ОТЗЫВ

официального оппонента доктора технических наук, профессора

Заслуженного изобретателя Российской Федерации

Гречишникова Евгения Владимировича

на диссертационную работу

КРИБЕЛЯ Александра Михайловича, выполненную на тему:

«Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

Актуальность темы диссертации. В соответствии с перечнем приоритетных проблем научных исследований в области обеспечения информационной безопасности Российской Федерации в качестве наиболее актуальных направлений является решение вопросов защиты информационной инфраструктуры РФ, в условиях ее вхождения в глобальные сети связи, а также выявление признаков функционирования программных средств реализации скрытого информационного воздействия в действующих информационно-телекоммуникационных системах.

При этом в качестве основных внешних угроз, представляющих наибольшую опасность для критически важных объектов в рамках обеспечения информационной безопасности Российской Федерации рассматриваются все типы компьютерных атак (КА) со стороны злоумышленников. Очевидно, что в условиях усиления глобального информационного противоборства, а также непрерывного развития системы КА, приоритетными направлениями совершенствования системы обеспечения информационной безопасности становятся: систематическое выявление КА и их источников, структуризация целей обеспечения информационной безопасности и определение соответствующих практических задач; разработка современных методов и средств защиты информации, обеспечения безопасности используемых информационных технологий; развитие сетей связи и систем управления этими сетями.

Необходимость решения перечисленных задач предопределяет актуальность представленной работы.

Новизна, теоретическая и практическая значимость полученных научных результатов. В ходе решения сформулированной в работе актуальной научной задачи, направленной на разработку аналитической модели и методик выявления аномалий и

классификация КА в сетевом трафике сети передачи данных (СПД) на основе применения фрактального анализа и методов машинного обучения, автором получены следующие новые научные результаты:

1. Аналитическая модель выявления аномалий в сетевом трафике СПД в условиях КА.

2. Методика раннего обнаружения аномалий в сетевом трафике СПД.

3. Методика классификации КА в сетевом трафике СПД.

4. Архитектура и программные компоненты системы раннего обнаружения и классификации КА в сетевом трафике СПД.

Научная новизна результатов исследования заключается в том, что:

в отличие от известных, разработанная аналитическая модель выявления аномалий в сетевом трафике СПД в условиях КА, одновременно описывает стационарный и нестационарный сетевой трафик, а также проводит обоснованный выбор фрактального метода выявления аномалий в интересах дальнейшей классификации КА в зависимости от типа трафика;

предложенная автором методика раннего обнаружения аномалий в сетевом трафике СПД, в отличие от известных, способна проводить прогнозирование и обнаружение известных и неизвестных КА на раннем этапе их проявления за счет совместного применения методов фрактального анализа и искусственной нейронной сети LSTM-типа (рекуррентные нейронные сети с долгой краткосрочной памятью), в результате чего сокращается время выявления аномалий и уменьшается количество ложных срабатываний;

разработанная 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;

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

Степень обоснованности и достоверности научных положений, выводов и рекомендаций, сформулированных в диссертации. Исходя из анализа каждого научного результата, следует сделать вывод, что научные положения, выводы и рекомендации, сформулированные в работе, достаточно обоснованы, обладают новизной и

достоверностью. Обоснованность полученных научных результатов подтверждается корректным применением положений теории вероятностей; фрактального анализа; методов машинного обучения; теории и практики систем связи; теории и практики проведения тестирования на проникновение; аналитико-статистических методов.

Достоверность полученных научных результатов обеспечивается полнотой и обстоятельностью проведенного автором анализа научных работ в предметной области, современных условий функционирования СПД, а также состояния КА злоумышленников, корректным применением апробированных математических положений, системностью исследуемых вопросов, корректностью постановки задач, формулировок, обоснованным введением ограничений и допущений, непротиворечивостью полученных результатов результатам предшествующих исследований в предметной области.

Публикации, реализация и апробация научных положений. По итогам проведенного исследования Крибелем А.М. опубликованы:

шесть статей, индексируемые в международных базах данных Web of Science и/или Scopus;

десять статей в рецензируемых научных изданиях, входящих в перечень, установленный Министерством науки и высшего образования Российской Федерации;

одно свидетельство о государственной регистрации программы для ЭВМ.

Основные научные и практические результаты работы докладывались и обсуждались на следующих 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).

Оценка содержания диссертации, степень ее завершенности. Работа написана технически грамотным языком, хорошо оформлена, стиль изложения доказательный, обладает внутренним единством, содержит новые научные результаты и положения, свидетельствующие о личном вкладе соискателя в науку. Ссылки на авторов и источники заимствования материалов приведены корректно.

Содержание работы соответствует паспорту специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Автореферат кратко и в достаточной мере отражает содержание диссертации, включает перечень основных научных работ автора, связанных с темой исследования.

Однако в работе следует отметить следующие недостатки.

Оценки качества разработанных соискателем математической модели выявления аномалий в сетевом трафике СПД в условиях КА; методики раннего обнаружения аномалий в сетевом трафике СПД и методики классификации КА в сетевом трафике СПД в работе представлены не полностью.

В выводах по четвертому разделу, в пункте 3 соискатель приводит в качестве достигаемого результата вероятность обнаружения ранее неизвестных атак 0,99. Однако, подробных материалов, поясняющих, как был достигнут такой эффект в работе в полной мере не представлено.

В заключении соискатель заявляет, что совокупное применение разработанных модели и методик по сравнению с другими подходами позволяет увеличить скорость обнаружения КА в 14 раз. Однако в тексте пояснительной записке доказательств получения такого эффекта не представлено.

Отмеченные недостатки носят частный характер и не ставят под сомнение достоверность, новизну, обоснованность и полезность основных научных положений и выводов и является самостоятельным направлением исследования.

Заключение. Представленная диссертационная работа написана на актуальную тему и является завершенным научно-квалификационным трудом. В ней получено новое решение актуальной научной задачи, заключающейся 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, что несомненно имеет значение для развития технической отрасли знаний.

По научной новизне, теоретической и практической значимости, обоснованности и достоверности полученных результатов диссертационная работа удовлетворяет требованиям ВАК, соответствует критериям, установленным пп. 9, 10, 11, 13 и 14 «Положения о присуждении ученых степеней», а её автор Крибель Александр Михайлович заслуживает присуждение ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент:

Доктор технических наук, профессор, Заслуженный изобретатель Российской Федерации, директор по научно-техническому развитию
АО «НИИ «Рубин» (г. Санкт-Петербург)

Гречишников Евгений Владимирович

«24» апреля 2023 г.

194100, Россия, Санкт-Петербург,
Кантемировская ул., 5
Тел.: +7 (812) 670-89-72
e-mail: E.V.Grechishnikov@rubin-spb.ru

Подпись Гречишникова Е.В. заверяю
Генеральный директор АО «НИИ «Рубин»
С. Степанов

«24» апреля 2023 г.