ОТЗЫВ

на автореферат диссертации Рыбакова Сергея Юрьевича «Обнаружение и классификация компьютерных атак методами мультифрактального анализа и машинного обучения», представленной на соискание учёной степени кандидата технических наук по специальности 2.3.6.«Методы и системы защиты информации, информационная безопасность (технические науки)».

Актуальность темы. Задача обнаружения и классификации компьютерных атак напрямую связана с обеспечением национальной безопасности, экономической стабильности и неприкосновенности личной информации. Компьютерные атаки активно используют маскировку и обфускацию, чтобы оставаться незамеченными для систем безопасности, имитируя легитимный сетевой трафик или поведение пользователей. Причём автоматизированные инструменты позволяют проводить атаки с беспрецедентной скоростью, что требует систем обнаружения, способных реагировать в режиме реального времени.

Сетевой трафик, даже в нормальном состоянии, часто обладает сложной, нелинейной, самоподобной структурой, которую невозможно описать простыми линейными моделями. Мультифрактальный анализ позволяет исследовать эти тонкие, изменяющиеся во времени зависимости на разных масштабах. Мультифрактальный анализ предоставляет уникальные, глубокие характеристики сетевого трафика, которые отражают нелинейные свойства. Машинное обучение, в свою очередь, эффективно использует эти признаки для построения устойчивых и надёжных моделей классификации, способных различать нормальное поведение от различных типов атак.

Таким образом, исследование, направленное на обнаружение и классификацию компьютерных атак методами мультифрактального анализа и машинного обучения, является актуальным. Оно предлагает инновационный и мощный подход к решению одной из наиболее острых проблем существенного повышения эффективности систем кибербезопасности и обеспечения надёжной защиты в условиях постоянно усложняющихся киберугроз.

Научная новизна диссертационных исследований. К сильным сторонам диссертации можно отнести:

– модель оценки фрактальной размерности, отличающаяся от известных дополнительной фильтрацией детализирующих коэффициентов вейвлет разложения;

– метод обнаружения и классификации компьютерных атак, который повышает достоверность и точность обнаружения компьютерных атак за счёт введения дополнительной информации о статистических характеристиках фрактальной размерности (ФР) сетевого трафика и компьютерных атак;

– новая модель оценки характеристик мультифрактального спектра фрактальной размерности (МСФР) трафика и компьютерных атак с помощью

последовательности текущих оценок ФР в окне фиксированной длины, варьируемой в зависимости от интервала разрешения (времени дискретизации), что позволяет формализовать новые полезные признаки классификации;

– новый метод композиции машинного обучения и мультифрактального анализа сетевого трафика, который позволяет повысить точность многоклассовой классификации компьютерных атак за счет добавления новых атрибутов.

Прикладная ценность диссертационной работы. Предложенная модель оценки фрактальной размерности повышает точность на 15…40% в зависимости от используемого типа материнского вейвлета. Предложенный метод обнаружения и классификации компьютерных атак повышает достоверность и точность обнаружения компьютерных атак в среднем на 10%. Новая модель оценки характеристик мультифрактального спектра фрактальной размерности трафика и компьютерных атак с помощью последовательности текущих оценок ФР в окне фиксированной длины, варьируемой в зависимости от времени дискретизации позволяет формализовать новые полезные признаки классификации. Новый метод композиции машинного обучения и мультифрактального анализа сетевого трафика позволяет повысить точность многоклассовой классификации компьютерных атак в среднем на 7-10%.

Практическая значимость диссертационной работы подтверждена актом внедрения разработанного программного обеспечения в проектную деятельность ФГУП «НИИ «Квант».

Формальная сторона вопроса. Результаты диссертационной работы отражены в 16 работах, в том числе в 9-ти научных изданиях перечня ВАК (в 2-х из них без соавторов); в 2-х научных рецензируемых изданиях по базе Scopus и в 4-х материалах конференций и других изданиях (в 1-м из них без соавторов). Получено свидетельство о Государственной регистрации программы для ЭВМ.

Анализ информации, представленной в автореферате, позволяет сформулировать следующие два замечания.

Замечание 1. Порог обнаружения выбирается на этапе обучения. Не совсем понятно, насколько порог обнаружения устойчив к сезонным или суточным изменениям в статистических характеристиках нормального трафика реальной сети?

Замечание 2. Диссертант утверждает, что фрактальные признаки дополняют существующие 115 признаков в базе данных Kitsune. В связи с этим возникает вопрос о принципиальной возможности построения эффективной системы обнаружения атак, основанной исключительно на фрактальных характеристиках, без привлечения традиционных признаков.

Однако отмеченные недостатки не снижают общей положительной оценки работы. Результаты работы достаточно полно отражены в публикациях автора. Работа апробирована на конференциях. В диссертации соискатель

грамотно выбрал направление исследования, вытекающего из цели и задач диссертации.

Заключение. Диссертационная работа «Обнаружение и классификация компьютерных атак методами мультифрактального анализа и машинного обучения» представляет научное исследование, удовлетворяющее квалификационным требованиям «Положения о присуждении учёных степеней, предъявляемым к кандидатским диссертациям. Автор диссертации, Рыбаков Сергей Юрьевич, заслуживает присуждения учёной степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность (технические науки)».

Зав. кафедрой «Информационная безопасность телекоммуникационных систем» института компьютерных технологий и информационной безопасности инженерно-технологической академии Южного федерального университета, Заслуженный работник высшей школы РФ, доктор технических наук (05.12.20 «Оптические системы локации, связи и обработки информации»), профессор

Почтовый адрес. 347928, Россия, г. Таганрог, Ростовская область, ГСП-17А, ул. Чехова, 2, ЮФУ. Тел.: 8-928-182-72-09. E-mail: rumyancev@sfedu.ru

Константин Евгеньевич Румянцев
10 ноября 2025 года

Я, Румянцев Константин Евгеньевич, даю согласие на обработку своих персональных данных, необходимых для процедуры защиты диссертации Рыбакова Сергея Юрьевича, включая размещение в сети Интернет на сайте ФГБОУ ВО «Санкт-Петербургский государственный университет промышленных технологий и дизайна» и в Федеральной информационной системе государственной научной аттестации (ФИСГНА)

Константин Евгеньевич Румянцев
10 ноября 2025 года

Подпись профессора К. Е. Румянцева заверяю.
Директор института компьютерных технологий
и информационной безопасности
инженерно-технологической академии
Южного федерального университета,
доктор технических наук, доцент

Геннадий Евгеньевич Веселов
10 ноября 2025 года