В диссертационный совет на базе
ФГБОУ ВО СПбГУПТД
24.2.385.09
191186, Санкт-Петербург, ул. Большая Морская, д.18

ОТЗЫВ

на автореферат диссертационной работы
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

Современные компьютерные атаки, зачастую скрываясь за сложными манипуляциями с сетевым трафиком, нарушают его нормальную мультифрактальную структуру, создавая тонкие, но характерные “отклонения”. Эти изменения, не улавливаемые традиционными методами, служат ключевыми индикаторами вредоносной активности. В условиях экспоненциального роста объемов данных, генерируемых системами безопасности, машинное обучение становится незаменимым инструментом. Оно не только позволяет эффективно обрабатывать и анализировать эти массивы информации, но и, что особенно важно, способно предсказывать потенциальные угрозы, выявляя поведенческие аномалии. Таким образом, синергия мультифрактального анализа, улавливающего эти тонкие отклонения в динамике трафика, и машинного обучения, обеспечивающего их обобщение и построение комплексных моделей принятия решений, формирует мощный подход к обнаружению и предотвращению киберугроз.

Все вышеизложенное свидетельствует о том, что тема диссертационной работы, посвященной обнаружению и классификации компьютерных атак

методами мультифрактального анализа и машинного обучения, а также повышению качества классификации компьютерных атак в компьютерных сетях с помощью комбинации мультифрактального анализа и машинного обучения является актуальной.

К числу наиболее значимых научных результатов, полученных лично автором, следует отнести:

- разработку и программную реализацию новой модели оценки фрактальных параметров компьютерных атак, которая отличается от известных наличием дополнительной фильтрацией, повышающей точность оценки в скользящем окне фрактальной размерности атак на 15…40% для различных типов материнских вейвлетов;

- использование 4-х дополнительных атрибутов, которое привело к снижению времени на обучение и тестирование для алгоритмов DTC и RF в 3,5 раза.

Полученные автором научные результаты представляются обоснованными и достоверными, что обеспечивается применением апробированных методов исследования, корректностью постановки задач, положительной их апробацией на научных конференциях.

По результатам исследования опубликовано 16 печатных работ, в том числе 9 в ведущих рецензируемых научных журналах ВАК РФ при Минобрнауке РФ. Основные результаты диссертационной работы прошли апробацию и были одобрены на 4 научных и практических конференциях.

В целом, анализ содержания представленного автореферата позволяет сделать вывод о том, что поставленная автором цель исследования достигнута, а научная задача решена в полном объеме. Вместе с тем, в ходе анализа работы выявлен ряд замечаний.

1. Представлен модифицированный алгоритм оценки показателя Херста (фрактальной размерности) с пороговой фильтрацией (трешолдинг), однако из автореферата не ясен выбор именно «жесткого» трешолдинга по сравнению с «мягким», кроме того, не указано, каким образом выбирается порог трешолдинга, и какое конкретно значение порога к примеру использовалось на рис. 1в.

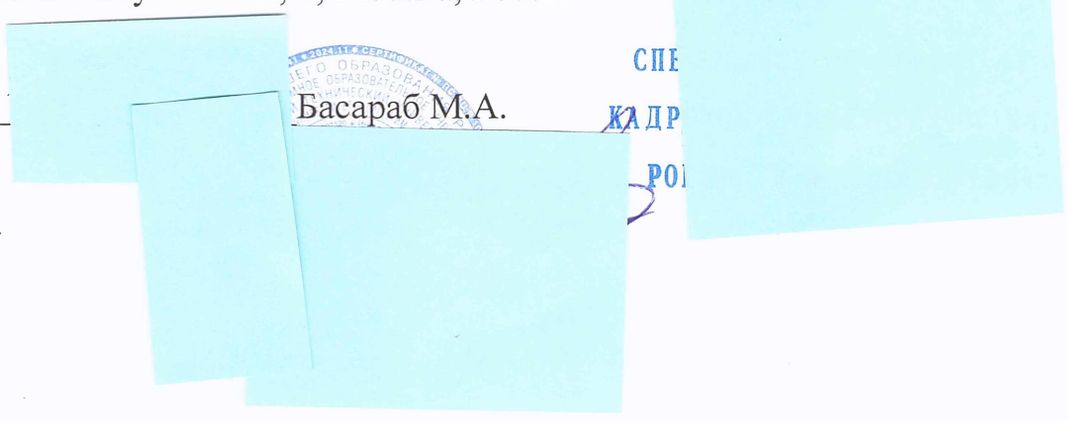
2. Нет обоснования выбора вейвлета Хаара и сравнения хотя бы с некоторыми другими типами ортогональных и биортогональных вейвлетов.
3. Для оценки показателя Херста автор использовал прямоугольное скользящее окно. Интерес представлял бы также анализ других типов оконных функций.

Указанные недостатки не снижают научную новизну, достоверность, теоретическую и практическую значимость полученных автором научных результатов. Требования по оформлению автореферата соблюдены.

Можно сделать вывод, что работа соответствует требованиям к диссертации на соискание ученой степени кандидата технических наук, указанных в «Положении о порядке присуждения ученых степеней», утвержденного постановлением Правительства №842 от 24.09.2013, а автор, Рыбаков Сергей Юрьевич, заслуживает присуждения ей степени кандидата технических наук по специальности 2.3.6. – Методы и системы защиты информации, информационная безопасность.

Я, Басараб Михаил Алексеевич, даю согласие на включение моих персональных данных в документах, связанных с работой диссертационного совета и их дальнейшую обработку.

Басараб Михаил Алексеевич,
доктор физико-математических наук, доцент
10.04.03 – радиофизика,
заведующий кафедрой «Информационная безопасность»
МГТУ им. Н.Э. Баумана,
105005, ул. 2-я Бауманская, 5, Москва, Россия



_____ Басараб М.А.

18.11.2025г.