масштаб
научно-
исследовательский
институт

АКЦИОНЕРНОЕ ОБЩЕСТВО
«НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ «МАСШТАБ»
(АО «НИИ «МАСШТАБ»)
Кантемировская ул., д. 5, лит. А, г. Санкт-Петербург,194100
тел.: (812) 309-03-21, факс: (812) 295-51-65
e-mail: info@mashtab.org www.mashtab.org
ОКПО 08613825, ОГРН 1127847056303, ИНН/КПП 7802777108/780201001

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

кандидата технических наук, доцента
Ефимова Вячеслава Викторовича
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»

Входные положения

Диссертационная работа выполнена в Федеральном государственном бюджетном учреждении науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук.

На отзыв были представлены:

- диссертация – 1 том объемом 215 листов;
- автореферат – брошюра объемом 1 усл. печ. лист.

1. Актуальность темы диссертационной работы

В настоящее время наблюдается рост инсайдерских атак. Все больше организаций сталкиваются с тем, что персональные данные пользователей появляются в сети Интернет в открытом доступе. Это связано с развитием информационных и телекоммуникационных технологий, которыми пользуются злоумышленники для совершения атак. Для обнаружения инсайдеров применяются математические методы, основанные на экспертных правилах (составляются экспертами по информационной безопасности), методы машинного обучения, реализуемые в программных средствах, и др. Каждый из указанных подходов имеет свои преимущества и недостатки. Чтобы совместить сильные стороны этих походов и устранить их недостатки, используют прием комбинирования, который по-прежнему остается не до конца исследованным в области обнаружения инсайдеров в компьютерных сетях. Комбинированное использование алгоритмов, основанных на экспертных правилах и методов машинного обучения позволит снизить количество пропусков атак и повысит

точность обнаружения инсайдерских сессий. Использование методов обработки больших данных оптимизирует работу с большими массивами данных и выполнять их анализ в заданные моменты времени.

Поэтому разработанный в диссертационной работе подход к обнаружению инсайдеров на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных, является перспективным, а рассматриваемая тема диссертационной работы Ушакова Игоря Александровича является актуальной как для государственных структур, так и для предприятий и организаций различных отраслей промышленности, где необходимо обеспечивать информационную безопасность данных.

2. Структура диссертационной работы

Структура диссертационной работы выглядит логичной и цельной, название глав и разделов соответствует выбранной теме и направлению исследований.

3. Научная новизна полученных результатов

Автором представлена модель представления больших данных об инсайдерских атаках в формате NoSQL, которая отличается 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. (*Ушаков, И.А. Гибридная модель базы данных NoSQL для анализа сетевого трафика. И.В. Котенко, И.А. Ушаков, Д.В. Пелёвин, А.Ю. Овраменко // Защита информации. Инсайд. – 2019. – № 1 (85). – С. 46-54*).

Разработанная 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. (*Ушаков, И.А. Выявление инсайдеров в корпоративной сети: подход на безе UBA и UEBA / И.В. Котенко, И.А. Ушаков, Д.В. Пелевин, А.И. Преображенский, А.Ю. Овраменко // Защита информации. Инсайд. – 2019. – № 5(89). – С. 26-35.)*

Соискатель разработал оригинальную методику обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных, которая отличается от существующих использованием модели представления больших данных об инсайдерских атаках (*Ушаков, И.А. Обнаружение инсайдеров в корпоративной компьютерной сети на основе технологий обработки больших данных. / И.А. Ушаков // Вестник Санкт-Петербургского государственного*

университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2019. – № 4. – С. 38-43).

Разработанная 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 (*Ушаков И.А. Система обнаружения инсайдеров в корпоративной компьютерной сети с использованием технологий машинного обучения: свидетельство о государственной регистрации программы для ЭВМ / И.А. Ушаков, И.В. Котенко, Ю.В. Твердохлебова. – Рег. № 2019666738. – 13.12.2019.*).

Таким образом, диссертационная работа содержит значимые научные результаты по заявленной специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»: «Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса». (п.3 паспорта специальности).

4. Степень обоснованности и достоверность научных положений, выводов и рекомендаций

Достоверность и достаточная степень обоснованности научных положений, выводов и рекомендаций подтверждается:

- выполненным анализом состояния научных и практических исследований в области обнаружения инсайдеров в компьютерных сетях;
- актами о внедрении результатов диссертационного исследования;
- публикациями в ведущих рецензируемых изданиях.

5. Практическая значимость

Разработанный методический аппарат и программная реализация могут быть использованы для обнаружения инсайдеров в компьютерных сетях, функционирующих в интересах Федеральных органов исполнительной власти и предприятий различных отраслей промышленностей.

Считаю целесообразным, кроме того, использование научных и практических результатов диссертации в учебном процессе учреждений высшего образования при подготовке аспирантов, магистров, специалистов и бакалавров в области телекоммуникаций, автоматизированных систем управления, защиты информации.

6. Замечания по диссертационной работе

Диссертационная работа выполнена на актуальную тему, связанную с решением задачи обнаружения инсайдеров в компьютерных сетях.

В качестве замечаний следует отметить:

1) В качестве метода обработки больших данных используется алгоритм MapReduce. Использование потоковой обработки данных с использованием надстройки Spark позволило бы повысить эффективность разработанной архитектуры и программной реализации.

2) Использование в качестве комбинаций алгоритмов простых математических операций объединения и пересечения в формуле на стр. 120 диссертации возможно стоило бы дополнить более сложными, например, использовать алгоритмы взвешенного голосования или голосования меньшинством.

3) Формулы в диссертации не пронумерованы.

4) Основные положения, за исключением 3 положения «Методика обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных», выносимые на защиту опубликованы соискателем не единолично, в соавторстве.

Следует отметить, что выявленные замечания не снижают положительную оценку диссертационного исследования и не влияют на новизну, практическую значимость, обоснованность и достоверность полученных в нем результатов.

7. Вывод

Диссертационная работа Ушакова Игоря Александровича на тему: «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных», представленная на соискание учёной степени кандидата технических наук по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность», является законченной научно-квалификационной работой, которая отличается хорошо структурированным и грамотным изложением. Полученные автором новые научные положения можно квалифицировать как решение важной научной задачи обнаружения инсайдеров в компьютерных сетях.

Результаты исследований апробированы на научных конференциях.

Основные результаты диссертационной работы в достаточной степени отражены в опубликованных автором 31 печатных работах, в том числе в 9 работах, рекомендованных ВАК РФ и в 2 журналах, входящих в базы цитирования Web of Science и Scopus. Уровень и объем публикаций соответствует требованиям п.11 и п.13 Положения о присуждении ученых степеней, утвержденного Постановлением Правительства Российской Федерации от 24.09.2013 года № 842 (в ред. Постановлений Правительства РФ от 21.04.2016 N 335, от 02.08.2016 N 748, от 29.05.2017 N 650, от 28.08.2017 N 1024, от 01.10.2018 N 1168) (далее Положение).

По результатам рассмотрения диссертации не обнаружены какие-либо факты использования заимствованных материалов без ссылки на источники, т.е. диссертация соответствует требованиям п. 14 Положения.

Автореферат диссертации, в целом, достаточно полно отражает ее содержание и соответствует требованиям п.25 Положения.

Уровень диссертации соответствует п. 9 Положения. Работа соответствует заявленной специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность», а соискатель, Ушаков Игорь Александрович, заслуживает присуждения учёной степени кандидата технических наук.

Официальный оппонент:

советник генерального директора, начальник научно-системного центра АО «НИИ «Масштаб»

кандидат технических наук, доцент

В.В. Ефимов

«19» марта 2020 г.

Подпись В.В. Ефимова заверяю:

Начальник центра по работе с персоналом АО «НИИ «Масштаб»

М. Б. Водолажская

«19» марта 2020 г.

ФИО: Ефимов Вячеслав Викторович
Ученая степень: кандидат технических наук
Ученое звание: доцент
Место работы: АО «НИИ «Масштаб»
Должность: советник генерального директора, начальник научно-системного центра АО «НИИ «Масштаб»
Рабочий почтовый адрес:194100, г. Санкт-Петербург, Кантемировская ул., д. 5, лит. А.
Телефон (рабочий): 8 (812) 309-03-21 (доб. 341)
Адрес электронной почты: v.efimov@mashtab.org