В диссертационный совет 24.2.385.09 при федеральном государственном бюджетном образовательном учреждении высшего образования «Санкт-Петербургский государственный университет промышленных технологий и дизайна»

ОТЗЫВ

официального оппонента, к.т.н., доцента Израилова Константина Евгеньевича 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 диссертационного исследования

Диссертационная работа Рыбакова С.Ю. посвящена одной из ключевых для современной информационной безопасности задач – повышению качества обнаружения и классификации компьютерных атак в компьютерных сетях, в том числе в сегментах Интернета вещей, за счёт совместного использования методов мультифрактального анализа сетевого трафика и алгоритмов машинного обучения. В связи с этим, актуальность темы не вызывает сомнений. Масштабное внедрение распределённых информационных систем, киберфизических комплексов и промышленного Интернета вещей сопровождается ростом количества уязвимостей и, как следствие, разнообразных по технике и интенсивности атак; при этом на первый план выходит не только своевременное обнаружение атаки, но и корректное определение ее класса и сценария развития. В существующих системах мониторинга проблема усиливается неопределенностью по виду и сигнатуре воздействия. Традиционные статистические методы и распространенные алгоритмы машинного обучения, опирающиеся на большое число малоинформативных признаков, демонстрируют заметную долю ложных срабатываний и ограниченную чувствительность к сложным атакам, меняющим глубинные (т.е. скрытые) свойства трафика. На этом фоне обращение диссертанта к (мульти)фрактальным характеристикам сетевого трафика как к источнику новых устойчивых атрибутов, отражающих структурные изменения при атаке, представляется обоснованным и перспективным, а сформулированная научная задача по разработке соответствующего научно-методического аппарата актуальной как для теории, так и для практики кибербезопасности.

Степень разработанности научной проблемы в диссертации проанализирована достаточно полно. Показано, что методам фрактального анализа в различных областях техники посвящено значительное число работ отечественных и зарубежных авторов, так же, как и методам обнаружения атак в компьютерных сетях средствами машинного обучения. При этом подчеркивается, что интегральная задача совместного использования (мульти)фрактального анализа с алгоритмами машинного обучения в целях повышения достоверности обнаружения и классификации атак до последнего времени оставалась недостаточно проработанной и требовала проведения дополнительных исследований, что и обусловило постановку цели и частных задач диссертации.

Структура и содержание диссертации и соответствие автореферата

Диссертация представляет собой завершенное научное исследование, обладающее четкой внутренней логикой и последовательностью изложения, состоит из введения, четырех глав, заключения, списка использованных источников и шести приложений.

Во введении обоснована актуальность темы, сформулированы цель и научная задача работы, определены объект и предмет исследования, приведены формулировки частных задач, сведения о методологической основе, апробации и внедрении результатов.

Первая глава содержит аналитический обзор современных методов обнаружения компьютерных атак, включая алгоритмы машинного обучения, а также подходы к (мульти)фрактальному анализу сетевого трафика. На основе критического анализа уточнены формулировки частных задач исследования.

Во второй главе разрабатывается и исследуется модифицированный алгоритм оценки фрактальной размерности на основе кратномасштабного анализа с использованием показателя Херста и процедур вторичной фильтрации (трешолдинга) детализирующих коэффициентов, ориентированный на работу в скользящем окне и фиксацию скачков фрактальных параметров в режиме, близком к реальному времени, в том числе для трафика интернета вещей.

Третья глава посвящена применению монофрактального анализа в задачах обнаружения и бинарной классификации атак – рассматривается влияние фрактальной размерности и ее статистических характеристик на качество классификации, показывается прирост информативности при включении этих атрибутов в модели машинного обучения.

В четвертой главе формализована модель мультифрактального спектра фрактальной размерности сетевого трафика и атак, построенная по последовательности оценок фрактальной размерности на различных временных масштабах, и предложен метод композиции мультифрактального анализа с алгоритмами машинного обучения для решения задач многоклассовой классификации в сетях Интернета вещей.

Выводы в **заключении** четко обоснованы и полностью характеризуют полученные в диссертации научные результаты.

Автореферат в целом корректно и без искажений отражает структуру и основные результаты работы, включая перечень положений, выносимых на защиту, сведения о теоретической и практической значимости, апробации и публикациях.

Научная новизна полученных результатов и их научная значимость

Научная новизна диссертации четко сформулирована и подтверждается совокупностью полученных результатов.

Автором разработана и программно реализована новая модель оценки фрактальных параметров компьютерных атак в режиме реального времени, использующая дополнительную фильтрацию коэффициентов вейвлет-разложения с помощью процедур трешолдинга. Показано, что такая модификация позволяет повысить точность оценки фрактальной размерности атак в скользящем окне на величину, достигающую 15–40% для различных типов материнских вейвлетов, и, как следствие, увеличить достоверность обнаружения атак.

Предложен метод обнаружения и классификации атак, в котором в качестве дополнительных атрибутов используются статистические характеристики фрактальной размерности – среднее значение, дисперсия, асимметрия и эксцесс плотности распределения; что в среднем обеспечивает прирост точности классификации порядка 10% относительно постановок, опирающихся только на традиционные признаки трафика.

Разработана модель оценки характеристик мультифрактального спектра фрактальной размерности трафика и атак в окне фиксированной длины, варьируемой в зависимости от интервала разрешения.

Синтезирован метод композиции мультифрактального анализа и машинного обучения, основанный на введении параметров мультифрактального спектра фрактальной размерности в качестве дополнительных признаков при многоклассовой классификации сетевого трафика и атак.

Все основные результаты, выносимые на защиту, в диссертации и автореферате прямо позиционируются как новые и ранее в таком виде в научной литературе не представлялись.

Степень обоснованности научных положений, выводов и рекомендаций, можно оценить как высокую. Теоретическая часть работы опирается на системный анализ, аппарат фрактального и вейвлет-анализа, теорию вероятностей, методы математической статистики, численного имитационного моделирования и машинного обучения, что позволяет строго вывести используемые в диссертации соотношения и алгоритмы. Для модифицированного алгоритма оценки фрактальной размерности последовательно анализируется влияние длины скользящего окна, глубины вейвлет-разложения, типа материнского вейвлета и параметров трешолдинга на точность оценивания и характеристики вероятности обнаружения атак.

Экспериментальные исследования проведены как на искусственно моделируемых последовательностях со скачкообразным изменением фрактальных свойств, так и на ряде общепринятых наборов данных для задач обнаружения атак, включая базы данных

для сетей общего назначения и сегментов Интернета вещей. Качество обнаружения и классификации оценивается по стандартным для кибербезопасности метрикам – точность, полнота, F1-мера, ROC-кривые и AUC, что позволяет объективно сравнивать эффективность предложенных решений с базовыми постановками.

Достоверность результатов исследования дополнительно подтверждается широкой апробацией результатов на международных и всероссийских научно-технических конференциях, а также, публикацией 16 научных работ, 12 из которых в изданиях из перечня рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук (Перечень ВАК), а также в приравниваемых к ним. Внедрение результатов в проектную деятельность ФГУП «НИИ «Квант» и учебный процесс МТУСИ в рамках дисциплин по искусственному интеллекту и обнаружению вторжений свидетельствует о практической проверке и надежности предложенных решений.

Теоретическая и практическая значимость диссертационного исследования

Теоретическая значимость работы состоит в развитии аппарата (мульти)фрактального анализа применительно к задачам обнаружения и классификации компьютерных атак в нестационарных сетевых средах. Предложенные модели оценки фрактальной размерности и мультифрактального спектра фрактальной размерности, а также метод композиции мультифрактального анализа и машинного обучения уточняют представления о статистических свойствах (мульти)фрактальных характеристик сетевого трафика при наличии и в отсутствии атак; при этом, указанные модели и методы предоставляют эксперту-разработчику средств защиты новый класс информативных признаков, непосредственно связанных с самоподобной и иерархической структурой трафика.

Практическая значимость результатов заключается в возможности их применения при мониторинге и обеспечении информационной безопасности компьютерных систем широкого профиля, включая киберфизические, промышленный Интернет вещей и другие сложные иерархические информационные системы, в том числе в условиях работы с короткими окнами наблюдения. 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 (использования).

Апробация результатов, публикации и личный вклад автора

Основные результаты диссертационной работы последовательно апробированы на ряде авторитетных международных и всероссийских конференциях, посвященных информационным технологиям и информационной безопасности.

По теме диссертации у автора имеется 16 научных работ, значительное количество которых (а, именно, 12) опубликовано в изданиях из Перечня ВАК (9 статей), в

журналах, входящих в международную систему цитирования (2 статьи) или является свидетельством о государственной регистрации программы для ЭВМ (1 результат интеллектуальной деятельности).

Согласно диссертации и автореферату, все основные научные результаты, касающиеся разработки методов, моделей, алгоритмов и их программной реализации, получены автором лично, а вклад соавторов ограничен постановкой отдельных задач и обсуждением результатов. Это находит отражение и в структуре публикаций, где Рыбаков С.Ю. выступает первым автором или ключевым соавтором работ, непосредственно связанных с тематикой диссертации. Степень самостоятельности проведенного исследования следует признать достаточной для кандидатской диссертации по специальности 2.3.6.

Соответствие диссертации паспорту специальности и требованиям ВАК

Диссертация соответствует двум пунктам паспорта специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность (технические науки)»:

– 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

1. В связи с тем, что предлагаемая концепция мультифрактального спектра фрактальной размерности опирается на рассмотрение трафика на различных временных масштабах, осталось неясным, существует ли некоторая нижняя граница временного масштаба, ниже которой применение мультифрактального анализа утрачивает практический смысл в контексте задач обнаружения и классификации кибератак.

2. В работе отмечается сокращение времени обучения моделей дерева решений и случайного леса при использовании расширенного признакового описания, включающего монофрактальные и мультифрактальные характеристики трафика. Однако целесообразно пояснить, в связи с чем произошло такое кратное сокращение времени на обучение и тестирование моделей.

3. Не указано, почему в качестве критерия качества оценки фрактальной размерности был выбран минимум среднего значения и дисперсии показателя Херста, а не другие статистические метрики.

4. В ряде фрагментов текста имеются незначительные стилистические и терминологические неоднородности (в обозначениях метрик, сокращениях, ссылках).

5. В контексте диссертационной работы целесообразно говорить не о компьютерных, а о сетевых атаках.

6. Ряд рисунков в тексте диссертации и автореферата имеет недостаточное качество.

Однако, указанные замечания не снижают качество диссертационной работы и не влияют на общую оценку ее научной новизны и практической значимости.

Заключение

В целом, 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 требованиям, предъявляемым ВАК Минобрнауки России к диссертациям на соискание ученой степени кандидата технических наук (пп. 9-14 «Положения о присуждении ученых степеней», утвержденным постановлением Правительства Российской Федерации № 842 от 24 сентября 2013 г. (с изменениями и дополнениями)). Диссертационная работа является завершенной научно-квалификационной работой, в которой изложены научно обоснованные технические решения, разработанные модели и методы повышения достоверности обнаружения и качества классификации компьютерных атак методами машинного обучения и мультифрактального анализа при проведении мониторинга сетевого трафика, имеющие существенное значение для развития страны.

С учетом изложенного считаю, что диссертация Рыбакова Сергея Юрьевича соответствует требованиям, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 2.3.6. «Методы и системы защиты информации, информационная безопасность», а ее автор заслуживает присуждения ученой степени кандидата технических наук по указанной специальности.

Официальный оппонент:

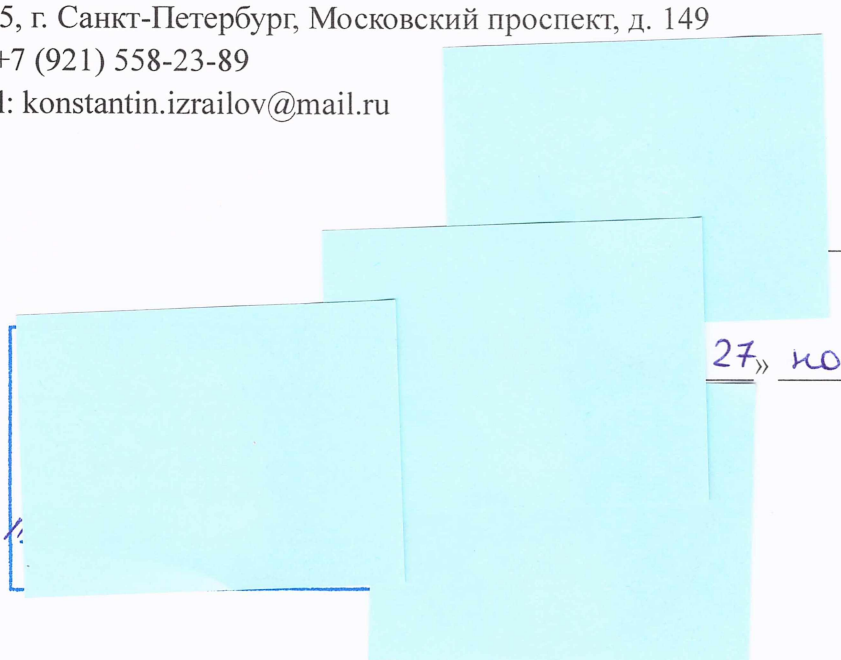
кандидат технических наук (специальность – 05.13.19 «Методы и системы защиты информации, информационная безопасность», доцент

профессор кафедры прикладной математики и безопасности информационных технологий Федерального государственного бюджетного образовательного учреждения высшего образования «Санкт-Петербургский университет Государственной противопожарной службы Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий имени Героя Российской Федерации генерала армии Е.Н. Зиничева»

196105, г. Санкт-Петербург, Московский проспект, д. 149

Тел.: +7 (921) 558-23-89

E-mail: konstantin.izrailov@mail.ru



___ Израилов К.Е.

«27» ноября 2025 г.