ЗАКЛЮЧЕНИЕ ДИССЕРТАЦИОННОГО СОВЕТА 24.1.206.01, СОЗДАННОГО НА БАЗЕ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО УЧРЕЖДЕНИЯ НАУКИ «САНКТ-ПЕТЕРБУРГСКИЙ ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК» МИНИСТЕРСТВА НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ, ПО ДИССЕРТАЦИИ НА СОИСКАНИЕ УЧЕНОЙ СТЕПЕНИ КАНДИДАТА НАУК

аттестационное дело № _____

решение диссертационного совета от 18.05.2023 г. № 1

О присуждении Крибелю Александру Михайловичу, гражданину Российской Федерации, ученой степени кандидата технических наук.

Диссертация «Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения» по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» принята к защите 16 марта 2023 г., протокол заседания № 1 диссертационным советом 24.1.206.01, созданным на базе Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», Министерства науки и высшего образования Российской Федерации, 199178, Россия, Санкт-Петербург, 14 линия ВО, дом 39, утвержден приказом Минобрнауки России №105/нк от 11 апреля 2012 г. (с изменениями согласно приказам №574/нк от 15 октября 2014 г., № 386/нк от 27 апреля 2017 г., №748/нк от 12 июля 2017 г., №301/нк от 23 ноября 2018 г., №467/нк от 4 августа 2020 г., №804/нк от 16 декабря 2020 г., 561/нк от 03 июня 2021 г., 384/нк от 19 апреля 2022 г.).

Соискатель Крибель Александр Михайлович, 01 января 1994 года рождения, в 2016 г. окончил специалитет Федерального государственного бюджетного образовательного учреждения высшего образования «Челябинский государственный университет» по специальности «10.05.03 Информационная безопасность автоматизированных систем» (диплом № 107405 0326662). Удостоверение о сдаче кандидатских экзаменов по специальности №2/2022 от

«05» июля 2022г. выдано Федеральным государственным бюджетным учреждением науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук», удостоверение о сдаче кандидатских экзаменов по иностранному языку и истории и философии науки №1833 от «07» апреля 2022г. выдано Федеральным государственным казенным военным образовательным учреждением высшего образования «Военная Орденов Жукова и Ленина Краснознаменная Академия Связи им. Маршала Советского Союза С.М. Буденного». В настоящее время Крибель Александр Михайлович работает младшим научным сотрудником лаборатории компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» Министерства науки и высшего образования Российской Федерации.

Диссертация выполнена в лаборатории компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургский Федеральный исследовательский центр Российской академии наук» Министерства науки и высшего образования Российской Федерации.

Научный руководитель – доктор технических наук ЛАУТА Олег Сергеевич, основное место работы: Федеральное государственное бюджетное образовательное учреждение высшего образования «Государственный университет морского и речного флота имени адмирала С.О. Макарова», кафедра «Комплексного обеспечения информационной безопасности», профессор кафедры.

Официальные оппоненты:

ГРЕЧИШНИКОВ Евгений Владимирович, доктор технических наук, профессор, Акционерное общество «Научно-исследовательский институт «Рубин», директор по инновационному развитию;

БИРЮКОВ Денис Николаевич, доктор технических наук, доцент, Федеральное государственное бюджетное военное образовательное учреждение высшего образования «Военно-космическая академия имени А.Ф. Можайского», кафедра «Систем сбора и обработки информации», начальник кафедры

дали положительные отзывы на диссертацию.

Ведущая организация – акционерное общество «Информационные технологии и коммуникационные системы» (АО «ИнфоТеКС»), г. Москва в своем положительном отзыве, подписанном Уривским Алексеем Викторовичем, кандидатом физико-математических наук, заместителем генерального директора по науке и инновациям АО «ИнфоТеКС», Гузевым Олегом Юрьевичем, кандидатом технических наук, старшим исследователем Центра научных исследований и перспективных разработок АО «ИнфоТеКС» и утвержденном Чапчаевым Андреем Анатольевичем, генеральным директором АО «ИнфоТеКС», указала, что диссертационная работа Крибеля А.М. является законченной научно-квалификационной работой, в которой решена актуальная научная задача, заключающаяся в 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, имеющая существенное значение для построения защищенных сетей передачи данных.

Разработанные в диссертационной работе методики и алгоритм имеют высокую скорость обнаружения компьютерных атак,

Следует отметить, что результаты проведенных Крибелем А.М. исследований могут быть использованы в системах обнаружения вторжений (IDS) и системах предотвращения вторжений (IPS).

Диссертация характеризует автора как сформированного специалиста, способного самостоятельно исследовать широкий круг теоретических и практических вопросов, получать обоснованные выводы и рекомендации. Содержание работы соответствует специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Задачи, поставленные в диссертационной работе, решены в полном объеме. Диссертация и автореферат изложены грамотным, четким и доказательным языком технических публикаций.

В целом диссертационная работа Крибеля А.М. соответствует требованиям пп. 9–14 «Положение о присуждении ученых степеней», утвержденного Постановлением Правительства Российской Федерации от 24.09.2013г. №842 (в редакции от 26.01.2023г. №101),предъявляемым к кандидатским диссертациям, а ее

автор заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Соискатель имеет 17 опубликованных работ, в том числе по теме диссертации 17 работ, опубликованных в рецензируемых научных изданиях 3 работы, индексируемых в WoS/Scopus – 6. Имеется 1 свидетельство о государственной регистрации программы для ЭВМ.

Основные научные результаты опубликованы в 17 научных трудах общим объемом 9,86 п.л., из которых объем личного вклада соискателя составляет 6,7 п.л. Наиболее значимые работы по теме диссертации:

1. **Kribel A.**, Kotenko I., Saenko I., Lauta O. A proactive protection of smart power grids against cyberattacks on service data transfer protocols by computational intelligence methods // Sensors. 2022. №22. 7506. Doi: 10.3390/s22197506 (Scopus Q1) *Личный вклад соискателя – 55%*

2. .**Kribel A.**, Kotenko I., Saenko I., Lauta O. An approach to detecting cyber attacks against smart power grids based on the analysis of network traffic self-similarity // Energies. 2020. №13(19). 5031. Doi: 10.3390/en13195031 (Scopus Q2) *Личный вклад соискателя – 55%.*

3. **Крибель А.М.**, Перов Р.А., Лаута О.С., 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. *Личный вклад соискателя – 45%.*

4. **Крибель А.М.**, Перов Р.А., Лаута О.С., Федулов Ю.В. Метод выявления аномалий в сетевом трафике // Наукоемкие технологии в космических исследованиях Земли. 2022. Т. 14. № 3. С. 25-31.. *Личный вклад соискателя – 35%.*

5. **Крибель А.М.**, Котенко И.В., Саенко И.Б., Лаута О.С. Метод раннего обнаружения кибератак на основе интеграции фрактального анализа и статистических методов // Первая миля. 2021. № 6 (98). С. 64-71. *Личный вклад соискателя – 35%.*

6. **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. *Личный вклад соискателя – 65%.*

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

Оригинальность содержания диссертации составляет не менее 87,8% от общего объёма текста (включая самоцитирование); цитирование оформлено корректно; заимствованного материала, использованного в диссертации без ссылки на автора либо источник заимствования, не обнаружено; научных работ, выполненных соискателем учёной степени в соавторстве без ссылок на соавторов не выявлено. Недостоверные сведения об опубликованных соискателем ученой степени работах в диссертации отсутствуют.

На диссертацию и автореферат поступило 6 отзывов, все отзывы положительные:

1. ФГБОУ ВО «Челябинский государственный университет». Отзыв составили профессор кафедры радиофизики и электроники д.ф-м.н., доцент Загребин М.А., доцент кафедры радиофизики и электроники к.ф-м.н. Анзулевич А.П. Замечания: Модель угроз недостаточно конкретизирована: каким образом определен злоумышленник и сформированы его возможности в отношении СПД. В четвертом разделе работы, посвященном описанию разработанных научно-технических предложений, автором не поясняется, как происходит классификация аномалий, то есть не охарактеризован критерий «аномальности» всплесков трафика в СПД.

2. ФГАОУ ВО «Санкт-Петербургский государственный университет аэрокосмического приборостроения». Отзыв составила доцент кафедры Метрологического обеспечения инновационных технологий и промышленной безопасности, к.т.н., доцент Степашкина А.С. Замечания: Не понятно, каким образом осуществляется интеграция разработанного метода и программного продукта в системы информационной безопасности предприятий. Отсутствуют расшифровки аббревиатур.

3. ФГКВОУ ВО «Военный ордена Жукова университет радиоэлектроники». Отзыв составил доцент 32 кафедры к.т.н. Пермяков А.С., начальник 32 кафедры, к.п.н., доцент Тихомиров В.А. Замечания: Недостаточно обоснованы показатели

защищенности СПД и показатель Херста в условиях КА. В автореферате не раскрыто, каким образом в методике вычисляются аномальные всплески в трафике. В автореферате не в полной мере раскрыты возможности программного комплекса раннего обнаружения КА: он только по нейтрализации или только выявления КА.

4. ФГАОУ ВО «Национальный исследовательский университет ИТМО». Отзыв составила доцент Факультета безопасности информационных технологий, к.т.н Евглевская Н.В. Замечания: Из автореферата не ясно, как связаны между собой компьютерные атаки «нулевого дня» и аномалии в сетевом трафике. При описании архитектуры и программного компонента системы раннего обнаружения и классификации КА в сетевом трафике СПД не раскрыто, какие образом реализована нейтрализация.

5. ФГКВОУ ВО «Краснодарское высшее военное орденов Жукова и Октябрьской Революции. Краснознаменное училище имени генерала армии С.М.Штеменко». Отзыв составили сотрудники д.т.н., профессор Максимов Р.В., к.т.н., доцент Медведев А.Н. Замечания: В автореферате недостаточно подробно раскрыт вопрос обоснования выбора показателя самоподобия в качестве критерия аномальности нестационарного трафика по отношению к использованию классических моделей временных рядов и методов машинного обучения. Из автореферата не совсем ясно, как оценивалась эффективность разработанных научно-технических предложений.

6. АО «Научно-технический центр «Атлас». Отзыв составил д.т.н. Егорова Н.А., к.т.н. Безяев А.В. Замечания: В автореферате неполно описана разработанная аналитическая модель: не указаны предположения, положенные в ее основу, отсутствуют объяснения параметров в формулах и границы их применимости. В автореферате не приведено обоснование выбора фрактального метода анализа в качестве математического аппарата для выявления аномалий в сетевом трафике. В автореферате не приведены условия, при которых были получены достаточно высокие значения вероятностей обнаружения КА.

Выбор официальных оппонентов и ведущей организации обосновывается тем, что д.т.н., профессор Гречишников Е.В. является известным ученым в области

построения защищенных сетей и систем связи в условиях преднамеренных деструктивных воздействий, защиты их от иностранной технической разведки и информационно-технических воздействий; д.т.н., профессор, Бирюков Д.Н. – известный специалист в области математических методов защиты информации; ведущая организация, акционерное общество «Информационные технологии и коммуникационные системы», является известной как в России, так и за рубежом организацией в области разработки и создания систем защиты информации, составляющей государственную тайну, а также защиты конфиденциальной информации, кроме того, широко известны достижения ее специалистов в области разработки программно-аппаратных VPN-решений и средств криптографической защиты информации (соответствующей тематике диссертации).

Диссертационный совет отмечает, что на основании выполненных соискателем исследований:

разработана новая научная идея по выявлению аномалий в сетевом трафике и классификации КА, построенная на оценке свойства самоподобия в сетевом трафике, обнаружении в аномалиях КА в реальном или близком к реальному масштабе времени, их классификации и принятии мероприятий по защите с применением ячеек рекуррентной нейронной сети с долгой краткосрочной памятью (LSTM) и управляемого рекуррентного блока (GRU).

предложены: аналитическая модель выявления аномалий в сетевом трафике СПД в условиях КА, которая описывает не только стационарный, но и нестационарный сетевой трафик и обосновывает выбор фрактального метода выявления аномалий в интересах дальнейшей классификации КА в зависимости от типа трафика;

методика раннего обнаружения аномалий в сетевом трафике СПД, которая позволяет проводить прогнозирование и обнаружение не только известных, но и неизвестных КА на раннем этапе их проявления благодаря совместному применению методов фрактального анализа и LSTM, в результате чего существенно сокращается время выявления аномалий и уменьшается количество ложных срабатываний;

методика классификации КА в сетевом трафике СПД, в которой обнаружение КА производится с использованием генеративно-состязательной сети, производящая дообучение классификатора на скрытых латентных представлениях, полученных автокодировщиком, исходя из анализа данных о функционировании СПД;

архитектура и программные прототипы компонентов системы раннего обнаружения и классификации КА в СПД, которые ориентированы на раннее обнаружение как известных, так и неизвестных КА с минимальным количеством ложных срабатываний за счет реализации методов фрактального анализа и искусственной нейронной сети LSTM-типа.

доказана перспективность использования предложенных методик, основанных на интеграции методов фрактального анализа и методов машинного обучения.

введены:

- новые показатели оценки защищенности сетевого трафика СПД, основанные на показателе Херста;
- требования к работе систем обнаружения и предотвращения вторжений, обеспечивающих информационную безопасность;

Теоретическая значимость исследования обоснована тем, что:

доказаны сформулированные в работе теоретические утверждения с совместным использованием основных положений теории фракталов, построенной на методах оценки самоподобия, таких как тест Дики-Фуллера, R/S анализ и метод DFA, а также гибридной нейронной сети позволяет увеличить вероятность обнаружения КА;

применительно к проблематике диссертации результативно (эффективно, то есть с получением обладающих новизной результатов) использован фрактальный анализ, методы машинного обучения, теория и практика систем связи, теория и практика проведения тестирования на проникновение, аналитико-статистические методы, теория информационной безопасности;

изложены методологические и методические основы оценки самоподобия параметров функционирования СПД с использованием фрактальных показателей и прогнозирования факта воздействия КА путем применения обоснованной структуры LSTM для построения алгоритмов работы и архитектуры системы раннего обнаружения и классификации компьютерных атак в сетевом трафике сети передачи данных;

раскрыты

проблемные аспекты применения имеющихся подходов в области обнаружения известных и неизвестных КА, основанных на сигнатурных методах, статистических методах и методах машинного обучения;

противоречие между возросшими деструктивными возможностями новых видов КА на СПД, приводящих к аномальной активности трафика, и устаревшими подходами к их выявлению в СПД;

изучены существующие методы построения моделей машинного обучения, алгоритмы оптимизации потоковой передачи данных между базой данных и серверными системами, теория сложности вычислений, архитектура вычислительных систем и систем передачи данных, принципы построения микросервисной архитектуры, системы управления конфигурацией сети, а также программные компоненты, предназначенные для сбора логов, метрик и трассировки пакетов;

проведена модернизация существующих методов выявления аномалий, классификации компьютерных атак в сетях передачи данных и выработке мер противодействия им.

Значение полученных соискателем результатов исследования для практики подтверждается тем, что:

разработаны и внедрены следующие результаты диссертационной работы:

- аналитическая модель выявления аномалий в сетевом трафике СПД в условиях КА, в отличие от известных, описывает не только стационарный, но и нестационарный сетевой трафик и обосновывает выбор фрактального метода выявления аномалий в интересах дальнейшей классификации КА в зависимости от типа трафика;

• методика раннего обнаружения аномалий в сетевом трафике СПД, в отличие от известных, способна проводить прогнозирование и обнаружение не только известных, но и неизвестных КА 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;

внедрены в научно-исследовательские работы «Корвет», «Потенциал-2018», «Свертка-СМ», проводимые в ФГКВОУ ВО «Военная орденов Жукова и Ленина Краснознаменная академия связи им. С.М. Буденного»);

• методика классификации КА в сетевом трафике СПД отличается от известных тем, что в ней обнаружение КА производится с использованием генеративно-состязательной сети, которая производит дообучение классификатора на скрытых латентных представлениях, полученных автокодировщиком, исходя из анализа данных о функционировании СПД;

• архитектура и программные прототипы компонентов системы раннего обнаружения и классификации КА в СПД отличаются от известных тем, что они ориентированы на раннее обнаружение как известных, так и неизвестных КА с минимальным количеством ложных срабатываний за счет реализации методов фрактального анализа и искусственной нейронной сети LSTM-типа;

реализованы в опытно-конструкторской работе «Опорник», разрабатываемой ПАО «Информационные и телекоммуникационные технологии».

определены возможности и перспективы практического использования полученных результатов диссертации при использовании в существующих системах глубокого анализа сетевого трафика и системах обнаружения КА;

создана система программных прототипов компонентов раннего обнаружения и классификации КА, ориентированная на раннее обнаружение как известных, так и неизвестных КА с минимальным количеством ложных срабатываний за счет реализации методов фрактального анализа и искусственной нейронной сети LSTM-типа.

представлены предложения и направления для интеграции предлагаемой системы с другими известными системами защиты и имеющимися в арсенале систем компьютерной безопасности методами детектирования атак.

Оценка достоверности результатов исследования выявила:

для экспериментальных работ достоверность полученных результатов подтверждена проведением всестороннего анализа работ по исследуемой проблеме, корректным применением научно-методического аппарата в виде использованных методов и теорий, апробацией основных результатов диссертации в печатных трудах и докладах на международных и всероссийских конференциях, положительными итогами практической реализации результатов работы;

теория построена на известных принципах, проверенных данных и фактах с использованием современных известных и апробированных методов исследования, согласуется с опубликованными частными результатами других исследователей;

идея базируется на анализе работ отечественных и зарубежных исследователей в области выявления аномалий и классификации КА;

использованы полученные характеристики для сравнения с данными, приведенными в современной научной литературе по защитным преобразованиям информации (сравнение авторских данных и данных, полученных ранее по рассматриваемой тематике);

установлено качественное и количественное соответствие результатов решения задачи разработки методов и алгоритмов защиты информации в процессе её сбора, хранения, обработки, передачи и распространения. При этом подтверждено преимущество предложенного подхода перед результатами, полученными другими авторами.

использованы современные методики сбора и обработки исходной информации, методы построения архитектуры корпоративной сети на основе элементов СПД, способы проведение анализа защищенности и методология тестирования на проникновение.

Личный вклад соискателя состоит в:

- сравнительном анализе методов машинного обучения предназначенных для обнаружения аномальных всплесков и выбросов;

- сравнительный анализ методов машинного обучения распространенных классификаторов, определение ошибок 1-го и 2-го рода;
- разработке аналитической модели, определяющей свойство временного ряда, на основе которого выбирается метод по обнаружению аномалий в сетевом трафике СПД;
- разработке модели нейронной сети, базирующейся на архитектуре автокодировщика, состоящий из ячеек LSTM с долгой краткосрочной памятью;
- разработке архитектуры гибридной нейронной сети, состоящей из классификатора и автокодировщика;
- разработке киберполигона, который состоит из микросервисной архитектуры, базирующейся на платформе kubernetes и позволяющий формировать датасет с реальным сетевым трафиком в условиях приближенных к реальным;
- формирование и разметка данных, полученных с помощью киберполигона;
- проведении таргетированных компьютерных атак на СПД;
- реализации программных прототипов компонентов системы раннего обнаружения аномалий и классификации компьютерных атак на основе математического аппарата разработанных модели и методик;
- разработке web-приложения, позволяющего перехватывать и проводить анализ http-запросов до того, как они попадут на сервер.
- разработке способа передачи скрытых латентных представлений, полученных на глубоком слое автокодировщика в модель классификатора;
- подготовке основных публикаций по выполненной работе.

В ходе защиты диссертации были высказаны следующие критические замечания:

стоило явно указать в работе, что понимается под «реальным временем» и «ранним обнаружением» - терминами, которые фигурируют, в том числе, и в научной новизне;

при описании архитектуры и программного компонента системы раннего обнаружения и классификации КА в сетевом трафике СПД не раскрыто, какие образом реализована нейтрализации;

в работе недостаточно описаны тестовые данные – что они из себя представляют количественно и качественно, источники данных, способы их обработки и нормализации. Также, слабо описаны план и детали экспериментов, а иногда эта информация и вовсе отсутствует.

Соискатель Крибель А.М. ответил на задаваемые ему в ходе заседания вопросы и привел собственную аргументацию:

под «ранним обнаружением» понимается обнаружение аномалий при первом их проявлении. Под «реальным временем» понимается время реагирования в данный момент;

на данном этапе реализована блокировка адреса отправителя и оповещение специалиста по ИБ;

база данных формировалась с помощью разработанного киберполигона, в котором сетевой трафик перенаправлялся на DPI – Security Onion и записывался в файлы с расширением .pcap. КА проводились с помощью дистрибутива Kali Linux на заведомо уязвимые сервисы и web-приложения. Разметка КА производилась с помощью программ Netsniff-ng и IDE Bro. Объем выборки 40 Гб. Основными характеристиками трафика являлись: время жизни пакета, скорость передачи пакета, количество подключений к серверу, отброшенные пакеты, повторно переданные пакеты.

Нормализация данных производилась либо удалением среднего и масштабированием дисперсии (при этом не учитывалась форма распределения). В случае http трафика использовалась токенезация с добавлением спец символов в начало и конец каждой последовательности для более равномерного распределения.

На заседании 18.05.2023 г. диссертационный совет принял решение за решение научной задачи, заключающейся в разработке аналитической модели и методик выявления аномалий и классификации компьютерных атак в сетевом трафике сети передачи данных на основе применения фрактального анализа и методов машинного обучения, имеющей значение для развития области информационной безопасности, присудить Крибелю А.М. ученую степень кандидата технических наук.

При проведении тайного голосования[1] диссертационный совет в количестве 18 человек, из них 5 докторов наук по специальности рассматриваемой диссертации, участвовавших в заседании, из 25 человек, входящих в состав совета, проголосовали: за 16, против 2.

Заместитель председателя диссертационного совета
доктор технических наук,
профессор РАН Ронжин Андрей Леонидович

Ученый секретарь диссертационного совета
кандидат технических наук Абрамов Максим Викторович
18.05.2023 г.

[1] Заседание диссертационного совета проводилось в удаленном интерактивном режиме.