РОСКОМНАДЗОР

УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ ПО СЕВЕРО-ЗАПАДНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ

ул. Галерная, д. 27, Санкт-Петербург, 190000
тел./факс: (812) 678-95-26, e-mail: rsockanc78@rkn.gov.ru

ТВЕРЖДАЮ
авления, к.т.н.
Д.В. Сахаров
«14» апреля 2020г.

ОТ

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

Актуальность темы диссертационной работы

На современном этапе необходимость обнаружения инсайдеров в компьютерных сетях с использованием современных технологий, включающих методы обработки больших данных и методы машинного обучения, приобретает все большую значимость. Такая потребность обосновывается регулярными и многочисленными отчетами крупных компаний о фиксированных случаях инсайдерских атак с последующим размещением в открытом доступе персональных данных работников. Применение моделей, алгоритмов и методик обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и способов обработки больших данных позволяет определять инсайдеров и снизить риски нарушения сетевой безопасности в сети организации. Поэтому исследуемая проблема является актуальной, а предлагаемый в диссертационной работе подход направлен на ее решение и повышает защищенность компьютерных сетей.

Цель работы и основные результаты.

Целью исследования является повышение защищенности компьютерных сетей (КС) за счет усовершенствования моделей, алгоритмов и методики обнаружения инсайдеров в КС с использованием

00192

комбинирования экспертных правил, методов машинного обучения и способов обработки больших данных.

Основными результатами работы являются:

1. Модель представления больших данных об инсайдерских атаках в формате NoSQL, отличающаяся от существующих 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.
2. Модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак, отличающиеся от существующих комплексным подходом к решению задачи обнаружения инсайдеров с учетом признаков и свойств пользователей, устройств, приложений, сервисов, включая параметр времени.
3. Методика обнаружения инсайдеров, отличающаяся от существующих 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.
4. Архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях, отличающаяся от известных архитектур и программных средств использованием предложенной методики обнаружения инсайдеров, обеспечивающей комбинированное применение технологий обработки больших данных, экспертных правил и методов машинного обучения.

Научная новизна полученных результатов.

Научная новизна полученных результатов диссертационной работы состоит в следующем:

1. Модель представления больших данных об инсайдерских атаках в формате NoSQL, отличающаяся 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.
2. Модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак отличаются от существующих применением комплексного подхода к решению задачи обнаружения инсайдеров с учетом признаков и свойств пользователей, устройств, приложений, сервисов, включая параметр времени.
3. Методика обнаружения инсайдеров отличается 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.

4. Архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях отличается от известных архитектур и программных средств использованием предложенной методики обнаружения инсайдеров, обеспечивающей комбинированное применение технологий обработки больших данных, экспертных правил и методов машинного обучения.

Достоверность и обоснованность

Автореферат достаточно полно и корректно описывает результаты диссертационного исследования. В работе использовались классические и современные методы исследования: системный, причинно-следственный и сравнительный анализ, теория вероятностей и теория множеств, функциональный и структурный синтез, использовался компьютерный эксперимент на базе имитационного моделирования.

Достоверность и обоснованность научных положений, основных выводов и результатов диссертации обеспечиваются тщательным анализом состояния исследований в данной области, подтверждается согласованностью результатов, полученных при экспериментах, успешной апробацией в ходе научных конференций всероссийского и международного уровня и публикацией в ведущих рецензируемых научных изданиях.

Полученные в работе результаты прошли апробацию на 12-ти научных и практических конференциях, в том числе международных. По материалам исследования опубликовано 40 работ, в том числе 9 – в рецензируемых изданиях из перечня ВАК, 2 – в изданиях, индексируемых в международных базах Scopus и Web of Science, получено 3 свидетельства о государственной регистрации программ для ЭВМ.

Недостатки

Вместе с тем необходимо отметить следующие недостатки:

1. В автореферате автор использует размытые понятия «инсайдер» и «компьютерная сеть», не давая четкого определения данных терминов.
2. Второй основной научный результат состоит из множества - модель и алгоритмы; возможно, имело бы смысл или дать иное название (комплекс алгоритмов на базе модели), или разбить их на несколько (модель и комплекс алгоритмов).
3. Не приводится анализ влияния количества исследуемых записей на результаты. Неясен критерий выбора количества в 100 тыс. записей.
4. В Таблице 1 используются буквенные обозначения "мер" без их расшифровки.

Выводы:

1. В целом, судя по автореферату и публикациям, диссертация Ушакова И.А., выполненная на тему: «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных» представляет собой самостоятельную научно-квалификационную работу, в которой представлена и решена актуальная научная задача по разработке модельно-методического аппарата для обнаружения инсайдеров в КС на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных.

2. Автореферат написан грамотно и логически связно. Указанные недостатки имеют частный характер и не снижают теоретической и практической ценности полученных результатов. Автор показал умение самостоятельно вести исследования в определенном научном направлении с доведением их до законченных технических решений. Результаты работы в достаточной степени опубликованы, апробированы и реализованы. Исследование Ушакова И.А. удовлетворяет требованиям п. 9-14 Положения о присуждении учёных степеней, утвержденного Постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 года, предъявляемым к кандидатским диссертациям.

3. Считаем, что Ушаков И.А. заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Отзыв составили:

Заместитель руководителя
Управления Роскомнадзора по СЗФО,
к.ф.-м.н. Потехин Игорь Юрьевич

Заместитель руководителя
Управления Роскомнадзора по СЗФО Ларсон Ирина Михайловна

Помощник руководителя
Управления Роскомнадзора по СЗФО,
к.филос.н. Скакун Артем Александрович