МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)

14 линия, д. 39, Санкт-Петербург, 199178
Телефон: (812) 328-33-11, факс: (812) 328-44-50
E-mail: spiiran@iias.spb.su, http://www.spiiran.nw.ru
ОКПО 04683303, ОГРН 1027800514411
ИНН/КПП 7801003920/780101001

УТВЕРЖДАЮ

Директор СПИИРАН

фессор РАН

Ронжин А.Л.

«14» января 2020 г.

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН)

по диссертации Ушакова Игоря Александровича «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

Диссертация «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных» выполнена в лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

Соискатель Ушаков Игорь Александрович прикреплен к Федеральному государственному бюджетному учреждению науки Санкт-Петербургскому институту информатики и автоматизации Российской академии наук для подготовки диссертации на соискание ученой степени кандидата технических наук без освоения программ подготовки научно-педагогических кадров в аспирантуре.

В 2010 году закончил Государственное образовательное учреждение высшего профессионального образования «Санкт-Петербургский

государственный университет телекоммуникаций» по специальности «Защищенные системы связи».

Справка о сдаче кандидатских экзаменов №56003010/рег №199, выдана в 2019 г. Федеральным государственным бюджетным образовательным учреждением высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича».

Научный руководитель — Котенко Игорь Витальевич, доктор технических наук, главный научный сотрудник лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук.

По результатам рассмотрения диссертации «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных» принято следующее заключение:

В диссертационной работе Ушакова И.А. решена научная задача разработки модельно-методического аппарата для обнаружения инсайдеров в компьютерных сетях на основе комбинированного использования экспертных правил, методов машинного обучения и обработки больших данных. Значительная практическая значимость и недостаточная научная проработка проблемы определили выбор темы, ее актуальность, цель, задачи, основные направления и содержание диссертационного исследования.

В работе лично Ушаковым И.А. получены **следующие результаты**:
1) модель представления больших данных об инсайдерских атаках в формате NoSQL, обеспечивающая хранение и анализ признаков пользователей в компьютерных сетях в различные моменты времени; 2) модель и алгоритмы комбинированного применения экспертных правил и методов машинного обучения в интересах обнаружения инсайдерских атак; 3) методика обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных; 4) архитектура и программная реализация системы обнаружения инсайдеров в компьютерных сетях с использованием комбинирования экспертных правил, методов машинного обучения и обработки больших данных.

В работе расширены классы атрибутов, необходимых для обнаружения инсайдеров; предложен новый подход к комбинированию двух классов алгоритмов, основанных на экспертных правилах и на методах машинного обучения, для решения задачи обнаружения инсайдеров в КС; методика обнаружения инсайдеров реализует последовательность операций, необходимых для решения задачи выявления внутренних злоумышленников, основывается на модели представления больших данных 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

программную реализацию для решения задачи обнаружения инсайдеров в КС; архитектура основана на модели представления больших данных в формате NoSQL, алгоритмах, основанных на экспертных правилах и методах машинного обучения, предложенных в диссертации.

Содержание диссертации и основные положения, выносимые на защиту, отражают личный вклад автора в опубликованных работах, причем вклад диссертанта был существенным. Представленные к защите результаты получены лично автором.

Достаточная степень достоверности полученных результатов обеспечивается проведением анализа существующих результатов исследований в предметной области, корректностью исходных предпосылок, соответствием результатов моделирования общим закономерностям, реализацией результатов работы в проекте, а также апробацией основных теоретических положений диссертации в печатных трудах и докладах на международных и российских научных конференциях: международной конференции по интеллектуальным распределенным вычислениям IDC-2019 (Санкт-Петербург, 2019), международной конференции IEEE SMARTWORLD ATC-2017 (Сан-Франциско, 2017); Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России» (Санкт-Петербург, 2015, 2017, 2019), Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании» в СПбГУТ (Санкт-Петербург, 2015–2019).

Новизна и практическая значимость результатов исследования. Научная новизна полученных результатов диссертационной работы состоит в следующем: 1) модель представления больших данных об инсайдерских атаках в формате NoSQL 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; 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 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 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.

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»

По результатам выполнения диссертационного исследования получено 3 свидетельства о регистрации программ для ЭВМ:

1. Ушаков И.А. Компонент предобработки трафика в корпоративной компьютерной сети с использованием алгоритма Map Reduce в Hadoop кластере: свидетельство о государственной регистрации программы для ЭВМ / И.А. Ушаков, И.В. Котенко, А.Ю. Овраменко. – рег. № 2019666737. – 13.12.2019.
2. 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.
3. Ушаков И.А. Система обнаружения инсайдера в корпоративной компьютерной сети, используя алгоритмы, основанные на экспертных правилах: свидетельство о государственной регистрации программы для ЭВМ / И.А. Ушаков, И.В. Котенко, Д.В. Пелёвин – рег. № 2019666959. – 17.12.2019.

Диссертационная работа соответствует требованиям п. 9-14 Положения о присуждении ученых степеней и п. 3 Паспорта специальностей ВАК по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность» (технические науки).

Полнота изложения материалов диссертации в работах, опубликованных соискателем. Основные результаты диссертации изложены в необходимой полноте в 40 печатных работах, в том числе в 9 статьях в научных журналах из Перечня ВАК, в 2 статьях в изданиях, индексируемых в международных базах Scopus и Web of Science:

1. 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.
2. Ушаков, И.А. Масштабируемое honeypot-решение для обеспечения безопасности в корпоративных сетях / А.В. Красов, Р.Б. Петрив, Д.В. Сахаров, Н.Л. Сторожук, И.А. Ушаков // Труды учебных заведений связи. 2019. – Т. 5. – №. 3. – С. 86-97.

3. Ушаков, И.А. Исследование модели сети ЦОД на основе политик Cisco ACI / Н.В. Савинов, К.А. Токарева, И.А. Ушаков, А.В. Красов, Д.В. Сахаров // Защита информации. Инсайд. – 2019. – № 4 (88). – С. 32-43.
4. Ушаков, И.А. Комплексный подход к обеспечению безопасности киберфизических систем на основе микроконтроллеров / И.В. Котенко, Д.С. Левшун, А.А. Чечулин, И.А. Ушаков, А.В. Красов // Вопросы кибербезопасности. 2018. – № 3 (27). – С. 29-38.
5. Ушаков, И.А. Обеспечение безопасности передачи multicast-трафика в ip-сетях / А.В. Красов, Д.В. Сахаров, И.А. Ушаков, Е.П. Лосин // Защита информации. Инсайд. 2017. – № 3 (75). – С. 34-42.
6. 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.
7. Ушаков, И.А. Система сбора, хранения и обработки информации и событий безопасности на основе средств Elastic Stack / И.В. Котенко, А.А. Кулешов, И.А. Ушаков // Труды СПИИРАН. – 2017. – № 5 (54). – С. 5-34.
8. Ушаков, И.А. Технологии больших данных для мониторинга компьютерной безопасности / И.В. Котенко, И.А. Ушаков // Защита информации. Инсайд. 2017. – № 3 (75) – С. 23-33.
9. Ушаков, И.А. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA / И.В. Котенко, И.А. Ушаков, Пелевин Д.В., Преображенский А.И., Овраменко А.Ю. // Защита информации. Инсайд. 2019. – № 5 (89). – С. 2-11.
10. Ushakov, I. Aggregation of elastic stack instruments for collecting, storing and processing of security information and events / I. Kotenko, A. Kuleshov, I. Ushakov // 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI) 2017. – PP. 1-8.
11. Ushakov, I. Approach to Detection of Denial-of-Sleep Attacks in Wireless Sensor Networks on the base of Machine Learning / A. Balueva, V. Desnitsky, I. Ushakov. – PP. 350-355.

Ценность научных работ соискателя заключается в том, что они раскрывают методологию и результаты решения задач, поставленных с диссертационном исследовании, а также обеспечивают воспроизводимость полученных научных результатов.

Диссертация «Обнаружение инсайдеров в компьютерных сетях на основе комбинирования экспертных правил, методов машинного обучения и обработки больших данных» Ушакова Игоря Александровича рекомендуется к защите на соискание ученой степени кандидата технических наук по

специальности 05.13.09 «Методы и системы защиты информации, информационная безопасность».

Заключение принято на расширенном семинаре лабораторий проблем компьютерной безопасности, информационно-вычислительных систем и технологий программирования, кибербезопасности и постквантовых криптосистем СПИИРАН. Присутствовало на семинаре 19 чел. Результаты голосования: «за» — 17 чел., «против» — 1 чел., «воздержалось» — 1 чел., протокол №1 от 14.01.2020 г.

Председатель семинара:
доктор технических наук, профессор,
руководитель лаборатории
информационно-вычислительных
систем и технологий программирования

Василий Юрьевич Осипов

Секретарь семинара:
кандидат технических наук, старший
научный сотрудник лаборатории
проблем компьютерной
безопасности

Александр Александрович Браницкий

14 января 2020г.