Федеральное государственное автономное образовательное учреждение высшего образования
"Санкт-Петербургский политехнический университет Петра Великого"

На правах
рукописи

Алексеев Илья Вадимович

ОБНАРУЖЕНИЕ РАСПРЕДЕЛЁННЫХ АТАК ОТКАЗА В ОБСЛУЖИВАНИИ В КРУПНОМАСШТАБНЫХ СЕТЯХ НА ОСНОВЕ МЕТОДОВ МАТЕМАТИЧЕСКОЙ СТАТИСТИКИ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени

кандидата технических наук

Санкт-Петербург — 2020

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО СПбПУ) в Институте кибербезопасности и защиты информации.

Научный руководитель: Зегжда Петр Дмитриевич, доктор технических наук, профессор, профессор, заслуженный деятель науки Российской Федерации.

Официальные оппоненты:
Козачок Александр Васильевич,
доктор технических наук, сотрудник Федерального государственного казённого военного образовательного учреждения высшего образования «Академия Федеральной службы охраны Российской Федерации».

Красов Андрей Владимирович,
кандидат технических наук, доцент, заведующий кафедрой Защищенных систем связи ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича».

Ведущая организация:
ФГБОУ ВО «Российский государственный гидрометеорологический университет».

Защита состоится «17» декабря 2020 года в __ ч. на заседании диссертационного совета У.05.13.19 на базе ФГАОУ ВО СПбПУ по адресу: 195251, г. Санкт-Петербург, ул. Политехническая, д. 29, ауд. 175.

С диссертацией, авторефератом можно ознакомиться в библиотеке и на сайте ФГАОУ ВО СПбПУ (www.spbstu.ru).

Автореферат разослан «__» _____ 2020 года.

Ученый секретарь диссертационного совета У.05.13.19, к.т.н. Лаврова Дарья Сергеевна

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы.

В настоящее время самым распространенным способом реализации атак на конечные устройства, будь то персональный компьютер пользователя или датчики и контроллеры в системе Интернета вещей, являются сетевые атаки. С помощью сетевых атак возможны: эксплуатация уязвимостей в программном обеспечении (ПО) устройства, удаленное управление через внедренное вредоносного программного обеспечения (ВПО), создание ботнет-сетей, а также выведение из строя узлов, связанных с критическими отраслями деятельности человека, что может привести к серьёзным последствиям.

Доступ к сети Интернет пользователю предоставляет провайдер. Глобально провайдеры соединены между собой магистральными опорными сетями, скорость данных в которых достигает более 100Гб/с-1Тб/с. Крупномасштабные сети, включают в себя как сетевые потоки легитимных пользователей, так и трафик атакующих лиц. Очевидно, что обнаружение аномалий на уровне маршрутизаторов крупномасштабных сетей позволит обеспечить предотвращение атак на конечных пользователей.

Распределенные атаки типа «отказ в обслуживании» (DDOS) привели к значительным финансовым потерям во всем мире. Представленные результаты соответствуют растущему числу устройств, подключенных к Интернету. Подобный рост обусловлен популяризацией Интернета вещей и характеризуется концепцией подключения любого устройства в любом месте в любое время. Одним из самых опасных вредоносных трафиков в Интернете являются высоконагруженные атаки DDOS, которые отвечают за более чем 65% всех подобных атак. При данном типе DDOS атаки злоумышленники координируют отправку большого количества случайных данных в попытке перегрузить вычислительные ресурсы жертвы или ближайшие сетевые соединения. Однако помимо высоконагруженных DDOS атак, становятся распространены и малонагруженные импульсные атаки. Это более скрытый тип атаки: события происходят быстро, сама атака разбивается на несколько импульсов и обычно длится меньше часа. Из-за скорости и специфики сложно определить, что ресурс подвергается атаке, поскольку обычные инструменты не обнаруживают этот тип угрозы.

Решение задачи обнаружения распределённых атак отказа в обслуживании в крупномасштабных сетях осложняется рядом причин. Во-первых, это высокая разнородность поступающих данных ввиду большого числа разнообразных устройств, подключенных к сети Интернет. Во-вторых, это высокий объем интенсивно поступающего трафика, что накладывает серьезные ограничения на

обнаружение аномалий, проявляющихся в виде небольших отклонений, которые сглаживаются на больших объемах данных. В-третьих, это высокие временные затраты для анализа крупномасштабного трафика, что ограничивает возможность применения большинства существующих методов обнаружения DDOS атак. Таким образом, задача обнаружения распределённых атак отказа в обслуживании в крупномасштабных сетях актуальна и обоснована.

Существующие подходы к обнаружению DDOS атак прежде всего направлены на выявление вредоносного сетевого трафика в слабонагруженных сетях, и в малой степени охватывают уязвимости, обусловленные сетевыми нагрузками. Ограниченное число исследований предлагают решение задачи обнаружения и предотвращения DDOS атак в крупномасштабных сетях на основе строгой фильтрации сетевых пакетов, применения разнообразных политик безопасности и методов математической статистики. Однако отсутствует решение, применяющее методы искусственного интеллекта для решения поставленной задачи с целью динамического реагирования на изменяемый сетевой трафик. Данная работа направлена на решение проблем, связанных с обеспечением информационной безопасности в крупномасштабных сетях и выявлением DDOS атак в них.

Степень разработанности темы исследования.

Проблеме обнаружения DDOS атак посвящено множество исследований российских и иностранных ученых, таких как О.И. Шелухин, А.В. Гармашев, В.В, Платонов, Ю. Гао, Ф.А. Сильвейра, Дж. Вентре, С.Ф.Чуи, Р. Робинсон, А.В. Лукацкий, Я.В. Тарасов, О.С. Терновой, И.И. Слеповичев, П.В. Ирматов, М.С. Комарова, А.А. Бежин.

Проблемам обнаружения DDOS атак в крупномасштабных сетях посвящены работы П.Д. Зегжды, Д.С. Лавровой, Ли Юеминг, Сун-Хо Ким, Лукаса Руфа, А. Вагнера, Б. Платтнера, А.В.Красова.

Объектом исследования является крупномасштабный сетевой трафик, содержащий DDOS атаки.

Предметом исследования являются методы и алгоритмы обеспечения информационной безопасности, выполняющие обнаружение сетевых DDOS атак.

Цель и задачи исследования.

Цель – повышение достоверности выявления вредоносного сетевого трафика, содержащего DDOS атаки, в крупномасштабных сетях за счет совместного применения аппарата вейвлет-преобразований, методов математической статистики и искусственного интеллекта.

Для достижения поставленной цели в работе решались следующие **задачи**:

1. Исследовать угрозы информационной безопасности в сети Интернет от распределенных атак отказа в обслуживании и существующие методы их обнаружения.

2. Создать и теоретически обосновать метод обнаружения DDOS атак в крупномасштабных сетях, включающий:

2.1. Извлечение минимально достаточного объема сетевых параметров для сокращения объема анализа выборки с помощью вейвлет-преобразования.

2.2. Проведение предварительной выборки потенциально вредоносного сетевого трафика путем анализа частотно-временных характеристик вейвлет-преобразования с последующей обработкой с помощью кластерного анализа.

2.3. Обнаружение DDOS атак в крупномасштабной сети путем анализа частотно-временных характеристик вейвлет-преобразования с последующей обработкой с помощью кластерного анализа.

3. Создать алгоритм адаптации, обеспечивающий коррекцию параметров выполнения метода обнаружения DDOS атак в крупномасштабных сетях относительно изменений интенсивности сетевой нагрузки и разнородности сети.

4. Осуществить оценку достоверности обнаружения DDOS атак в крупномасштабных сетях.

5. Разработать архитектуру системы обнаружения DDOS атак с применением принципа модульности и провести экспериментальные исследования эффективности его применения для выявления угроз безопасности в крупномасштабных сетях.

Научная новизна.

1. Сокращение объема информации и времени анализа без снижения достоверности обнаружения DDOS атак в крупномасштабных сетях. Данный метод использован в программе для ЭВМ и зарегистрирован Федеральной Службой по Интеллектуальной Собственности под номером №2018660604.

2. Разработан алгоритм адаптации, обеспечивающий коррекцию параметров выполнения метода обнаружения DDOS атак в крупномасштабных сетях относительно изменений интенсивности сетевой нагрузки и разнородности сети.

3. Впервые предложено использовать сочетание методов математической статистики и искусственного интеллекта для решения задачи определения вредоносного сетевого трафика в крупномасштабных сетях.

Предложенные методы и алгоритмы позволяют существенно повысить результативность процесса выявления DDOS атак в крупномасштабных сетях.

Теоретическую значимость работы составляют предложенный метод обнаружения DDOS атак в крупномасштабных сетях на основе отобранных параметров сетевых пакетов с использованием вейвлет-преобразования, методов математической статистики и искусственного интеллекта за счет проведения машинного обучения с последующим уточнением с применением кластерного анализа с целью сокращения данных и времени анализа, а также алгоритм адаптации, обеспечивающий коррекцию параметров выполнения метода обнаружения DDOS атак в крупномасштабных сетях относительно изменений интенсивности сетевой нагрузки и разнородности сети.

Практическая значимость результатов работы заключается в возможности применения предложенного метода к обнаружению DDOS атак в крупномасштабных сетях за счет проведения анализа сетевого трафика, проходящего через точки обмена сети Интернет. Предложенные методы и алгоритмы могут быть использованы провайдерами крупномасштабных сетей для улучшения существующих систем выявления и анализа сетевых атак. Предложенный метод выявления DDOS атак на основе методов машинного обучения и математической статистики также может быть использован для построения средств выявления сетевых DDOS атак и защиты от целенаправленных атак.

Методологию и методы исследования составили методы математической статистики, теории искусственного интеллекта и анализа данных.

Положения, выносимые на защиту:

1. Метод обнаружения DDOS атак в крупномасштабных сетях, отличающийся:

1.1 Использованием минимально достаточного объема сетевых параметров для сокращения объема анализа выборки с помощью вейвлет-преобразования.

1.2 Проведением предварительной выборки потенциально вредоносного сетевого трафика с целью сокращения времени обнаружения.

2. Алгоритм адаптации, обеспечивающий коррекцию параметров выполнения метода обнаружения DDOS атак в крупномасштабных сетях относительно изменений интенсивности сетевой нагрузки и разнородности сети.

Научная специальность и отрасль науки, которым соответствует диссертация.

Диссертация соответствует специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» отрасли технических наук – пп. 3, 5, 9 раздела 2 «Области исследований» паспорта специальности: «Методы, модели и средства выявления, идентификации и классификации угроз

нарушения информационной безопасности объектов различного вида и класса»; «Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет»; «Модели и методы оценки защищенности информации и информационной безопасности объекта».

Степень достоверности результатов исследования подтверждается всесторонним анализом предшествующих научных работ в данной области, полученными экспериментальными данными, апробацией результатов в научных публикациях и докладах на конференциях, их внутренней непротиворечивостью и адекватностью физическим представлениям об исследуемом процессе.

Внедрение результатов работы.

Результаты диссертационной работы нашли свое отражение в научной деятельности при финансовой поддержке Министерства образования и науки Российской Федерации в рамках ФЦП «Исследования и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014-2020 годы» (соглашение № 14.578.21.0231, уникальный идентификатор соглашения RFMEFI57817X0231), в проектной деятельности АО «НПК «ТРИСТАН», а также в учебном процессе Института кибербезопасности и защиты информации ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого» при организации дисциплин «Программно-аппаратные средства обеспечения информационной безопасности», «Сети и системы передачи информации» и «Безопасность компьютерных сетей» в виде методических рекомендаций по проведению лекционных, практических и лабораторных занятий, а также для сопровождения научной деятельности аспирантов и докторантов по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Апробация результатов работы.

Основные результаты исследований и научных разработок докладывались и обсуждались на научно-технической конференции «Методы и технические средства обеспечения безопасности информации» (Санкт-Петербург, 2018).

Публикации по теме работы.

Результаты научно-квалификационной работы отражены в 6 публикациях, в том числе 3 публикаций в рецензируемых журналах из перечня ВАК РФ, 1 публикаций в изданиях из перечня Scopus и Web of Science, свидетельство РФ о регистрации программы для ЭВМ.

Объем и структура работы.

Диссертация состоит из введения, четырех глав, заключения, списка использованных источников из 129 наименований и списка сокращений и

условных обозначений. Общий объем работы составляет 134 страниц, в том числе 24 рисунка и 3 таблицы.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы исследования, поставлена цель и определены основные задачи. Сформулированы основные научные результаты исследований и положения, выносимые на защиту. Раскрыта научная новизна, теоретическая и практическая значимость полученных результатов. Представлены сведения по апробациям и публикациям по теме исследований. Приведена краткая аннотация содержания диссертации по главам. Рассмотрены возможности практического применения предложенных в работе подходов и методов.

В первой главе приведены результаты исследования угроз информационной безопасности в сети Интернет и существующих методов обнаружения распределенных атак отказа в обслуживании. Описаны примеры сетевых топологий, представлен анализ особенностей построения сети, приведен перечень компонентов сети и указание их функционального назначения.

Представлен анализ известных уязвимостей в компонентах сети, демонстрирующий DDOS уязвимости. Разработана классификация DDOS атак, представлены примеры по каждой категории DDOS атаки.

Современные магистральные сети имеют пропускную способность более 4 Тбит/с в пике и более 2 Тбит/с в среднем. DDOS атаки являются одной из самых опасных атак, нарушающих информационную безопасность целевой системы, в 2020-ом году число атак возросло примерно в 2 раза по сравнению с прошлым годом. Средняя нагрузка DDOS атаки составляет 5-10 Гб/с. Основным типов DDOS атак по состоянию на 2019 год является TCP SYN-flood атака. При этом АО и ПО, применяемое компаниями для организации веб-сервисов и услуг доступа, до сих пор содержат уязвимости, которые не всегда оперативно исправляют. Спецификации сетевых протоколов изначально разработаны и эксплуатируются «как есть». Для исправления уязвимостей применяются расширения сетевых протоколов, различные политики безопасности, фильтрации и эвристики. Однако каждая компания применяет данные техники локально и отсутствуют популярные и эффективные коммерческие решения для обнаружения DDOS атак в магистральных сетях. На уровне крупномасштабных сетей применяются техники системного администрирования и фильтрации по методу черного списка, а также статистические методы анализа сетевого трафика на высоком уровне анализа сетевого потока, что демонстрирует слабую эффективность.

Решение задачи обнаружения распределённых атак отказа в обслуживании в крупномасштабных сетях осложняется рядом причин. Во-первых, это высокая

разнородность поступающих данных ввиду большого числа разнообразных устройств, подключенных к сети Интернет. Во-вторых, это высокий объем интенсивно поступающего трафика, что накладывает серьезные ограничения на обнаружение аномалий, проявляющихся в виде небольших отклонений, которые сглаживаются на больших объемах данных. В-третьих, это высокие временные затраты для анализа крупномасштабного трафика, что ограничивает возможность применения большинства существующих методов обнаружения DDOS атак. Таким образом, задача обнаружения распределённых атак отказа в обслуживании в крупномасштабных сетях актуальна и обоснована.

Во второй главе приводятся результаты исследования подходов и методов обнаружения DDOS атак. Приведен сравнительный анализ рассмотренных подходов к выявлению DDOS атак. Выявлены ограничения в их практическом применении.

Существующие подходы к обнаружению DDOS атак прежде всего направлены на выявление вредоносного сетевого трафика в слабонагруженных сетях, и в малой степени охватывают уязвимости, обусловленные сетевыми нагрузками. Ограниченное число исследований предлагают решение задачи обнаружения и предотвращения DDOS атак в крупномасштабных сетях на основе строгой фильтрации сетевых пакетов, применения разнообразных политик безопасности и методов математической статистики. Однако отсутствует решение, применяющее методы искусственного интеллекта для решения поставленной задачи с целью динамического реагирования на изменяемый сетевой трафик.

На основе выполненного анализа формулируются требования, которыми должен обладать метод, позволяющий эффективно обнаруживать DDOS атаки:

1. Способность эффективно и своевременно обнаруживать DDOS атаки в крупномасштабных сетях.
2. Адаптация к постоянному изменению сетевой нагрузки в крупномасштабных сетях.
3. Адаптация к постоянному изменению уровня разнородности сетевого трафика.

Алгоритм должен быть реализуемым, обладать внутренней непротиворечивостью и адекватностью. Наиболее перспективными с точки зрения точности обнаружения DDOS атак являются гибридные методы, основанные на использовании алгоритмов искусственного интеллекта. Эффективность методов обнаружения DDOS атак, основанных на гибридном подходе, определяется сочетанием эвристической параметризации входных данных, применения статистического анализа для их обработки и методов искусственного интеллекта.

В третьей главе описан разработанный метод к выявлению вредоносного сетевого трафика, представляющего DDOS атаку, в крупномасштабных сетях на основе математической статистики и искусственного интеллекта, включающий:

– определение набора сетевых параметров протоколов TCP и UDP достаточного для дальнейшего анализа с целью выявления DDOS атак;

– анализ частотно-временных характеристик вейвлет-преобразования с помощью методов математической статистики и искусственного интеллекта за счет проведения машинного обучения с последующим уточнением с применением кластерного анализа, позволяющий провести предварительную выборку потенциально вредоносного сетевого трафика с целью сокращения времени обнаружения и с целью обнаружения DDOS атак в крупномасштабной сети;

Предлагается следующий метод - рассматривать временные интервалы со смещением друг относительно друга так, чтобы в интервале преобладала неизменная часть трафика из предыдущего окна. Так как в определенном интервале времени сетевой трафик протокола одного типа разнороден, атака отказа в обслуживании внесет определенную однородность по ряду параметров. Следовательно, на стыках разнородного потенциально безопасного трафика и однородного потенциально вредоносного трафика происходят всплески частот ДВП, которые и предлагается отслеживать.

Всплески становится легче отследить если интервалы временные вычислять внахлест друг на друга. Таким образом, в результате предобработки исследователь получает набор данных, составленный из окон следующего вида:

$$\text{Окно}_{i+x*offset} = \begin{cases} \text{Временной ряд для параметра}_1 \\ \text{Временной ряд для параметра}_2 \\ \text{Временной ряд для параметра}_3 \end{cases}, \qquad (1)$$

где i – номер окна, $offset$ – смещение по времени, x – номер смещения.

Таким образом, если временной интервал выбран в 10сек, а смещение в 5сек, то будут составлены следующие окна:

$$\big[[0\text{сек} - 10\text{сек}], [5\text{сек} - 15\text{сек}]\big],$$
$$\big[[10\text{сек} - 20\text{сек}], [15\text{сек} - 25\text{сек}]\big],$$
$$\ldots$$
$$\big[[\text{n} * 10\ \text{сек} - (\text{n}+1) * 10\ \text{сек}], [\text{n} * 10 + 5\ \text{сек} - (\text{n}+1) * 10 + 5\ \text{сек}]\big], \quad (2)$$
$$\ldots$$

При этом группировка данных должна быть выполнена по первому интервалу, так как именно относительно данного смещения рассматривается динамика изменения состава трафика.

Затем каждая полученная последовательность подается на вход дискретному вейвлет-преобразованию, на выходе из которого наибольший интерес представляют коэффициенты детализации,

$$S(t_i) = \sum_{k=1}^{2^{N-M}} a_{M,k}\varphi_{M,k}(t_i) + \sum_{m=1}^{M}\sum_{k=1}^{2^{N-M}} d_{m,k}\,\psi_{m,k}(t_i), \qquad m,k \in I, \qquad (3)$$

где $\varphi_{M,k}(t_i)$ – базисная масштабирующая функция, $\psi_{m,k}(t_i)$ – базисная вейвлет-функция, $a_{M,k}$, $d_{m,k}$ – аппроксимирующие и детализирующие коэффициенты, m,k – параметры масштаба и сдвига в пространстве целых чисел I, N – максимальный уровень разложения.

Для того, чтобы охарактеризовать поведение сетевого трафика в заданном временном окне предлагается отслеживать степень зависимости разных параметров сетевого пакета. В качестве метрики, позволяющей определять данную степень зависимости, может быть использован коэффициент множественной корреляции, который для последовательностей x,y,z вычисляется по следующей формуле:

$$R_{y(x,z)} = \sqrt{\frac{r_{xy}^2 + r_{zy}^2 - 2 * r_{xy} * r_{zy} * r_{xz}}{1 - r_{xz}^2}}\,, (4)$$

где r_{xy}, r_{zy}, r_{xz} – парные коэффициенты корреляции, которые вычисляются следующим образом:

$$r_{xy} = \frac{\sum(x_i - < x >) * (y_i - < y >)}{\sqrt{\sum(x_i - < x >)^2 * \sum(y_i - < y >)^2}} \quad (5)$$

Отклонение коэффициента множественной корреляции $R_{y(x,z)}$ от порогового значения указывает на наличие в сетевом трафике аномалии. Чем теснее связаны сетевые пакеты на исследуемом интервале, тем выше значение коэффициента множественной корреляции, тем меньше вероятность наличия DDOS атаки на данном интервале. Данный выбор обусловлен высокой вероятностью изменения значений коэффициентов множественной корреляции на стыках трафика с атакой и без.

Таким образом, данное исследование демонстрирует возможность обнаружения DDOS атак, составляющих не менее 15% от анализируемого временного интервала сетевого трафика.

На основании данного заключения, предлагается использовать методы искусственного интеллекта с целью применения алгоритмов машинного обучения для создания адаптивной модели обнаружения DDOS атак.

Для того, чтобы применить методы машинного обучения, необходимо унифицировать число параметров - коэффициентов множественной корреляции - внутри каждого временного интервала. Данные коэффициенты сгруппированы по временным интервалам, но внутри временного интервала может находиться различное число коэффициентов в зависимости от интенсивности сетевого трафика. Для того, чтобы унифицировать трафик в рамках каждого временного окна, предлагается использовать среднеквадратичное отклонение над заданными интервалами. СКО определяется следующей формулой:

$$\mathrm{S} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2}\,, (6)$$

где $\bar{x}$ – среднее арифметическое выборки, определяемое следующей формулой:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i\,, (7)$$

Унифицированные данные предлагается использовать для обучения искусственного интеллекта, применяя алгоритм кластеризации К-средних. В данном алгоритме определяются центры кластеров с наибольшим числом элементов сконцентрированных в данной области, и далее алгоритм стремится минимизировать суммарное квадратичное отклонение точек кластеров от центров этих кластеров по следующей формуле:

$$\mathrm{V} = \sum_{i=1}^{k}\sum_{x\epsilon S_i}(x - \mu_i)^2\,, (8)$$

где k – число кластеров, S - полученные кластеры, μ_i центры всех масс векторов x из кластера S_i.

Предлагаемый метод состоит из двух итераций и представлен на рисунке 1.

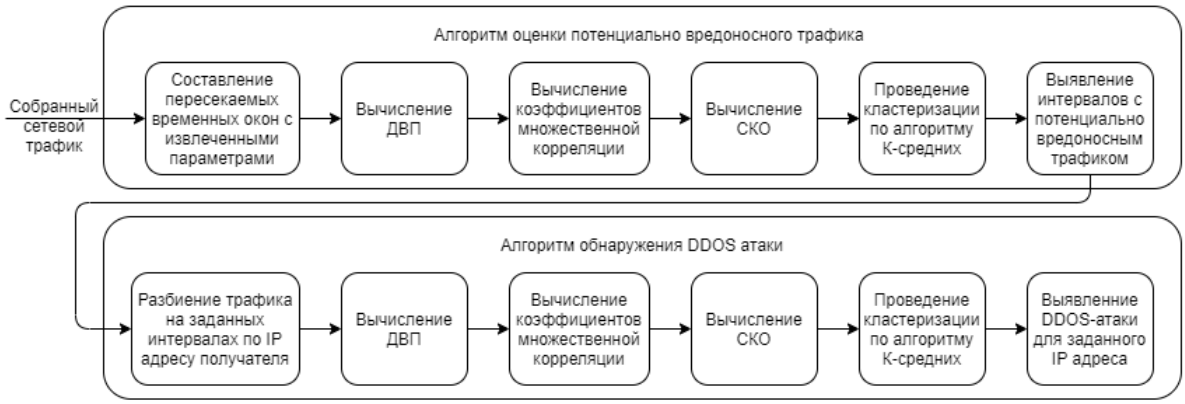


Рисунок 1 - Общая схема предложенного метода обнаружения DDOS атак

Первая итерация позволяет вычислить в магистральных сетях участки всплесков в сетевом трафике. Так как первая итерация позволяет определить потенциально вредоносный трафик, а, следовательно, DDOS атаку, то на второй итерации разбиение подозрительных временных интервалов сетевого трафика по IP-адресам получателя позволяет дифференцировать выборку относительно предполагаемой жертвы. Во время выполнения второй итерации на обнаруженных участках трафик сортируется по IP-адресам получателей и снова происходит отбор параметров, вычисление ДВП, коэффициентов множественной корреляции, приведение к СКО и запуск алгоритма K-средних. Данная итерация позволяет отбросить большинство ложноположительных всплесков, которые могут появиться в основном в UDP трафике.

Следует отметить, что вычисление СКО используется для унификации параметров для второй итерации, так как по различным IP-адресам интенсивность трафика может различаться, из-за чего на различных интервалах может получиться различное число коэффициентов, в то время как кластеризацию необходимо проводить для равного числа параметров. Тем не менее для унификации модели на каждой итерации выполняются одинаковые шаги.

Данный метод основан на извлечении частотно-временных характеристик сетевых параметров из крупномасштабных данных и их объединении в рамках временных интервалов с помощью вычисления коэффициентов множественной корреляции для выявления первичных потенциально вредоносных составляющих крупномасштабного сетевого трафика с целью повышения производительности работы системы. Чем теснее связаны коэффициенты уровня разложения вейвлет-преобразования, тем выше значение коэффициента множественной корреляции, тем меньше вероятность наличия DDOS атаки на данном интервале. Полученные статистические оценки временных интервалов

анализируются искусственным интеллектом с применением алгоритма кластерного анализа. Данный этап позволяет определить временной интервал, содержащий потенциально вредоносный DDOS трафик, объем которого не менее 15% от общего трафика в данном временном интервале.

Далее выявленные потенциально вредоносные временные интервалы разбиваются относительно атакуемых получателей данных и также анализируются их статистические оценки временных интервалов искусственным интеллектом с применением алгоритма кластерного анализа с целью уточнения обнаружения DDOS атаки в крупномасштабных сетях.

Таким образом, в данной главе представлен и теоретически обоснован метод обнаружения DDOS атак в крупномасштабных сетях.

В четвертой главе описана модульная архитектура спроектированного экспериментального макета системы обнаружения DDOS атак в крупномасштабных сетях и блок адаптации, обеспечивающий коррекцию параметров выполнения метода обнаружения DDOS атак в крупномасштабных сетях относительно изменений интенсивности сетевой нагрузки и разнородности сети.

Алгоритм адаптации выполняет важную задачу анализа текущей сетевой нагрузки для коррекции выполнения метода обнаружения DDOS атак в крупномасштабных сетях, а именно: коррекция временных интервалов анализа сетевых данных, коррекция соотношения пересекаемых временных окон, коррекция извлекаемых сетевых параметров, коррекция уровня разложения вейвлет-преобразования. Регулярное изменение данных параметров является важной задачей в связи постоянной изменчивостью разнородности и интенсивности сетевого трафика и обусловлено повышением достоверности обнаружения DDOS атак в крупномасштабных сетях в динамике. На рисунке 2 представлена общая архитектура работы предлагаемого метода обнаружения с учетом модуля адаптации.

Представлены результаты тестирования разработанного макета на сформированной выборке сетевого трафика. Полученные экспериментальные результаты подтверждают эффективность предложенных методов, демонстрируя высокий процент вероятности обнаружения атаки.

На рисунке 3 представлены фрагменты результатов для UDP и TCP трафика на этапе первой итерации. Данный этап позволяет определить временной интервал, содержащий потенциально вредоносный DDOS трафик, объем которого не менее 15% от общего трафика в данном временном интервале.

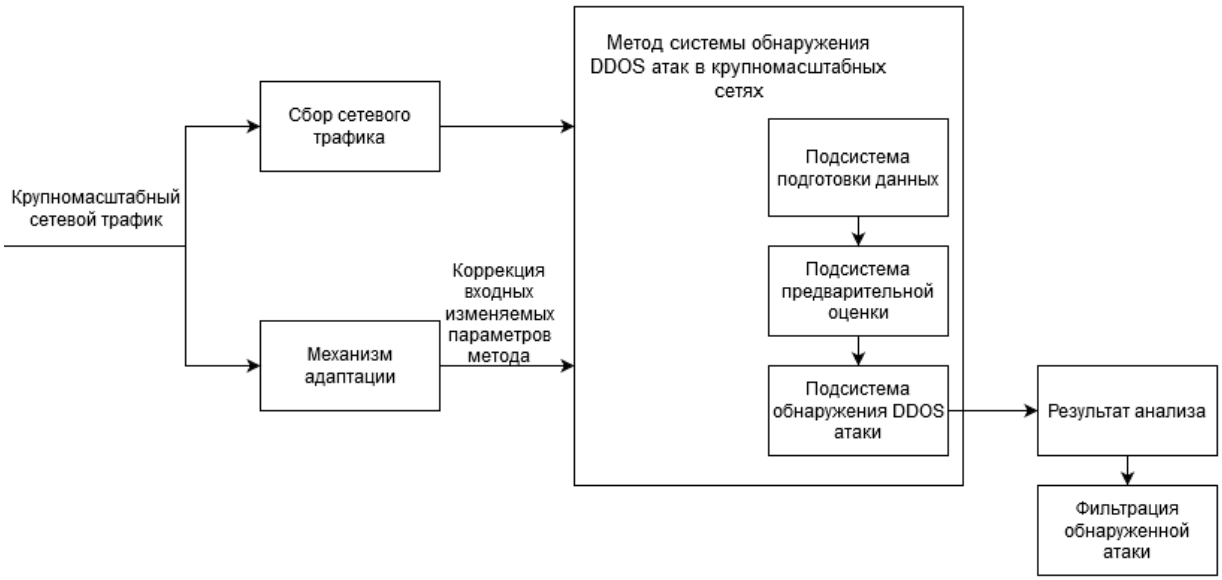
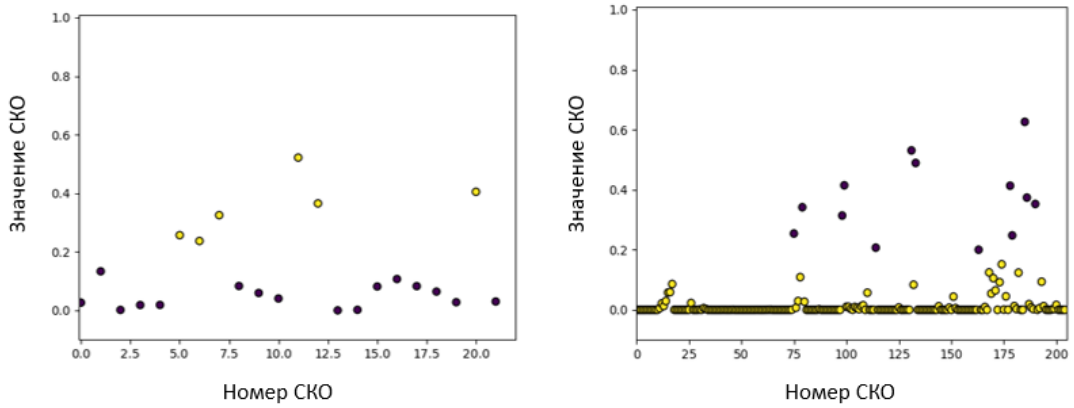


Рисунок 2 - Архитектура предлагаемого метода

На рисунке 4 представлен график примера второй итерации с определением IP-адреса получателя, на которого совершается атака. Полученные потенциально вредоносные временные интервалы разбиваются относительно атакуемых адресов с целью уточнения обнаружения DDOS атаки в крупномасштабных сетях. На данном этапе атака обнаруживается однозначно.

При анализе TCP трафика вероятность обнаружения атаки составляет 98.2% (TP), 1.8% ложноотрицательных (FN). При анализе UDP трафика вероятность обнаружения атаки составляет 97.3% (TP), 0.7% ложноотрицательных (FN) и 2% ложноположительных (FP).



a) UDP b) TCP

Рисунок 3 – Фрагменты результатов для первой итерации предложенного метода

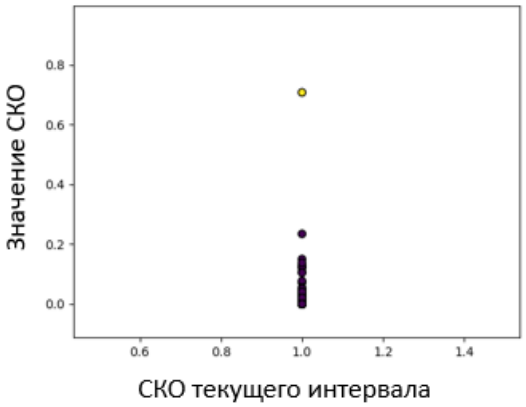


Рисунок 4 – График определения IP-адреса получателя, на который совершается атака

Ниже приведена сравнительная таблица различных методов обнаружения DDOS атак. Основным критерием отбора существующих методов являлась масштабируемость. Анализ демонстрирует отсутствие общего метода, позволяющего с одинаковой эффективностью обнаруживать различные типы DDOS атак на различных наборах данных.

Также данные сравнительные методы, в отличие от предложенного метода, не удовлетворяют следующим требованиям:

1. Адаптация к постоянному изменению сетевой нагрузки в крупномасштабных сетях.
2. Адаптация к постоянному изменению уровня разнородности сетевого трафика.

Таблица 1 – Сравнительная таблица различных методов обнаружения DDOS атак.

Название методов	**TCP трафик**			**UDP трафик**		
	TP	**FN**	**FP**	**TP**	**FN**	**FP**
Предлагаемый алгоритм на основе методов математической статистики и искусственного интеллекта	**98.2**	**1.8**	**0**	**97.3**	**0.7**	**2**
Алгоритм на основе фильтрации параметров	86.81	3.1	10.1	87.67	3.23	9.1
Фильтрация + анализ потоков	91	2.2	6.8	87.67	3.23	9.1
Фильтрация + статистический анализ	91.9	1.1	7.0	98.19	0.63	1.18
Модель принятия решений	-	-	-	97.4	2.4	
Статистический SYN анализ	93-95	5-7		-	-	-

Применение разработанного прототипа системы обнаружения DDOS атак в крупномасштабных сетях на сформированном сетевом трафике

продемонстрировало факт обнаружения атаки, при условии, что атакующим трафиком являлось лишь 15% сетевых пакетов. Полученные экспериментальные результаты подтверждают эффективность предложенного метода и разработанных методов и алгоритмов, демонстрируя эффективное обнаружение DDOS атак в крупномасштабных сетях.

Скорость работы данного метода при параллельном использовании на 16-ти ядрах и загрузкой крупномасштабного сетевого трафика в оперативную память не превышает 34 секунд.

Таким образом, в данной главе представлен механизм адаптации предложенного метода, его архитектура, результаты экспериментальных исследований и проведена сравнительная оценка достоверности обнаружения DDOS атак.

В заключении приведены основные результаты и выводы, полученные в ходе выполнения работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

В результате диссертационного исследования предложен метод обнаружения вредоносного сетевого трафика, составляющего DDOS атаку, в крупномасштабных сетях. Получены следующие основные результаты:

1. Предложен и теоретически обоснован метод обнаружения DDOS атак в крупномасштабных сетях на основе отобранных параметров сетевых пакетов с использованием вейвлет-преобразования, методов математической статистики и проведения машинного обучения с последующим уточнением с применением кластерного анализа. Данный метод основан на сокращении объема информации и времени анализа без снижения достоверности обнаружения DDOS атак в крупномасштабных сетях. Данный метод использован в программе для ЭВМ и зарегистрирован Федеральной Службой по Интеллектуальной Собственности под номером №2018660604.
2. Разработан алгоритм адаптации, обеспечивающий коррекцию параметров выполнения метода обнаружения DDOS атак в крупномасштабных сетях относительно изменений интенсивности сетевой нагрузки и разнородности сети.
3. Осуществлена оценка достоверности обнаружения DDOS атак.
4. Впервые предложено использовать сочетание методов математической статистики и искусственного интеллекта для решения задачи определения вредоносного сетевого трафика в крупномасштабных сетях.
5. Разработана архитектура системы обнаружения DDOS атак с применением принципа модульности и проведены экспериментальные исследования эффективности его применения для выявления угроз безопасности в крупномасштабных сетях.

Предполагается проведение дальнейших исследований по интеграции разработанной системы обнаружения распределённых атак отказа в обслуживании в крупномасштабных сетях в жизненный цикл функционирования крупномасштабных сетей, включая дальнейшее уменьшение времени задержки от сбора трафика до выдачи результата анализа.

СПИСОК РАБОТ, ОПУБЛИКОВАННЫХ ПО ДИССЕРТАЦИИ:

Публикации в изданиях, рецензируемых ВАК:

1. Лаврова Д.С. Анализ безопасности на основе контроля зависимостей параметров сетевого трафика с использованием дискретного вейвлет-преобразования / Лаврова Д.С., **Алексеев И.В**., Штыркина А.А. // Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 2. – С. 9-15.
2. **Алексеев И.В**. Обнаружение распределенных атак отказа в обслуживании в крупномасштабных сетях на основе методов математической статистики и искусственного интеллекта / **Алексеев И.В.** // Проблемы информационной безопасности. Компьютерные системы. - 2020. - № 2 (42). - С. 46-52.
3. **Алексеев И.В**., Классификация уязвимостей сетевых протоколов на основе спецификаций / **Алексеев И.В**., Зегжда П.Д. // Проблемы информационной безопасности. Компьютерные системы. – 2020. – № 1. – С. 24-32.

Публикации в других изданиях:

Патенты и свидетельства:

4. Зегжда П.Д. Программа для анализа безопасности на основе контроля зависимостей параметров сетевого трафика с использованием дискретного вейвлет-преобразования / Зегжда П.Д., Лаврова Д.С., **Алексеев И.В.** // Свидетельство о регистрации программы для ЭВМ RU 2018660604, 27.08.2018. Заявка № 2018617984 от 26.07.2018.

В изданиях, рецензируемых SCOPUS и Web of Science:

5. Lavrova D.S. Security analysis based on controlling dependences of network traffic parameters by wavelet transformation / Lavrova D.S., **Alekseev I.V.,** Shtyrkina A.A. // Automatic Control and Computer Sciences. – 2018. – Т. 52. № 8. – С. 931-935.

В других изданиях:

6. **Алексеев И.В**. Анализ безопасности магистральных каналов связи на основе контроля зависимостей параметров сетевого трафика с использованием дискретного вейвлет-преобразования / **Алексеев И.В**., Зегжда П.Д., Лаврова Д.С., Штыркина А.А. // Методы и технические средства обеспечения безопасности информации. 2018. № 27. С. 16-17.