

ПРОГНОЗИРОВАНИЕ DDoS-АТАК С ИСПОЛЬЗОВАНИЕМ ГРАДИЕНТНОГО БУСТИНГА

**Осипенко А.В., Устинов С.А., студенты 5 курса факультета
безопасности**

**Научный руководитель – Немирович-Данченко М.М., доктор
физико-математических наук, профессор
ФГБОУ ВО «Томский государственный университет систем
управления и радиоэлектроники»**

Ключевые слова: DDoS-атаки, прогнозирование, машинное обучение, градиентный бустинг, MSE.

Данная работа рассматривает тренды DDoS-атак в 2022-2023 годах. Реализовано прогнозирование DDoS-атак с помощью градиентного бустинга, среднеквадратичная ошибка модели составила 0.000183. Полученные результаты могут помочь в разработке новых методов защиты от кибератак.

Введение. В настоящее время одним из самых распространенных видов кибератак являются DDoS-атаки. Если оценивать глобальные тенденции данного вида атак в 2023 году, можно обратиться к материалам StormWall. Данная компания изучала атаки за первое полугодие 2023 года на своих клиентов в различных секторах: финансовом, электронной коммерции, телекоммуникациях, развлечениях, транспорте, образовании и логистике [1]. Из выявленных особенностей можно выделить следующие тренды:

- 1) Заметное увеличение использования ботнетов.
- 2) Повышение на 136% количества многовекторных атак. Хакеры нацелены на несколько уровней сети одновременно, стремясь нанести максимальный ущерб.
- 3) Сдвиг в целевых секторах. Киберпреступники ориентированы на ключевые отрасли (финансы, развлечения, телекоммуникации, государственные системы, здравоохранение, транспорт).

Так, например, в отчете отмечается значительный рост DDoS-атак на государственные службы. Данный сектор столкнулся с увеличением атак на 168% за год, что является рекордным значением. Под атаками оказались государственные учреждения в различных странах, включая Россию, Польшу, Швейцарию, Германию и США.

Цель работы. Так как DDoS-атаки могут приводить к серьезным финансовым потерям и ущербу репутации для организаций, необходимо научиться сводить их последствия к минимуму. Сделать это можно с помощью прогнозирования, которое позволяет заранее определить возможные угрозы и принять меры для их предотвращения.

В данной работе используется один из методов машинного обучения (МО), а именно градиентный бустинг. Основная идея данного алгоритма заключается в последовательном применении предсказателя, при этом каждая последующая модель минимизирует ошибку предыдущей [2].

Результаты исследования. В работе использовалась статистика, предоставляемая международной компанией «Лаборатория Касперского» [3]. В результате сбора данных был сформирован временной ряд «DDoS-атаки по дням», состоящий из 822 значений с ежедневными наблюдениями с 1 июля 2020 года по 30 сентября 2022 года (рисунок 1).

В контексте использования фреймворка LightGBM для прогнозирования были использованы следующие библиотеки: lightgbm, mean_squared_error, matplotlib.pyplot, MinMaxScaler. После загрузки временной ряд был разделен для обучения и тестирования модели в соотношении 80%:20%. Таким образом, для обучения градиентный бустинг использовал первые 660 значений от исходного набора данных, а на оставшихся 162 наблюдениях делал прогноз, опираясь на значения, полученные во время обучения.

Также особенностью данной реализации стало то, что модель делает предсказания, основываясь не на всех имеющихся данных, а опираясь только на 14 соседних значений (lookback = 14). Такое введение позволяет модели прогнозировать будущие наблюдения как можно точнее. Количество итераций (деревьев) в модели было взято 100. Экспериментальным путем было выявлено, что именно при таком значении модель ошибается минимально. Из корректируемых

параметров настраивались следующие: 'num_leaves': 5, 'learning_rate': 0.1, 'feature_fraction': 1.0.



Рис. 1 – Временной ряд «DDoS-атаки по дням»

Результаты после окончательной настройки градиентного бустинга, обучения модели и тестирования представлены на рисунке 2.

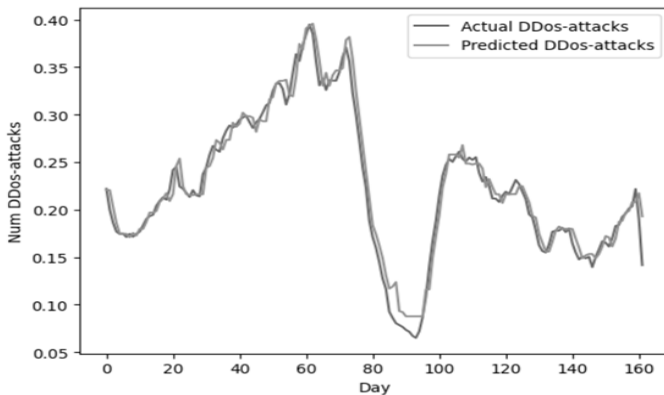


Рис. 2 – Прогнозирование на тестовом наборе данных

В результате работы градиентного бустинга среднеквадратичная ошибка (MSE) временного ряда составила 0.000183. В таблице 1 представлены результаты расчета MSE.

Таблица 1 – Результаты расчета MSE для ряда «DDoS-атаки по дням»

Модель	MSE (нормализованное)	Обратная нормализация	Прогноз на будущее (1 день)
Градиентный бустинг	0,000183	51 единица	577 единиц

Для лучшего понимания полученное нормализованное значение ошибки было обратно переведено в исходный формат. Таким образом, рассматриваемый метод МО в среднем ошибается на 51 единицу, что само по себе не является критичным значением, так как в исходном временном ряду есть дни, в которых наблюдалось порядка 3500 DDoS-атак. Также, опираясь на полученные результаты, можно предположить, что прогнозным значением на будущее, а именно на 1 октября 2022 года, будет 577 DDoS-атак.

Заключение. В результате исследования было реализовано прогнозирование DDoS-атак с помощью градиентного бустинга, который в дальнейшем может быть использован для анализа трафика и выявления аномальных паттернов, указывающих на возможную кибератаку. Благодаря данному факту, можно своевременно принимать меры по защите сети. Кроме того, такой способ прогнозирования может помочь в разработке новых методов защиты от DDoS-атак, что является актуальной задачей в сфере информационной безопасности.

Библиографический список:

1. Обзор за 2 квартал 2023 года: отчет StormWall о DDoS-атаках.
– URL: <https://stormwall.network/ddos-report-stormwall-q-2-2023> (дата обращения 12.01.2024).

2. A Detailed Guide On Gradient Boosting Algorithm With Examples.
– URL: <https://www.analytixlabs.co.in/blog/gradient-boosting-algorithm/> (дата обращения: 13.01.2024).

3. Отчеты о DDoS-атаках. – URL: <https://securelist.ru/category/ddos-reports/> (дата обращения: 13.01.2024).

FORECASTING DDOS-ATTACKS USING GRADIENT BOOSTING

Osipenko A.V., Ustinov S.A., 5th year students of the Faculty of Security

Scientific supervisor – Nemirovich-Danchenko M.M., Doctor of Physical and Mathematical Sciences, Professor

Tomsk State University of Control Systems and Radioelectronics

Keywords: *DDoS-attacks, forecasting, machine learning, gradient boosting, MSE.*

This work examines the trends of DDoS-attacks in 2022-2023. The prediction of DDoS-attacks using gradient boosting was implemented. The MSE of the model was 0.000183. The results obtained can help in the development of new methods of protection against cyber attacks.