Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.73:004.056

Миланович
Евгений Александрович

Контроль сетевого трафика в системах безопасности сети

АВТОРЕФЕРАТ
на соискание степени магистра информатики и вычислительной техники
по специальности 1–40 81 02 Технологии виртуализации и облачных вычислений

_____

Научный руководитель

Селезнёв Игорь Львович

кандидат технических наук, доцент

_____

Минск 2020

ОБЩАЯ ХАРАКТЕРИСТИКА

Цель и задачи исследования

Объектом исследования является мониторинг безопасности локальной сети.

Предметом исследования является система анализа трафика компьютерной сети.

Цель исследования – разработка программного средства обеспечивающее анализ трафика в режиме реального времени с высокой точностью.

Задачи исследования:

1. Обзор методов мониторинга сети;
2. Анализ технологий, используемых для анализа сетевого трафика;
3. Разработка системы анализа трафика компьютерной сети.

Публикации

Миланович, Е.А. Актуальные уязвимости в системах контроля доступа / Е.А. Миланович // Молодой ученый. – 2019. – №44. – С.88–90 [1–А].

Миланович, Е. А. Система анализа сетевого трафика для обеспечения безопасности сети / Е. А. Миланович, И. Л. Селезнёв. — Текст: непосредственный // Молодой ученый. — 2020. — № 15 (305). — С. 86–89 [2–А].

Апробации

Нет

ВВЕДЕНИЕ

Постоянный контроль за работой локальной сети, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль – это необходимый первый этап, который должен выполняться при управлении сетью. Ввиду важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами.

На этапе мониторинга выполняется более простая процедура – процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Перспективным направлением является использование нейронных сетей. Они позволяют быстро и качественно выполнять поставленную задачу.

Целью работы является развитие нейронных сетей для анализа трафика. Создание оптимизированной модели, превосходящей аналоги по различным параметрам.

Компоненты данной системы в дальнейшем могут быть интегрированы в процесс построения сложных нейронных сетей и программные средства по мониторингу и аудиту сетей.

СОДЕРЖАНИЕ РАБОТЫ

Общий объем магистерской диссертации составляет 66 страниц, включая 9 иллюстраций, 11 таблиц, библиографический список из 31 наименования, 1 приложение

Во **введении** дается обоснование актуальности работы, описываются прикладные задачи, в которых может быть использована разработанная система, приводится краткий перечень требований к разрабатываемой системе. Также в разделе приводится краткий обзор проблематики задачи и современного состояния исследований по классификации трафика компьютерной сети.

В **общей характеристике** работы сформулированы цель и задачи исследования, даны сведения об объекте и предмете исследования, приведены публикации результатов.

В **первой главе** произведен анализ актуальных методов аудита состояния и безопасности сети. Приведены исследования на тему классификации трафика компьютерной сети. Сделан подробный анализ этих исследований и выделены выявленные достижения и проблемы. Рассмотрены три основных алгоритма классификации трафика, какие используются на данный момент.

Во **второй главе** приводится подробное описание разработанной нейронной сети. Описываются подробности оптимизации модели с экспериментальной проверкой и обоснованием выбранных решений.

В **заключении** приводится краткий обзор результатов, полученных на каждом из этапов исследования, приводится обоснование выбранных методов и инструментов, дается критический анализ разработанной системы, и приводится описание проблем, которые будут более подробно раскрыты в дальнейших исследованиях.

ЗАКЛЮЧЕНИЕ

В ходе исследования был проведен анализ существующих методов анализа трафика. Были проанализированы решения по классификации трафика, т.к. в этой области наблюдаются проблемы с точность и стабильностью применяемых методов.

В результате исследования была построена облегченная нейронная сеть, способная классифицировать сетевой трафик в реальном времени с высокой точностью. Были спроектированы эффективные процедуры обработки и оптимизации данных, которые можно применить и для других методов контролируемого машинного обучения. Разработан быстрый метод определения ключевых атрибутов в нейронной сети на основе весов соединений. Этот метод подобрал более подходящие атрибуты, какие позволили увеличить точность классификации с 94%–97% до 99.0%.

Результаты проведенных экспериментов показывают, что существуют фундаментальные различия между сетью персептрона и применяемыми методами наивной байесовской классификации, которые проявляются в ключевых атрибутах, идентифицированных обеими системами.

Используя последние исследования как отправную точку, получилось найти оптимизированную конфигурацию нейронной сети, что позволило достичь точности классификации выше 99%. В разработанной облегченной модели били применены методы one–hot embedding на 13 самых популярных серверных портах, 9 атрибутов идентифицированных по весам соединений, один скрытый слой с 12 нодами и функция активации tanh.

При классификации данных, собранных через продолжительный промежуток времени, все системы испытывают снижение точности классификации. Однако, в разработанной модели, получилось снизить потери на 3,8% по сравнению с самым эффективным существующим методом классификации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

1–А. Миланович, Е.А. Актуальные уязвимости в системах контроля доступа / Е.А. Миланович // Молодой ученый. – 2019. – №44. – С.88–90.

2–А. Миланович, Е. А. Система анализа сетевого трафика для обеспечения безопасности сети / Е. А. Миланович, И. Л. Селезнёв. — Текст: непосредственный // Молодой ученый. — 2020. — № 15 (305). — С. 86–89.