ОТЗЫВ
НА АВТОРЕФЕРАТ ДИССЕРТАЦИИ
КРИБЕЛЯ АЛЕКСАНДРА МИХАЙЛОВИЧА
НА ТЕМУ

«Выявление аномалий и классификация компьютерных атак в сети передачи данных на основе применения фрактального анализа и методов машинного обучения», представленной на соискание ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность»

В настоящее время компьютерные сети завоевывают все большую популярность. Примерами их реализации могут служить сети Интернета вещей, сети робототехнических комплексов, сенсорные сети и т.д. Компьютерные сети следует рассматривать как высокоразвитые системы с многоуровневой иерархической структурой. Для управления такими сложными, разветвленными и нелинейными системами необходимы поиск и использование инновационных подходов для прогнозирования развития событий с целью выработки правильных и оперативных управляющих решений.

Использование в компьютерных сетях информационных и коммуникационных технологий сбора информации дает возможность злоумышленнику воздействовать на эти сети путем реализации кибератак. Воздействие кибератак возможно за счет массового использования устаревших операционных систем, малоэффективных механизмов защиты и наличия множественных уязвимостей в незащищённых сетевых протоколах. Использование подобных уязвимостей даёт потенциальному злоумышленнику возможность изменять настройки встроенных сетевых устройств, прослушивать и перенаправлять трафик, блокировать сетевое взаимодействие и получать несанкционированный доступ к внутренним компонентам компьютерных сетей. В этом случае кибератаки следует рассматривать как один из ключевых факторов, определяющих живучесть компьютерных сетей.

Несмотря на наличие множества решений по защите компьютерных сетей от кибератак (например, Arbor Networks), тематика научных исследований по-прежнему остается актуальной. Особую значимость имеют методы и подходы, связанные с обнаружением и анализом аномальной активности сетевого трафика, вызванной воздействием кибератак. Это направление позволяет реализовать раннее детектирование кибератак. Все это послужило поводом для поиска новых методов обнаружения и прогнозирования кибератак, реализуемых злоумышленниками.

Воздействие кибератак приводит к появлению в трафике компьютерных сетей аномальной активности. Для постоянного мониторинга и обнаружения аномальной активности сетевого трафика необходимо учитывать множество факторов. К таким факторам относятся: (1) наличие большого количества

сетевых маршрутов, на которых периодически возникают резкие колебания задержки в передаче данных и большие потери пакетов, (2) появление новых свойств сетевого трафика, (3) необходимость обеспечения высокого качества обслуживания приложений и т.д.

В связи с вышеизложенным, диссертация Крибеля А.М. является актуальной и имеет важное практическое значение.

Цель исследования - повышение эффективности выявления аномалий и классификации компьютерных атак (КА) в сетевом трафике сети передачи данных (СПД).

Научная задача – разработка аналитической модели и методик выявления аномалий и классификация КА в сетевом трафике СПД на основе применения фрактального анализа и методов машинного обучения.

Положения, выносимые на защиту:

1. Аналитическая модель выявления аномалий в сетевом трафике СПД в условиях КА.
2. Методика раннего обнаружения аномалий в сетевом трафике СПД.
3. Методика классификации КА в сетевом трафике СПД.
4. Архитектура и программные компоненты системы раннего обнаружения и классификации КА в сетевом трафике СПД.

Научная новизна результатов исследования заключается в том, что:

разработанная аналитическая модель выявления аномалий в сетевом трафике СПД в условиях КА, в отличие от известных, описывает не только стационарный, но и нестационарный сетевой трафик и обосновывает выбор фрактального метода выявления аномалий в интересах дальнейшей классификации компьютерных атак в зависимости от типа трафика;

разработанная методика раннего обнаружения аномалий в сетевом трафике СПД, в отличие от известных, способна проводить прогнозирование и обнаружение не только известных, но и неизвестных КА на раннем этапе их проявления благодаря совместному применению методов фрактального анализа и искусственной нейронной сети LSTM-типа (рекуррентные нейронные сети с долгой краткосрочной памятью), в результате чего существенно сокращается время выявления аномалий и уменьшается количество ложных срабатываний;

разработанная методика классификации КА в сетевом трафике СПД отличается от известных тем, что в ней обнаружение компьютерных атак производится с использованием генеративно-состязательной сети, которая производит дообучение классификатора на скрытых латентных представлениях, полученных автокодировщиком, исходя из анализа данных о функционировании СПД;

предложенная архитектура и программные прототипы компонентов системы раннего обнаружения и классификации КА в СПД отличаются от известных тем, что они ориентированы на раннее обнаружение как известных, так и неизвестных КА с минимальным количеством ложных

срабатываний за счет реализации методов фрактального анализа и искусственной нейронной сети LSTM-типа.

Результаты по положениям, выносимым на защиту в диссертационной работе, получены автором самостоятельно, в частности разработаны: модель выявления аномалий в сетевом трафике СПД в условиях КА; методики раннего обнаружения аномалий в сетевом трафике СПД и классификации КА в сетевом трафике СПД. Разработан и зарегистрирован в установленном порядке программный компонент обнаружения аномалий сетевого трафика на основе принципов фрактального анализа данных, а также опубликованы самостоятельно и в соавторстве прочие результаты, при этом вклад соискателя в совместных публикациях был решающим.

В качестве основных недостатков работы можно было бы выделить следующие:

1. Из автореферата не ясно, как связаны между собой компьютерные атаки «нулевого дня» и аномалии в сетевом трафике.

2. При описании архитектуры и программного компонента системы раннего обнаружения и классификации КА в сетевом трафике СПД не раскрыто, каким образом реализована нейтрализация КА.

Но, несмотря на указанные недостатки, диссертация Крибеля А.М. является завершенной научной квалификационной работой, отличающейся актуальностью и полнотой проведенного исследования, в которой решена новая научная задача, имеющая важное значение для информационной безопасности страны. Автореферат изложен лаконично, технически грамотным языком.

Работа отвечает пп. 9, 10, 11 и 14 требований «Положения о присуждении ученых степеней», а ее автор заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность».

Доцент
Факультета безопасности
информационных технологий
Федерального государственного
автономного образовательного учреждения
высшего образования
«Национальный исследовательский университет ИТМО»

Евглевская Наталья Валерьевна

» апреля 2023 г.
e-mail: n.evglevskaya@gmail.com
Тел.: 8-906-277-12-89
Почтовый адрес: 197101, г.Санкт-Петербург, Кронверкский проспект, д.49, литер А