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

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

Представленный к рассмотрению автореферат диссертационной работы Рыбакова С.Ю. посвящен решению актуальной научной проблемы в области информационной безопасности. Анализ материалов позволяет сделать следующие выводы.

Актуальность исследования определяется необходимостью разработки новых методов противодействия современным компьютерным угрозам, характеризующимся высокой степенью адаптивности и способностью к маскировке. Использование мультифрактального анализа для выявления структурных аномалий сетевого трафика в сочетании с методами машинного обучения представляет собой перспективное направление исследований.

Научная новизна представленной работы убедительно подтверждается рядом существенных результатов. Разработанная автором модифицированная модель оценки фрактальной размерности с применением процедуры трешолдинга коэффициентов вейвлет-разложения демонстрирует принципиально новый подход к обработке сетевого трафика. Предложенный метод использования статистических характеристик фрактальной размерности для улучшения качества классификации атак представляет значительный интерес с точки зрения повышения достоверности обнаружения. Особого внимания заслуживает введение понятия мультифрактального спектра фрактальной размерности как нового признакового пространства, что открывает перспективы для создания более совершенных систем анализа сетевой активности. Разработанный комбинированный метод, интегрирующий мультифрактальный анализ и машинное обучение, демонстрирует высокую эффективность при решении задач классификации компьютерных атак.

Достоверность полученных результатов обеспечивается комплексом методически грамотных подходов. Корректное применение математического аппарата фрактального и вейвлет-анализа свидетельствует о глубокой теоретической подготовке автора. Экспериментальная проверка на репрезентативных наборах данных проведена с соблюдением необходимых требований к верификации научных результатов. Статистическая значимость полученных результатов подтверждается строгими количественными оценками, а сравнительный анализ с существующими методами выполнен на должном научном уровне.

Особого внимания заслуживает публикационная активность автора, выразившаяся в 16 печатных работах, 9 из которых опубликованы в рецензируемых журналах из перечня ВАК. Данный факт свидетельствует не только о высокой степени проработанности темы, но и о признании значимости полученных результатов широким научным сообществом.

Практическая значимость исследования подтверждается не только теоретическими выкладками, но и реальными актами внедрения в деятельность ФГУП «НИИ «Квант», что свидетельствует о готовности разработок к промышленному применению. Внедрение результатов в учебный процесс МТУСИ дополнительно подчеркивает ценность работы для подготовки высококвалифицированных специалистов в области информационной безопасности.

Диссертация соответствует п.6. «Методы, модели и средства мониторинга, предупреждения, обнаружения и противодействия нарушениям и компьютерным атакам в компьютерных сетях» и п.15. «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности» паспорта специальности 2.3.6.

К автореферату имеются следующие замечания:

1. В рекомендациях автореферата (стр. 15) предлагается калибровка порогов на эталонном трафике. Однако осталось непонятным, что понимается под "эталонным трафиком" в контексте постоянно меняющихся сетевых условий.
2. В работе фрактальные признаки дополняют существующие 115 признаков в базе данных Kitsune. В связи с этим остается вопрос о принципиальной возможности построения эффективной системы обнаружения атак, основанной исключительно на фрактальных характеристиках, без привлечения традиционных признаков.

Не смотря на указанные замечания, диссертационная работа Рыбакова Сергея Юрьевича является завершенной научно-квалификационной работой и соответствует требованиям п. 9-14 «Положения о присуждении ученых степеней», предъявляемых к кандидатским диссертациям, а ее автор, Рыбаков Сергей Юрьевич, заслуживает присвоения ему ученой степени кандидата технических наук по специальности 2.3.6. Методы и системы защиты информации, информационная безопасность

Я, Красов А.В., даю согласие на включение моих персональных данных в документах, связанных с работой диссертационного совета и их дальнейшую обработку.

Красов Андрей Владимирович,

Кандидат технических наук, доцент,

05.13.01 Системный анализ, управление и обработка информации (технические системы)

Заведующий кафедрой Зачищенных систем связи, федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

193232, Санкт-Петербург, пр. Большевиков д.22, корп.1, литера А, Ж

подпись _____ Красов А.В.