МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет телекоммуникаций и информатики»
(ПГУТИ)

Юридический адрес:
Льва Толстого ул., д.23, г. Самара, 443010
Почтовый адрес:
Московское шоссе, д. 77, г. Самара, 443090
тел. (846) 333 58 56
E-mail: info@psuti.ru, www.psuti.ru
ОКПО 01179900; ОГРН 1026301421992
ИНН/КПП 6317017702/631701001

14.11.2025 № 2803/02-01-01

УТВЕРЖДАЮ
Проректор по научной работе федерального государственного бюджетного образовательного учреждения высшего образования "Поволжский государственный университет телекоммуникаций и информатики", д.т.н., профессор

_____ Горбачев Олег Валериевич

14.11. 2025 г.

ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

федерального государственного бюджетного образовательного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики» на диссертацию Рыбакова Сергея Юрьевича «Обнаружение и классификация компьютерных атак методами мультифрактального анализа и машинного обучения», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность.

Актуальность темы диссертационного исследования

Диссертационная работа Рыбакова С.Ю. направлена на решение **важной научно-технической проблемы**, связанной с обеспечением информационной безопасности в условиях стремительного роста сложности и разнообразия компьютерных атак в современных сетях, включая IoT-сегменты. Существующие методы обнаружения и классификации атак зачастую критически зависят от полноты разметки данных, не обладают достаточной устойчивостью к

нестационарности сетевого трафика и испытывают трудности с идентификацией момента начала атаки. В этой связи разработка методов, способных надежно фиксировать малые и кратковременные аномалии в поведении трафика в реальном времени, представляется чрезвычайно востребованной.

Перспективность выбранного научного направления подтверждается тем, что совместное использование мультифрактального анализа и машинного обучения позволяет выявить глубинные закономерности в сетевом трафике, обладающем свойствами самоподобия, и зафиксировать искажения его фрактальных свойств, вызванные атаками. Учет динамики изменения фрактальных характеристик на различных временных масштабах открывает новые возможности для повышения чувствительности и достоверности систем обнаружения вторжений.

Таким образом, тема диссертационного исследования Рыбакова Сергея Юрьевича является **актуальной** и соответствует приоритетным направлениям развития науки и технологий в области информационной безопасности.

Структура и содержание диссертационной работы

Диссертация представляет собой законченное научное исследование, отличающееся целостностью и логичностью построения. Работа состоит из введения, четырех глав, заключения, списка использованных источников из 125 наименований и шести приложений. Основное содержание изложено на 122 страницах, содержит 39 рисунков и 19 таблиц. Структура работы обеспечивает последовательное раскрытие темы, логическую взаимосвязь разделов и полное обоснование выносимых на защиту научных положений.

Новизна исследований и полученных результатов

Целью диссертационной работы является повышение качества классификации компьютерных атак в компьютерных сетях с помощью комбинации мультифрактального анализа и машинного обучения.

Для достижения поставленной цели автор решает следующие задачи: разработку улучшенной модели оценки фрактальных свойств компьютерных атак в онлайн-режиме методами вейвлет-анализа; разработку метода повышения эффективности алгоритмов обнаружения/классификации атак в компьютерных

сетях методами машинного обучения при условии дополнительной информации о фрактальных свойствах атак и сетевого трафика; разработку модели алгоритмической и численной оценки мультифрактальных свойств сетевого трафика и компьютерных атак; разработку метода композиции машинного обучения и мультифрактального анализа сетевого трафика для улучшения многоклассовой классификации компьютерных атак.

В диссертации получены следующие результаты, которые могут быть квалифицированы как новые:

– Разработана и программно реализована модифицированная модель оценки фрактальной размерности на основе вейвлет-анализа с дополнительной фильтрацией детализирующих коэффициентов, позволяющая повысить точность оценки в скользящем окне на 15–40% в зависимости от типа вейвлета и обеспечить прирост достоверности обнаружения атак в онлайн-режиме.

– Предложен метод обнаружения и классификации компьютерных атак, основанный на учете статистических характеристик фрактальной размерности сетевого трафика и атак, который позволил повысить достоверность и точность классификации в среднем на 10%, а также сократить время обучения и тестирования алгоритмов машинного обучения.

– Введено понятие и разработана модель мультифрактального спектра фрактальной размерности (МСФР), формализующая новые информативные признаки для многоклассовой классификации атак. Показана изменчивость фрактальной размерности на различных интервалах дискретизации и получены статистики параметров МСФР для нормального трафика и различных типов атак.

– Разработан метод композиции методов машинного обучения и мультифрактального анализа, обеспечивающий повышение точности многоклассовой классификации атак на 7–10% на реальных наборах данных. Для ряда классов атак, таких как Mirai, достигнуты показатели AUC OVR, близкие к единице, что демонстрирует высокую эффективность предложенных решений.

Анализ обоснованности и достоверности научных положений сформулированных в диссертации

Обоснованность первого положения подтверждается строгим математическим выводом модифицированной модели оценки фрактальной размерности, корректным применением аппарата вейвлет-анализа и статистической оценкой, показавшей снижение дисперсии оценок и прирост достоверности обнаружения атак на 15–40% в онлайн-режиме. Результаты верифицированы на известных базах данных.

Обоснованность второго положения подтверждается сравнительными экспериментами с широким классом алгоритмов машинного обучения, продемонстрировавшими прирост точности классификации в среднем на 10% и сокращение времени обучения/тестирования.

Обоснованность третьего положения подтверждается введением модели мультифрактального спектра фрактальной размерности, выявлением изменчивости фрактальной размерности на различных масштабах времени и получением статистик параметров МСФР для различных типов трафика и атак. Положение апробировано на профильных научных конференциях.

Обоснованность четвертого положения подтверждается экспериментальным приростом точности многоклассовой классификации на 7–10% относительно базовых постановок без фрактальных признаков на реальных и общепринятых наборах данных при адекватности используемых моделей.

В целом, все положения имеют строгую математическую и экспериментальную поддержку, выводы и рекомендации соответствуют целям и задачам исследования.

Теоретическая и практическая значимость работы

Теоретическая значимость работы заключается в развитии математического аппарата мультифрактального анализа применительно к задачам обнаружения и классификации компьютерных атак. Разработанные модели и методы вносят вклад в теорию обработки нестационарных сигналов и машинного обучения в контексте информационной безопасности.

Практическая значимость результатов диссертации состоит в том, что разработанные алгоритмы и их программные реализации позволяют повысить точность и достоверность обнаружения и классификации компьютерных атак в сетевом трафике, включая сегменты интернета вещей, при нестационарности и априорной неопределённости. Сформулированные рекомендации и определенные параметры обеспечивают эффективную работу предложенных решений на коротких окнах наблюдения, что особенно актуально для сегментов Интернета вещей.

Результаты работы внедрены в проектную деятельность ФГУП «Научно-исследовательский институт «Квант» при проектировании и создании автоматизированных систем в защищенном исполнении и используются в учебном процессе МТУСИ, что подтверждено соответствующими актами внедрения.

Достоверность научных положений, представленных в диссертации, подтверждается следующими фактами:

– корректным использованием современного математического аппарата;

– репрезентативностью проведенного экспериментального исследования на известных общедоступных наборах данных;

– сравнительным анализом с широким классом алгоритмов машинного обучения и стандартными метриками оценки качества.

Все основные результаты, полученные в диссертации, опубликованы в 16 научных печатных работах, в том числе: 9 - в научных изданиях перечня ВАК РФ; 2 - в научных рецензируемых изданиях по базе Scopus; 4 – в материалах конференций и других изданиях. Получено свидетельство о Государственной регистрации программы для ЭВМ. Среди опубликованных работ 2 из них написаны лично диссертантом, а также одна статья, написанная в соавторстве. Публикационная активность и апробация свидетельствуют о качественном обсуждении и признании результатов научным сообществом.

Содержание диссертации и автореферата в полной мере отвечает паспорту специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Оформление диссертации соответствует ГОСТ Р 7.0.11–2011 «Диссертация и автореферат диссертации. Структура и правила оформления», М.: Стандартинформ, 2012.

Автореферат диссертации выполнен с соблюдением установленных требований, точно отражает ее содержание, полученные в ней практические и теоретические результаты и выводы.

Рекомендации по использованию результатов и выводов диссертации

Результаты представленной работы рекомендуется к использованию в организациях, обеспечивающих информационную безопасность информационных систем, для предупреждения, обнаружения и классификации компьютерных атак в сетевом трафике, в том числе в условиях нестационарности и априорной неопределенности.

Результаты работы позволяют повысить достоверность обнаружения компьютерных атак в компьютерных сетях за счет композиции положений машинного обучения и характеристик мультифрактального спектра фрактальной размерности сетевого трафика и компьютерных атак и могут применяться в системах обнаружения вторжений, для фильтрации и блокирования вредоносного и нежелательного трафика, а также для обучения и тестирования классификаторов при внедрении решений в центрах мониторинга безопасности.

Соответствие диссертационной работы паспорту специальности

Содержание диссертационной работы полностью соответствует специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность» (технические науки). Научные результаты диссертации соответствуют следующим пунктам паспорта специальности:

п.6. Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях.

п.15. Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

Замечания по диссертационной работе

Замечание 1. В диссертации показана эффективность фрактальных признаков для обнаружения атак, изменяющих объем трафика. Однако требует пояснения, насколько предлагаемый метод чувствителен к низкоинтенсивным атакам, которые не приводят к существенному изменению общего объема переданных данных, но меняют его временную структуру.

Замечание 2. Требуется пояснить, является ли основным фактором повышения точности классификации способность мультифрактального анализа выявлять новые закономерности или же эффект связан с увеличением количества признаков.

Замечание 3. Констатация отсутствия свойства самоподобия при отсутствии компьютерных атак в трафике IoT требует дополнительного пояснения, поскольку она вступает в некоторое противоречие с устоявшимися представлениями о фрактальной природе сетевого трафика, сформированными на основе исследований агрегированных потоков в классических компьютерных сетях.

Замечание 4. В работе недостаточно четко описана модель угроз. Присутствуют отсылки к ряду атак, однако нет детального рассмотрения и классификации данных атак, а также не раскрыты показатели, по которым данные атаки фиксируются системой.

Выявленные недостатки не влияют на общую положительную оценку научных результатов выполненного соискателем диссертационного исследования.

Заключение

Диссертационная работа Рыбакова Сергея Юрьевича «Обнаружение и классификация компьютерных атак методами мультифрактального анализа и машинного обучения» по актуальности, научной новизне, теоретической и практической значимости соответствует всем требованиям ВАК Минобрнауки России предъявляемым к диссертациям на соискание ученой степени кандидата наук. Работа соответствует требованиям пунктов 9–14 «Положения о присуждении ученых степеней», утвержденным постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г. (с изменениями и дополнениями), поскольку является завершенной научно-квалификационной работой, в которой

изложены научно обоснованные модели, методы, алгоритмы и программные решения для мониторинга сетевого трафика и повышения достоверности обнаружения и точности классификации компьютерных атак, а ее автор, Рыбаков Сергей Юрьевич заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность (технические науки).

Диссертационная работа Рыбакова Сергея Юрьевича обсуждена на расширенном заседании кафедры информационной безопасности федерального государственного бюджетного образовательного учреждения высшего образования «Поволжский государственный университет телекоммуникаций и информатики» 29 октября 2025 года, протокол № 3.

Зав. кафедрой «Информационная безопасность»

д.т.н., доцент Шакурский Максим Викторович

Профессор кафедры «Программная инженерия»

д.т.н., доцент Карташевский Игорь Вячеславович

01.11 2025

Сведения о составителях отзыва:
Шакурский Максим Викторович, д.т.н., доцент, заведующий кафедрой «Информационная безопасност». Докторская диссертация защищена в 2022 году по специальности 2.3.6 - Методы и системы защиты информации, информационная безопасность. Ученое звание доцента получено в 2019 году по специальности «Теоретическая электротехника».

Карташевский Игорь Вячеславович, д.т.н., доцент, профессор кафедры «Программная инженерия», заведующий научно-исследовательской лабораторией специальности 05.12.13 – Системы, сети и устройства телекоммуникаций, ученое звание доцента присвоено в 2024 году по специальности «Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей».

Федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет телекоммуникаций и информатики»
443010, г. Самара, ул. Льва Толстого, д. 23