УДК 004.056

ТЕЗИС ДОКЛАДА «ОБНАРУЖЕНИЕ АТАК В КОМПЬЮТЕРНЫХ СЕТЯХ ПРИ ПОМОЩИ СТАТИСТИЧЕСКОГО МЕТОДА КОНТРОЛЬНЫХ КАРТ CUSUM»

Каримов Н. А.[1] (бакалавр)
Научный руководитель – инженер факультета безопасности информационных технологий Савков С. В.[1]
[1]Университет ИТМО
nik.kolya.karimov@mail.ru

Введение

Обнаружение атак в компьютерных сетях играет важную роль в современной информационной безопасности. Особое внимание стоит уделить атакам типа DDoS (Distributed Denial of Service). Согласно статистике Cloudflare, за первые два квартала 2025 года по всему миру было выявлено 27,8 миллионов атак данного типа. Основная доля случаев такого воздействия (20 миллионов) осуществлялась на сетевом и транспортном уровнях модели OSI (Open Systems Interconnection). Своевременное обнаружение атак данного типа позволит предотвратить нарушение доступности сервисов информационной системы [1].

Существующие системы обнаружения вторжений (СОВ) разделяются на две большие группы: сигнатурные и статистические. Первые используют шаблоны, в которых хранится информация о модификации сетевых пакетов, позволяющих осуществляются атаки. Вторая группа включает себя методы, основывающиеся на анализе объема данных в сети. Сперва создается модель, описывающая поведения пользователей в период отсутствия атак. Во время обнаружения аномалий, числовые характеристики сетевого трафика сравниваются с эталонными значениями. В случае обнаружения существенных отклонений, выводится уведомление о возможной атаке. Таким образом, целью работы является повышение точности обнаружения атак в компьютерных сетях.

Основная часть

В рамках данной работы реализуется метод контрольных карт кумулятивных сумм (CUSUM). Данный выбор обусловлен накопительной характеристикой данного способа. Метод обладает возможностью обнаружения атак, характеризующихся различной скоростью отправки вредоносного трафика. Реализуется алгоритм обнаружения атак, а также программный модуль, реализующий этот алгоритм.

Разрабатываемый алгоритм включает две фазы: вычисление эталонных параметров и обнаружение атак.

Определение величин в период отсутствия атак осуществляется на основании стандарта «ГОСТ Р ИСО 7870-4-2023 Статистические методы. Контрольные карты. Часть 4. Карты кумулятивных сумм» [2]. Требуется сбор не менее 125-ти элементов выборки без отметок об аномалиях. Обнаружение аномалий во время данного периода осуществляется с помощью 3-х внешних СОВ. Считается, что период содержит аномалию, если было получено соответствующие уведомление не менее чем от 2-х систем обнаружения вторжений. В случае, если во время сбора эталонных величин атак обнаружено не было, сохраняются стандартные значения величин CUSUM. Иначе, для всех возможных значений параметров вычисляются кумулятивные суммы и выдвигаются предположения об атаках. Полученные данные сравниваются с реальными отметками об атаках. На основании чего для всех значений вычисляется метрика AUC. Набор данных с наибольшей соответствующей величиной используется для обнаружения.

На протяжении всего процесса обнаружения на основе эталонных значений вычисляются кумулятивные суммы. Вычисление осуществляется как для общего объема трафика, так и для данных в среднем по IP-адресам. Критерием для обнаружения атаки является одновременное превышение пороговых значений, установленных для обоих видов агрегации.

Был реализован программный модуль на языке программирования C++. Он реализует сбор сегментов TCP с флагами SYN, ACK и RST. Эти данные используются для выявления аномалий на основе разработанного алгоритма.

Для тестирования была разработана среда эмуляции на языке программирования Python. Моделирование атак осуществлялось с помощью утилиты hping3.

Выводы

В ходе тестирования программного модуля было проведено 360 тестов, в 120 из которых реализовывались атаки SYN, ACK и RST flood. Для получения более точного результата данные воздействия воспроизводились с различной частотой отправки вредоносных сегментов. По результатам тестов были вычислены такие величины, как: достоверность, точность, полнота, метрика f1 (среднее гармоническое между точностью и полнотой). Те же величины, основываясь на проведенных тестах, были рассчитаны для СОВ Snort, Suricata и Zeek. Разработанный алгоритм продемонстрировал наилучшие показатели по каждой характеристике. Заявленная цель работы достигнута: точность обнаружения атак в компьютерных сетях увеличена относительно существующих программных решений.

Литература

1. DDoS threat report for 2025 Q1 [Электронный ресурс]. — Режим доступа: https://radar.cloudflare.com/reports/ddos-2025-q1 (Дата обращения: 20.02.2026).
2. ГОСТ Р ИСО 7870-4-2023. Статистические методы. Контрольные карты. Часть 4. Карты кумулятивных сумм. Введ. 01.03.2024. М.: Российский институт стандартизации, 2023.