Экз. № 1

ОТЗЫВ

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

Массовое развитие информационных систем ведет к росту числа уязвимостей и компьютерных атак (КА), что повышает значимость не только их обнаружения, но и точной классификации.

Проблема усугубляется неопределенностью момента и сигнатуры атаки, а также ограниченностью существующих методов. Машинное обучение (МО), хотя и является перспективным направлением, сталкивается с трудностями при обработке малозначимых признаков и не способно надежно выявлять сложные атаки, искажающие структуру трафика. В этой связи поиск новых информативных признаков становится ключевой задачей. Одним из таких перспективных направлений является анализ фрактальных и мультифрактальных характеристик. Установлено, что сетевой трафик обладает свойством самоподобия, а аномальная активность закономерно изменяет его фрактальную размерность. Поскольку КА проявляют себя на разных временных масштабах, что указывает на их мультифрактальную природу, переход к соответствующему анализу является научно обоснованным. Таким образом, работа, направленная на интеграцию мультифрактального анализа и МО для обнаружения и классификации КА, отвечает современным вызовам кибербезопасности и несомненно является актуальной.

Цель и задачи исследования сформулированы четко и направлены на решение конкретной научной проблемы. Логика исследования выстроена последовательно: от анализа объекта и критического осмысления существующих методов к разработке и верификации собственных моделей и алгоритмов.

Обоснованность и достоверность полученных результатов подтверждается несколькими факторами: корректным использованием современных математических методов, проведением вычислительных экспериментов на известных, апробированных базах данных, статистической значимостью полученных результатов, а также их успешной апробацией на

ведущих научных конференциях. Важным аргументом является также публикационная активность автора: 16 печатных работ, 9 из которых – в рецензируемых журналах из перечня ВАК, что говорит о признании научного сообщества.

Практическая ценность работы убедительно доказана актами внедрения в проектной деятельности ФГУП «НИИ «Квант» и в образовательный процесс МТУСИ. Это свидетельствует о том, что разработанные решения имеют не только теоретическую, но и прикладную значимость для отрасли.

Научная новизна и результаты работы изложены в автореферате четко и содержат конкретные, количественно оцененные достижения. К наиболее значимым из них следует отнести:

- Разработку новой модели оценки фрактальной размерности с дополнительной фильтрацией коэффициентов вейвлет-разложения, обеспечивающей повышение точности на 15–40% в зависимости от типа материнского вейвлета.
- Создание метода обнаружения и классификации компьютерных атак, который за счет использования статистических характеристик фрактальной размерности повышает достоверность обнаружения в среднем на 10%.
- Введение понятия и разработку модели мультифрактального спектра фрактальной размерности, формализующей новые полезные признаки для классификации.
- Разработку метода композиции машинного обучения и мультифрактального анализа, демонстрирующего повышение точности многоклассовой классификации компьютерных атак на 7–10%.

Особого внимания заслуживают полученные практические результаты, такие как снижение времени на обучение и тестирование алгоритмов DTC и RF в 3,5 раза за счет введения всего четырех дополнительных фрактальных атрибутов. Это свидетельствует не только о повышении точности, но и об увеличении эффективности предложенных решений.

В качестве замечаний к автореферату можно отметить следующее:

1. В работе используется ансамблевый метод Random Forest. Не совсем понятно в чем заключаются преимущества именно деревьев решений для работы с введенными фрактальными признаками по сравнению, например, с линейными моделями.

2. На стр. 7 автореферата указано, что для анализа использовались базы данных DARPA99, UNSW-NB15, Kitsun, однако обоснование того

почему был выбран именно этот набор датасетов учитывая их специфику - отсутствует.

Указанные замечания носят уточняющий характер и не снижают общего высокого уровня проведенного исследования.

Представленный автореферат свидетельствует о том, что диссертационная работа Рыбакова Сергея Юрьевича является законченным научным исследованием, в котором решена актуальная научная задача, имеющая теоретическую и практическую значимость. Соискатель продемонстрировал глубокие знания в области защиты информации, владение современным математическим аппаратом и методами машинного обучения.

Диссертация соответствует всем требованиям, предъявляемым к кандидатским диссертациям, а ее автор, Рыбаков Сергей Юрьевич, заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6. – Методы и системы защиты информации, информационная безопасность.

Я, Козачок Александр Васильевич, даю согласие на включение моих персональных данных в документах, связанных с работой диссертационного совета и их дальнейшую обработку.

Сотрудник Академии ФСО России
доктор технических наук, доцент

Козачок Александр Васильевич

«21» ноября 2025 г.

Федеральное государственное казенное военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации» (Академия ФСО России)
Тел.: +7(4862) 54-94-99
E-mail: a.kozachok@academ.msk.rsnet.ru
Адрес: Россия, 302015, г. Орел, ул. Приборостроительная, д. 35

Подпись сотрудника Академии ФСО России доктора технических наук, доцента Козачка Александра Васильевича ЗАВЕРЯЮ:

Руководитель кадрового аппарата Академии ФСО России

А.Б. Семибратов