МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ «САНКТ-ПЕТЕРБУРГСКИЙ ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК» (СПб ФИЦ РАН)
14 линия В.О., д. 39, Санкт-Петербург, 199178
Телефон: (812) 328-34-11, факс: (812) 328-44-50, E-mail: info@spcras.ru, https://spcras.ru/
ОКПО 04683303, ОГРН 1027800514411, ИНН/КПП 7801003920/780101001

УТВЕРЖДАЮ
Директор СПб ФИЦ РАН
Профессор РАН

____ А.Л. Ронжин
15 февраля 2023 г.

ЗАКЛЮЧЕНИЕ

Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) по диссертации Крибеля Александра Михайловича «Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность (технические науки)

Диссертация «Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения» выполнена в лаборатории компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук».

Соискатель Крибель Александр Михайлович является младшим научным сотрудником лаборатории компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» и подготовил диссертацию на соискание ученой степени кандидата технических наук без освоения программ подготовки научно-педагогических кадров в аспирантуре.

Крибель Александр Михайлович в 2016 году закончил Челябинского государственного университета по специальности «Информационная безопасность автоматизированных систем».

Справки о сдаче кандидатских экзаменов № 2/2022 выдана 05 июля 2022 года Федеральным государственным бюджетным учреждением науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» (СПб ФИЦ РАН) и № 1833 от 7 апреля 2022 года Федеральным государственным казённым военным образовательным учреждением высшего образования Военная орденов Жукова и Ленина Краснознаменная академия связи имени Маршала Советского Союза С.М. Буденного» Министерства обороны Российской Федерации.

Научный руководитель — Лаута Олег Сергеевич, доктор технических наук, профессор кафедры Комплексного обеспечения информационной безопасности Федерального государственного бюджетного образовательного учреждения высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова».

По результатам рассмотрения диссертации «Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения» принято следующее заключение:

Оценка выполненной соискателем работы:

В работе выполнен детальный анализ моделей воздействия компьютерных атак в сети передачи данных, а также алгоритмов выявления компьютерных атак, систем мониторинга и методик противодействия компьютерным атакам в сети передачи данных. Разработана аналитическая модель выявления аномалий в сетевом трафике сети передачи данных в условиях компьютерных атак. Разработаны методики раннего обнаружения аномалий в сетевом трафике сети передачи данных и классификации компьютерных атак в сетевом трафике сети передачи данных. Разработана архитектура и программный прототип компонентов системы раннего обнаружения и классификации компьютерных атак в сетевом трафике сети передачи данных, проведена экспериментальная и теоретическая оценка эффективности предложенных моделей, методик и архитектуры. Предложенная архитектура и программные прототипы компонентов системы раннего обнаружения и классификации компьютерных атак в сетях передачи данных отличаются от известных тем, что они ориентированы на раннее обнаружение как известных, так и неизвестных компьютерных атак с минимальным количеством ложных срабатываний за счет реализации методов фрактального анализа и искусственной нейронной сети LSTM-типа. Проведена апробация программного прототипа при реализации его в системах глубокой проверки пакетов и предотвращения вторжений.

Личное участие соискателя в получении результатов, изложенных в диссертации:

Содержание диссертации и основные положения, выносимые на защиту, отражают личный вклад автора в опубликованных работах. Публикация полученных результатов проводилась совместно с научным руководителем Лаутой О.С., причем вклад диссертанта был существенным. Представленные к защите результаты получены лично автором.

Степень достоверности результатов проведенных исследований:

Достоверность научных положений, основных выводов и результатов диссертации подтверждается анализом состояния исследований в данной области, согласованностью теоретических выводов с результатами экспериментальной проверки алгоритмов, а также апробацией основных теоретических положений диссертации в печатных трудах и докладах на международных и российских научных специализированных конференциях: Международная научно-практическая конференция «РусКрипто» (Московская область, 2021 и 2022); Межвузовская научно-практическая конференция «Актуальные проблемы обеспечения информационной безопасности» (Самара, 2017); Двенадцатая общероссийская молодежная научно-техническая конференция «Молодежь. Техника. Космос.» (Санкт-Петербург, 2020); Всероссийская научно-техническая конференция «Состояние и перспективы развития современной науки по направлению «Информационная безопасность»» (Анапа, 2021 и 2020); Всероссийская научно-техническая конференция «Состояние и перспективы развития современной науки по направлению «АСУ, информационно-телекоммуникационные системы»» (Анапа, 2021); Всероссийская научно-практическая конференция РАРАН «Актуальные проблемы защиты и безопасности» (Санкт-Петербург, 2019); Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании» (Санкт-Петербург, 2019); Всеармейская научно-практическая конференция «Инновационная деятельность в Вооруженных Силах Российской Федерации», (Санкт-Петербург, 2017).

Научная новизна полученных результатов:

Разработана аналитическая модель выявления аномалий в сетевом трафике сетей передачи данных в условиях компьютерных атак, в отличие от известных, описывает не только стационарный, но и нестационарный сетевой трафик и обосновывает выбор фрактального метода выявления аномалий в интересах дальнейшей классификации компьютерных атак в зависимости от типа трафика.

Разработана методика раннего обнаружения аномалий в сетевом трафике сетей передачи данных, в отличие от известных, способна проводить прогнозирование и обнаружение не только известных, но и неизвестных компьютерных атак на раннем этапе их проявления благодаря совместному применению методов фрактального анализа и искусственной нейронной сети LSTM-типа (рекуррентные нейронные сети с долгой краткосрочной памятью), в результате чего существенно сокращается время выявления аномалий и уменьшается количество ложных срабатываний.

Разработана методика классификации компьютерных атак в сетевом трафике сетей передачи данных отличается от известных тем, что в ней обнаружение компьютерных атак производится с использованием генеративно-состязательной сети, которая производит дообучение классификатора на скрытых латентных представлениях, полученных автокодировщиком, исходя из анализа данных о функционировании сетей передачи данных.

Разработана архитектура и программные прототипы компонентов системы раннего обнаружения и классификации компьютерных атак в сетях передачи

данных отличаются от известных тем, что они ориентированы на раннее обнаружение как известных, так и неизвестных компьютерных атак с минимальным количеством ложных срабатываний за счет реализации методов фрактального анализа и искусственной нейронной сети LSTM-типа.

Практическая значимость полученных результатов:

Разработанные аналитическая модель и методики представляют собой научно-методическую основу, практическая реализация которой позволяет описать различные типы трафика в сетях передачи данных, определять аномальные активности, основываясь на принципах самоподобия, и, исходя из типа трафика с применением различных методов машинного обучения, выявлять компьютерные атаки. Разработанные методики являются математической основой системы раннего обнаружения компьютерных атак, основанные на обнаружении аномалий в сетях передачи данных и принятии эффективных мероприятий по защите с применением нейронной сети автокодировщика, состоящей из ячеек с долгой краткосрочной памятью и управляющим рекуррентным блоком. При этом повышается оперативность, точность и полнота выявления аномалий в сетях передачи данных, что позволяет на практике эффективно применять разработанный подход в системах глубокой проверки сетевых пакетов в сетях передачи данных.

Разработанные модели, методики и алгоритм выявления аномалий и классификация компьютерных атак были реализованы в программной системе и использованы рядом коммерческих и государственных организаций в научно-образовательном процессе, в частности, при проведении исследовательских работ СПб ФИЦ РАН, Военной академии связи, ПАО «Интелтех» и в учебном процессе Военной академии связи, получены соответствующие акты внедрения. Программный компонент обнаружения аномалий сетевого трафика на основе принципов фрактального анализа данных имеет свидетельство о государственной регистрации программы для ЭВМ.

Специальность, которой соответствует диссертация

Работа соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность (технические науки).

Полнота изложения материалов диссертации в работах, опубликованных соискателем

Основные результаты диссертации изложены в достаточной полноте в следующих 17 научных публикациях:

1. Kotenko, I., Saenko, I., Lauta, O., Kribel, A. A proactive protection of smart power grids against cyberattacks on service data transfer protocols by computational intelligence methods // Sensors 2022, 22, 7506. **(WoS/Scopus – Q1).**

2. Kotenko, I., Saenko, I., Lauta, O., Kribel, A. An approach to detecting cyber attacks against smart power grids based on the analysis of network traffic self-similarity // Energies, 2020, 13(19), 5031. **(WoS/Scopus – Q2).**

3. Kribel, A., Saenko, I., Kotenko, I. Detection of Anomalies in the Traffic of Information and Telecommunication Networks Based on the Assessment of its Self-Similarity // Proceedings - 2020 International Russian Automation Conference, RusAutoCon 2020, 2020, pp. 713–718, 9208147. **(WoS/Scopus).**

4. Kotenko, I., Saenko, I., Kribel, A., Lauta, O. A technique for early detection of cyberat-tacks using the traffic self-similarity property and a statistical approach // Proceedings - 29th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2021, 2021, pp. 281–284, 9407132. **(WoS/Scopus).**

5. Kotenko, I., Saenko, I., Lauta, O., Kribel, A. Ensuring the survivability of embedded computer networks based on early detection of cyber attacks by integrating fractal analysis and statistical methods // Microprocessors and Microsystemsthis link is disabled, 2022, 90, 104459. **(WoS/Scopus – Q3).**

6. Kotenko, I., Saenko, I., Lauta, O., Kribel, A. Anomaly and cyber attack detection technique based on the integration of fractal analysis and machine learning methods // Informatics and Automationthis link is disabled, 2022, 21(6), pp. 1328–1358. **(WoS/Scopus – Q3).**

7. Панков А.В., Крибель А.М., Лаута О.С., Васильев Н.А. Метод по совершенствованию информационно- аналитической работы на основе комплексирования результатов распознавания состояний объектов контроля с использованием методов машинного обучения // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 2. С. 27-35. **(Перечень ВАК)**.

8. Перов Р.А., Лаута О.С., Крибель А.М., Федулов Ю.М. Комплексная методика обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 2. С. 44-51. **(Перечень ВАК)**.

9. Перов Р.А., Лаута О.С., Крибель А.М., Федулов Ю.В. Метод выявления аномалий в сетевом трафике // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 3. С. 25-31. **(Перечень ВАК)**.

10. Котенко И.В., Саенко И.Б., Лаута О.С., Крибель А.М. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6 (98). С. 64-71. **(Перечень ВАК)**.

11. Крибель А.М., Лаута О.С., Филин А.В., Фень А.С. Метод обнаружения аномалий в сетевом компьютерном трафике на основе нейронной сети с использованием LSTM // Электросвязь. 2021. № 12. С. 43-48. **(Перечень ВАК)**.

12. Саенко И.Б., Лаута О.С., Карпов М.А., Крибель А.М. Модель угроз ресурсам ИТКС как ключевому активу критически важного объекта инфраструктуры // Электросвязь. 2021. № 1. С. 36-44. **(Перечень ВАК)**.

13. Котенко И.В., Крибель А.М., Лаута О.С., Саенко И.Б. Анализ процесса самоподобия сетевого трафика как подход к обнаружению кибератак на компьютерные сети // Электросвязь. 2020. № 12. С. 54-59. **(Перечень ВАК)**.

14. Крибель А.М. Методика обнаружения коллизий сетевого трафика // Известия Тульского государственного университета. Технические науки. 2021. № 12. С. 182-190. **(Перечень ВАК)**.

15. Крибель А.М., Перов Р.А., Лаута О.С., Сычужников В.Б. Методика обнаружения компьютерных атак с помощью фрактального анализа и методов машинного обучения // Известия Тульского государственного университета. Технические науки. 2022. № 5. С. 166-178. **(Перечень ВАК)**.

16. Крибель А.М., Перов Р.А., Лаута О.С., Скоробогатов С.Ю. Модель выявления аномалий в сетевом трафике сети передачи данных в условиях компьютерных атак // Известия Тульского государственного университета. Технические науки. 2022. № 5. С. 228-239. **(Перечень ВАК)**.

17. Котенко И. В., Саенко И. Б., Лаута О. С., Крибель А.М. Программный компонент обнаружения аномалий сетевого трафика на основе принципов фрактального анализа данных // Свидетельство о регистрации программы для ЭВМ 2021680188, 07.12.2021.

Ценность научных работ соискателя заключается в том, что они раскрывают методологию решения задачи по разработке аналитической модели и методик выявления аномалий и классификация компьютерных атак в сетевом трафике сети передачи данных на основе применения фрактального анализа и методов машинного обучения, поставленной в диссертационном исследовании, а также обеспечивают воспроизводимость полученных научных результатов.

Диссертационная работа соответствует требованиям пунктов 9-14 «Положения о присуждении ученых степеней», утвержденного Постановлением Правительства РФ от 24.09.2013 №842.

Диссертация «Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения» Крибеля Александра Михаловича рекомендуется к защите на соискание ученой степени кандидата технических наук по специальности 2.3.6 - Методы и системы защиты информации, информационная безопасность (технические науки).

Заключение принято на расширенном семинаре Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук». Присутствовало на заседании 11 чел. Результаты голосования: «за» — 11 чел., «против» — 0 чел., «воздержалось» — 0 чел., протокол №1 от 30.01.2023 г.

Главный научный сотрудник
лаборатории компьютерной безопасности
доктор технических наук, профессор

Молдовян Николай Андреевич

Ведущий научный сотрудник
лаборатории компьютерной безопасности
кандидат технических наук, доцент

Чечулин Андрей Алексеевич