Александрович Олимпиев

«26» марта 2020 г.

С отзывом ведущей организации СОГЛАСЕН
Начальник научно-исследовательского отдела
кандидат технических наук

Константин Алексеевич Смирнов

«26» марта 2020 г.