В диссертационный совет на базе
ФГБОУ ВО СПбГУПТД
Д 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

Для решения насущных проблем классификации компьютерных атак (КА) широкое распространение получили технологии машинного обучения. Такие методы позволяют разрабатываемой системе обнаружения быстро адаптироваться к постоянно меняющейся природе интернет-ресурсов и учитывать специфику анализа сетевого трафика.

В диссертационной работе Рыбакова С.Ю. проведен анализ современных методов и алгоритмов обнаружения КА. Дана оценка фрактальной размерности (ФР) с использованием методов мультифрактального анализа и машинного обучения. Разработан методический аппарат по оценке фрактальных свойств КА с использованием вейвлет анализа в режиме онлайн. Проведена экспериментальная оценка фрактальных свойств компьютерных атак. Дополнительно представлены результаты исследования процесса обнаружения КА в виде фиксации скачков фрактальной размерности в реальном времени.

Новая модель оценки характеристик мультифрактального спектра фрактальной размерности трафика компьютерных атак с помощью последовательности текущих оценок ФР в окне фиксированной длины, варьируемой в зависимости от интервала разрешения, позволяет формализовать новые полезные признаки классификации. Предложенный метод обнаружения и классификации КА повышает достоверность и точность их обнаружения в среднем на 10% за счет введения дополнительной информации о статистических характеристиках ФР сетевого трафика.

Полученные результаты имеют определенную теоретическую и практическую ценность, содержат реализацию разработанных алгоритмов при мониторинге и обеспечении ИБ компьютерных систем широкого профиля, в том числе киберфизических систем, в промышленном Интернете вещей, а также в других сложных информационных системах с иерархической структурой.

Разработанное автором программное обеспечение позволяет осуществлять оценки показателя Херста сетевого трафика в скользящем окне с применением процедуры трешолдинга, что позволяет повысить точность текущей оценки ФР и, тем самым, увеличить точность обнаружения аномалии в сетевом трафике в режиме online. Акты внедрения результатов работы подтверждают ее практическую ценность.

В качестве замечания хочу отметить следующее: из изложенного в автореферате не ясно, существует ли нижняя граница временного масштаба, предел детализации, за которым фрактальный анализ теряет практическую значимость для задач обнаружения кибератак. Тем не менее, отмеченное замечание не снижает общей положительной оценки диссертационной работы.

Считаю, что диссертационная работа Рыбакова Сергея Юрьевича на тему: «Обнаружение и классификация компьютерных атак методами мультифрактального анализа и машинного обучения» удовлетворяет требованиям ВАК Российской Федерации к кандидатским диссертациям, а сам Рыбаков С.Ю. заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6. – Методы и системы защиты информации, информационная безопасность.

Я, Дворянкин Сергей Владимирович, даю согласие на включение моих персональных данных в документах, связанных с работой диссертационного совета и их дальнейшую обработку.

Дворянкин Сергей Владимирович,
доктор технических наук, профессор
(05.13.19 - «Методы и системы защиты информации, информационная безопасность»),
профессор кафедры стратегий и технологий кибербезопасности (каф. 43) ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ»
115409, Российская Федерация, г. Москва, Каширское шоссе, д. 31
Тел.служ. : 8 (495) 788-5699, email: info@mephi.ru

«14» 11 2025 г. _ С.В. Дворянкин

Подпись С.В. Дворянкина заверяю