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

Отзыв на автореферат диссертации
Рыбакова Сергея Юрьевича
на тему «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

Рассматриваемая диссертационная работа Рыбакова С.Ю. посвящена важной проблеме современной информационной безопасности – созданию методов обнаружения сетевых аномалий, устойчивых к постоянной эволюции способов реализации компьютерных атак. Особенностью исследования является ориентация на выявление не внешних признаков угроз, а глубинных изменений в структуре сетевого трафика, что представляется перспективным направлением.

Актуальность работы определяется необходимостью перехода от сигнатурного анализа к методам, способным выявлять ранее неизвестные атаки, маскирующиеся под легитимный трафик. Предложенный автором подход основан на анализе фундаментальных свойств сетевых процессов, что позволяет обнаруживать аномалии независимо от их конкретной реализации.

Научная ценность работы заключается в создании целостной методики анализа сетевой активности, объединяющей два перспективных направления. Разработанная модель оценки фрактальных характеристик с дополнительной фильтрацией данных демонстрирует существенное улучшение точности – до 40% в зависимости от условий эксперимента. Практически значимым результатом является не только рост точности классификации, но и сокращение времени обучения моделей при добавлении фрактальных признаков.

Особого внимания заслуживает введение концепции мультифрактального спектра, позволившей анализировать сетевую активность на различных временных масштабах. Этот подход открывает возможности для создания систем обнаружения, чувствительных к атакам, проявляющимся только на определенных уровнях детализации трафика.

Достоверность полученных результатов подтверждается их верификацией на репрезентативных наборах данных и статистической значимостью. Публикационная активность автора и факты внедрения разработанных решений в практическую

деятельность свидетельствуют о признании научным сообществом и практической ценности работы.

В качестве замечания к автореферату можно отметить следующее:

Из представленного текста автореферата не совсем понятно, как предложенный метод комбинации машинного обучения и мультифрактального анализа будет вести себя в условиях целенаправленной атаки, когда злоумышленник знает о его использовании и пытается адаптировать трафик для минимизации учета фрактальных свойств на характеристики обнаружения.

Не смотря на указанное замечание, диссертационная работа Рыбакова Сергея Юрьевича является завершенной научно-квалификационной работой и соответствует требованиям пунктов 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, Васильев Роман Александрович, даю согласие на включение моих персональных данных в документах, связанных с работой диссертационного совета и их дальнейшую обработку.

Отзыв составил:

Васильев Роман Александрович
Кандидат технических наук, доцент (05.13.19 - Методы и системы защиты информации, информационная безопасность)
Начальник отдела аудита информационной безопасности
Департамента информационной безопасности
Акционерное общество «Финансы, информация, технология» (АО «ФИНТЕХ»)
119180, Москва, 1-й Хвостов пер., 11а
Тел.: +7(499) 246-40-11 (доб. 465)
E-mail: r.vasilev@fintech.ru

« 7 » 11 2025г. Р.А. Васильев

Подпись Р.А. Васильева заверяю

Начальник отдела кадров АО «ФИНТЕХ» Н.А. Зуева