Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники
Кафедра информационных технологий автоматизированных систем

УДК 004.891.3

Шаюнов
Евгений Михайлович

Методы выявления аномальных и аварийных состояний сети

АВТОРЕФЕРАТ

диссертации на соискание степени магистра технических наук

по специальности 1-40 80 02 – Системный анализ, управление и обработка информации

Научный руководитель
Шавель Александр Николаевич
кандидат физ.-мат. Наук

Минск 2020

КРАТКОЕ ВВЕДЕНИЕ

Разработка системы обнаружения атак (СОА) является одним из приоритетных направлений в области информационной безопасности. Важность решения этой задачи обусловливается постоянным увеличением и разнообразием компьютерных сетевых угроз, реализация которых может приводить к серьезным потерям в различных компаниях. В связи с ростом количества и сложности серверных атак требуется тратить большие силы на их предотвращение. В компаниях, вовлеченных в производство продукции, для поддержания безопасности сетевых ресурсов расходуются крупные финансовые и материальные средства, направленные на содержание специального оборудования в виде компонентов СОА и обслуживающего его персонала. Для обеспечения корректной пакетной передачи данных необходимо выполнять их сборку в минимальный логический поток — сетевое соединение, что позволит оперировать более высокоуровневыми характеристиками сетевого трафика для выявления аномалий, свойственных сетевому и транспортному уровням модели OSI.

Существует множество методов и средств обеспечения сетевой безопасности, таких как шифрование, VPN, брандмауэры и т.д. Но все они слишком статичны, чтобы обеспечить эффективную защиту. Используемая система должна иметь способность обновляться, так как мошенники постоянно меняют методы атаки на информационные ресурсы. Использование интеллектуальной модели системы обнаружения атак может решить такую задачу. Системы обнаружения с интеллектуальной поддержкой обладают высоким потенциалом, поэтому исследования и разработка систем принятия решений в этой области активно ведутся в настоящее время.

Для сохранения преимуществ всех методов и подходов используется прием их комбинирования, который по-прежнему остается не до конца доработанным, поэтому задача обнаружения аномальных сетевых соединений до сих пор является актуальной.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования. Целью данной работы является разработка прототипа системы сбора сетевого трафика для анализа и выявления несанкционированной активности. В рамках диссертации были решены следующие задачи:

1. обозначение проблемы обеспечения безопасности сети и анализ современных методик анализа сетевого трафика;
2. разработка оптимальной архитектуры системы;
3. создание алгоритмов статистической обработки полученных данных;
4. реализация прототипа программной системы обнаружения вредоносного трафика на основе разработанной архитектуры и алгоритмов.

Новизна полученных результатов. На данный момент существует достаточное количество различных СОА, но тем не менее все они основаны на каком-нибудь одном методе, гибридных СОА на сегодняшний день практически нет. Также практически не используются методы системного анализа и использование искусственного интеллекта для отражения сетевых атак. В ходе работы рассматривается как раз использование гибридных СОА, а также методы статистического анализа для обнаружения и предотвращения потенциальной атаки.

Положения, выносимые на защиту. Положениями, выносимыми на защиту являются:

1. модели статистических методов обнаружения сетевых атак, их сравнительная характеристика;
2. архитектура и подходы к реализации разрабатываемой системы мониторинга;
3. программная реализация системы мониторинга.

Апробация результатов диссертации. Основные результаты диссертации были представлены на 56 научной конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

Опубликованность результатов исследования. Результаты диссертации изложены в печатном сборнике материалов 56 научной конференции аспирантов, магистрантов и студентов учреждения образования

«Белорусский государственный университет информатики и радиоэлектроники».

Структура и объем диссертации. Диссертация состоит из введения, четырёх глав, заключения и четырёх приложений. Основной материал изложен на 50 страницах. Полный объем диссертации составляет 65 страниц с 24 рисунками и 2 таблицами. Список литературы содержит 30 наименований.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В **первой главе** приведен подробный обзор возможных аномальных состояний сети. Приведена классификация сетевых аномалий, а также их описание. Выполнен анализ методов обнаружения сетевых атак, предложена их классификация. Произведен обзор алгоритма обнаружения сетевых аномалий и обзор алгоритма обнаружения злоупотреьлений в сети. Определены место и роль ИИ в задачах обнаружения аномальных сетевых соединений. Представлены наиболее распространённые методы статистического анализа, а также их сравнительная характеристика. Выполнена постановка задачи исследования, и сформулирована цель работы.

Во **второй главе** представлены классификация клпссических СОА, приведена их сравнительная характеристика. Рассмотрены все достоинства и недостатки систем. Рассмотрены различные характеристики систем обнаружения вторжений, их плюсы и минусы. Рассмотрена классификация СОА по параметрам. Также была рассмотрена архитектура классической СОА, перечислены основные элемены системы, описана их работа. Рассмотрена глобальная архитектура системы обнаружения вторжений. Приведена структурная схема классической системы обнаружения вторжений и описана работа всех ее элементов и датчиков. Рассмотрено взаимодействие различных СОА друг с другом. Приведены достоинства и недостатки подобного взаимодействия. Перечислены требования, предъявляемые к современным СОА. Рассмотрены примеры существующих систем обнаружения и приведены плюсы и минусы этих систем.

В **третьей главе** рассмотрен вопрос проектирования собственной системы обнаружения аномалий. Были поставлены следющие задачи:

1. Задача перехвата трафика
2. Задача анализа трафика
3. Задача хранения трафика

Разработана и представлена схема подзадач системы анализа сетевого трафика. Рассматривается работа снифферов для обеспечения работы системы. Рассмотрены библиотеки, задействованные в современных СОА для использования их в собственной системе.

В **четвёртой главе** рассмотрен вопрос разработки прототипа системы анализа трафика. Приведена структурная схема системы анализа сетевого трафика. Рассмотрена модель данных, которая должна поступать на вход

системы. Рассмотрена работа основных модулей системы и обоснование выбора программных средств для разработки данных модулей. Представлена работа непосредственно самой системы мониторинга.

ЗАКЛЮЧЕНИЕ

Изучение современных методик анализа сетевого трафика показало, что статистическое исследование трафика, исходящего из локальной сети во внешнюю сеть на текущий момент активно не используется в системах защиты. Основное направление подобных систем – это мониторинг работоспособности оборудования, нагрузки на каналы; а для локальных сетей это защита от угроз приходящих из внешней сети.

Созданные алгоритмы статистической обработки являются первым приближением для серьезной аналитики. В будущем следует учесть, что получаемые данные имеют гораздо больший объем. Необходимо постоянно оптимизировать и дорабатывать систему во избежание потери актуальности.

В рамках магистерской диссертации был разработан прототип системы анализа трафика, который решает следующие задачи:

1. обрабатывает дамп трафика;
2. преобразует и сохраняет сетевые пакеты в базу данных;
3. отображает разработанную аналитику.

Предполагаемый эффект, в случае применения подобных систем у большого числа пользователей, выглядит перспективным. Стоит учитывать, что назначение системы не защита трафика, а анализ большого потока и выявление возможных статистически некорректных случаев, на основе которых система сможет принять решение о выполнении действий по предотвращению потенциальной атаки.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

№ п/п	Название	Пе-чатн. или руко-писн.	Изд-во, журн. (название, №, год) или № авторского свидетельства	Кол-во печат-ных листов или стр.	Фамилии соавторов
1	2	3	4	5	6
1	Алгоритмы вычисления линейной свертки	Печатн.	Минск: БГУИР, 2017.	4	Латушкин К.Ю., Фам М.Т., Конюх В. А.
2	Системный анализ серверов для выявления аномальных и аварийных состояний сети	Печатн.	Минск БГУИР 2020	2	