Алгоритмы машинного обучения в противодействии атакам отказа в обслуживании

А.С. Соколов

МИРЭА - Российский технологический университет

Аннотация: В статье рассматриваются современные алгоритмы машинного обучения, применяемые для обнаружения и предотвращения атак отказа в обслуживании. В работе анализируются различные подходы, такие как классификация трафика, аномалия в поведении системы и анализ сетевых пакетов, которые позволяют авторам разработать систему раннего предупреждения о возможных атаках. Также обсуждаются перспективы применения машинного обучения для обеспечения более надежной защиты сетевой инфраструктуры по результатам проведенных экспериментов. Результаты работы представляют большую научную и практическую ценность для специалистов в сфере кибербезопасности и в моделировании систем защиты.
Ключевые слова: информационная безопасность, отказ в обслуживании, машинное обучение, сетевой трафик.

Введение

В современном мире с ростом повсеместной цифровизации и развитием технологий, появляются новые возможности осуществить атаки на все компоненты информационных систем. Атакой, которая будет служить иллюстрацией такой угрозы, является DDoS. Она нацелена на нарушение работы выбранного в качестве цели ресурса путем его перегрузки [1] многочисленными запросами.

Стандартные методики противодействия атакам обслуживания, которые включают в себя фильтрацию трафика и изменение масштабов инфраструктуры, в современных условиях показывают недостаточную эффективность в связи с разнообразием и сложностью применяемых атак. Поэтому особое место на рынке решений занимают продукты, основанные на технологиях машинного обучения.

Машинное обучение предоставляет новаторский подход к определению и предотвращению DDoS-атак. Созданные посредством анализа больших объемов данных и компиляции сигнатур, такие технологии призваны решать комплексные задачи в обеспечении доступности ресурсов. В данной работе

выполнен анализ основных методологических практик и алгоритмов машинного обучения для того, чтобы найти их преимущества и недостатки. Кроме того, выполнена программная реализация одного из алгоритмов ML [2] в качестве возможного решения задачи классификации сетевого трафика, что особенно актуально в современной технологической сфере.

DDoS-атака направлена на то, чтобы сделать недоступным для пользователей онлайн-сервис путем его перегрузки трафиком из множества источников [3]. Данный тип атаки подразделяется на три категории: атаки на уровне сети, атаки на уровне приложений, а также комбинированные атаки.

Для осуществления атак отказа в обслуживании злоумышленники используют ботнеты – объединенные в одну или несколько сетей зараженные устройства, которые служат для организации удаленных координированных атак.

При успешной реализации подобных инцидентов информационной безопасности, последствиями атак отказа в обслуживании чаще всего являются серьезные финансовые убытки, нарушение бизнес-процессов [4-5], простой сервиса, потерю данных, а также большой репутационные ущерб.

Машинное обучение для противодействия кибератакам

Машинное обучение – одно из подмножеств раздела искусственного интеллекта, которое направлено на разработку алгоритмов и поиск закономерностей. Обучение моделей ML происходит на больших объемах данных, на основе которых, в дальнейшем модель сможет делать прогнозы.

Методы машинного обучения могут помочь не только в распознавании имеющихся угроз, но также в поиске неизвестных ранее атак. Их способности к анализу больших объемов данных в реальном времени делает их незаменимыми в современных системах кибербезопасности. Применение этих алгоритмов позволяет организациям выстроить надежные защитные

механизмы, которые способны противостоять эволюционирующим киберугрозам.

Одним из ключевых аспектов использования технологий машинного обучения в вопросе решения задачи классификации сетевого трафика является выбор алгоритмов и методов предварительной обработки данных.

На теоретическом уровне алгоритм можно определять исходя из источника данных и целей анализа. Алгоритмы классификации часто используются для анализа сетевого трафика из-за их возможностей обрабатывать большое количество признаков и выявлять сложные паттерны, характерные для атак отказа в обслуживании.

Экспериментальная часть

Для реализации модели классификации сетевого трафика выбран набор данных под названием «DDOS Attack Network Logs» с одного из самых больших онлайн-репозиториев наборов данных «Kaggle.com». В наборе данных содержится около 2 100 000 помеченных сетевых журналов различных типов сетевых атак. В базу данных входят следующие типы сетевых атак [6]: UDP-Flood, Smurf, SIDDOS, HTTP-FLOOD, а также обычный трафик.

Набор данных представлен в виде файла с названием «final-dataset.arff». Расширение ARFF — расширение файлов, в которых находятся данные в машинно-читаемом формате, который часто используется в области обработки данных и машинного обучения.

На этапе предобработки данных нужно убедиться, что все данные имеют правильный формат для анализа и моделирования. Используя функцию «countplot» из библиотеки Seaborn построим диаграмму, на которой можно увидеть, какие классы пакетов преобладают в данных. Построение данной диаграммы изображено на рис.1. Например, если на графике наблюдается значительное преобладание одного класса, это может указывать

на несбалансированность данных, что важно учитывать при построении модели машинного обучения. Если в данных много пакетов класса "нормальный" по сравнению с "атакующими", это может повлиять на обучение модели [7-8] и ее способность правильно классифицировать атакующие пакеты.

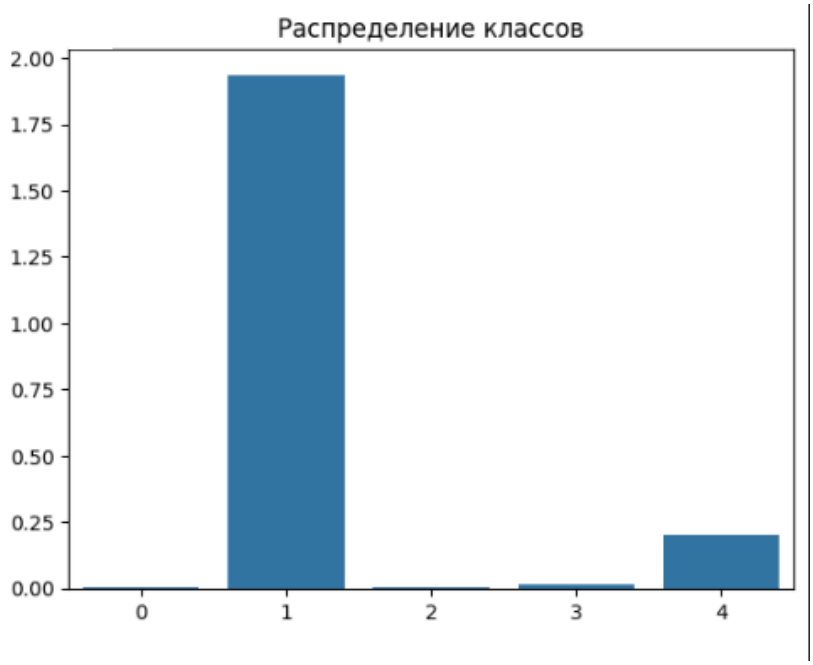

Рис. 1. – Диаграмма распределения классов

Далее была проведена оценка обоснованности анализа на основании построенной корреляционной матрицы. С её помощью можно выявить признаки, которые наиболее взаимозависимы. Если два признака имеют высокую корреляцию, возможно, имеет смысл оставить только один из них, чтобы избежать избыточности данных и улучшить производительность модели. На основе матрицы, представленной на рис.2, из выборки были удалены высоко коррелирующие данные.

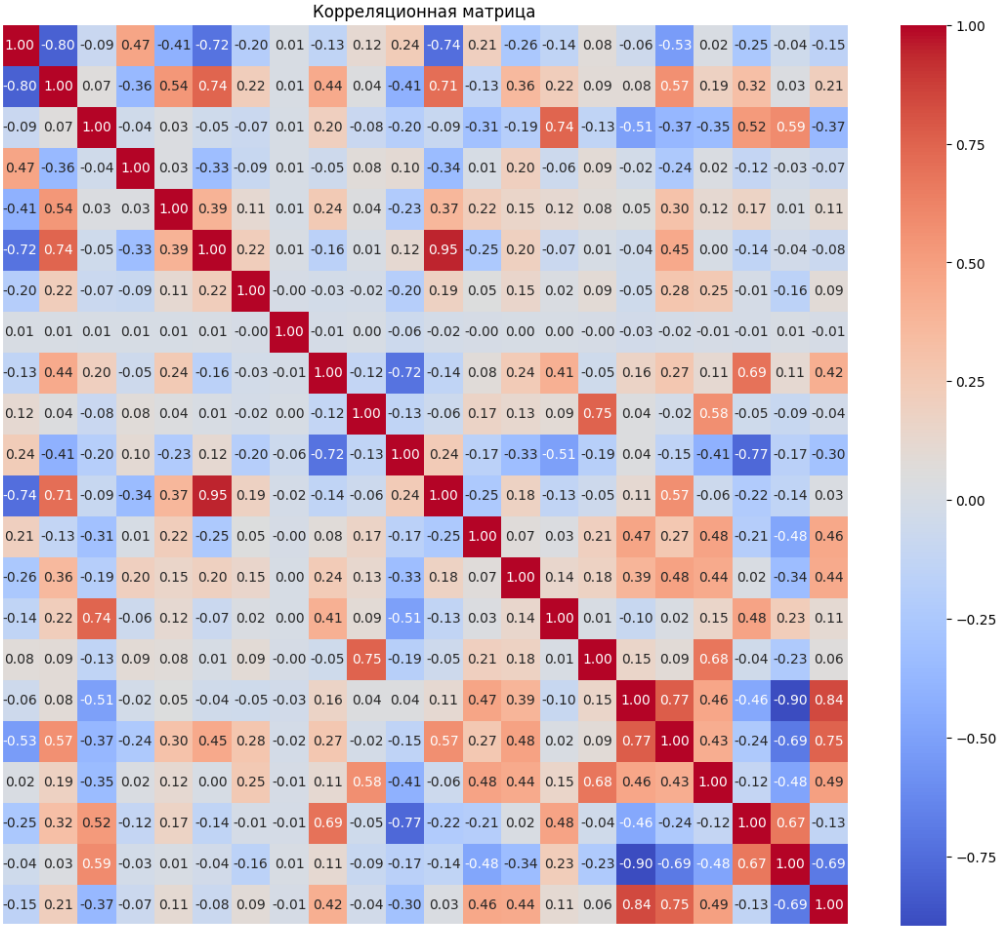

Рис. 2. – Корреляционная матрица

Далее происходит стандартное разделение данных на тренировочный и тестовый наборы с использованием функции «train_test_split». Была создана и обучена модель RandomForestClassifier из библиотеки «scikit-learn». Сначала был создан объект класса «RandomForestClassifier» с параметром n_estimators=100, что указывает на использование 100 «деревьев в лесу». Затем модель была обучена на тренировочной выборке с использованием метода «fit». В процессе обучения модель строит множество решений деревьев [9], чтобы научиться классифицировать сетевой трафик.

Далее нужно программно рассчитать и составить матрицу ошибок. Матрица ошибок представляет собой таблицу, показывающую, сколько раз элементы одного класса были классифицированы как элементы другого

класса. На рис.3 изображены результаты расчета и построения матрицы ошибок.

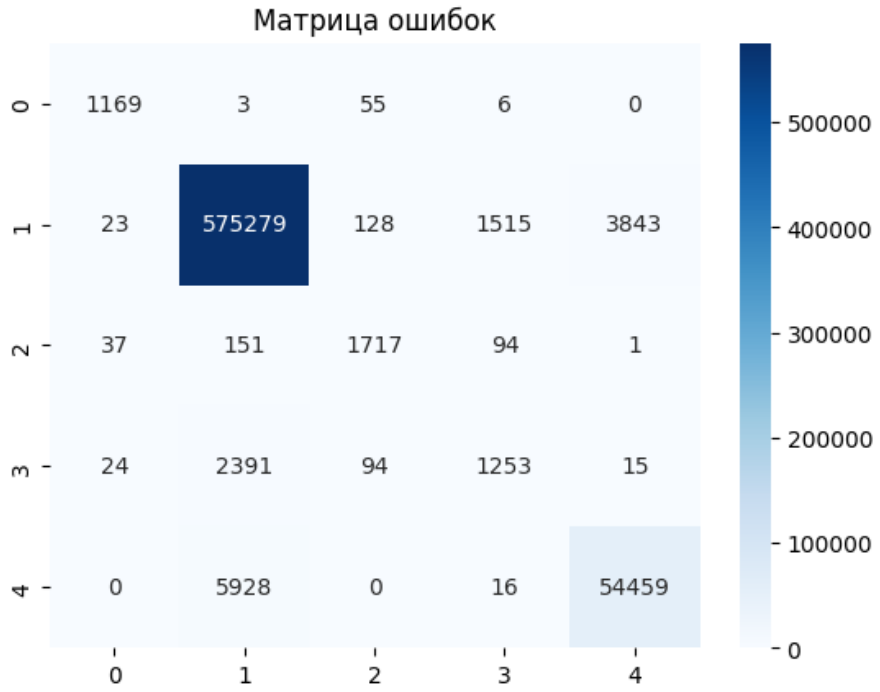

Рис. 3. – Матрица ошибок

На основе полученных результатов эксперимента была построена ROC-кривая для оценки производительности модели классификации. Функция roc_curve служит инструментом вычисления значений ложноположительных и истинноположительных показателей. Функция auc вычисляет площадь под ROC-кривой, которая служит мерой качества классификации. Чем ближе значение AUC к 1, тем качественнее выполняет свою работу модель. В нашем случае модель показала результат 0,94, что является крайне высоким. Результаты построения ROC-кривой показаны на рис.4.

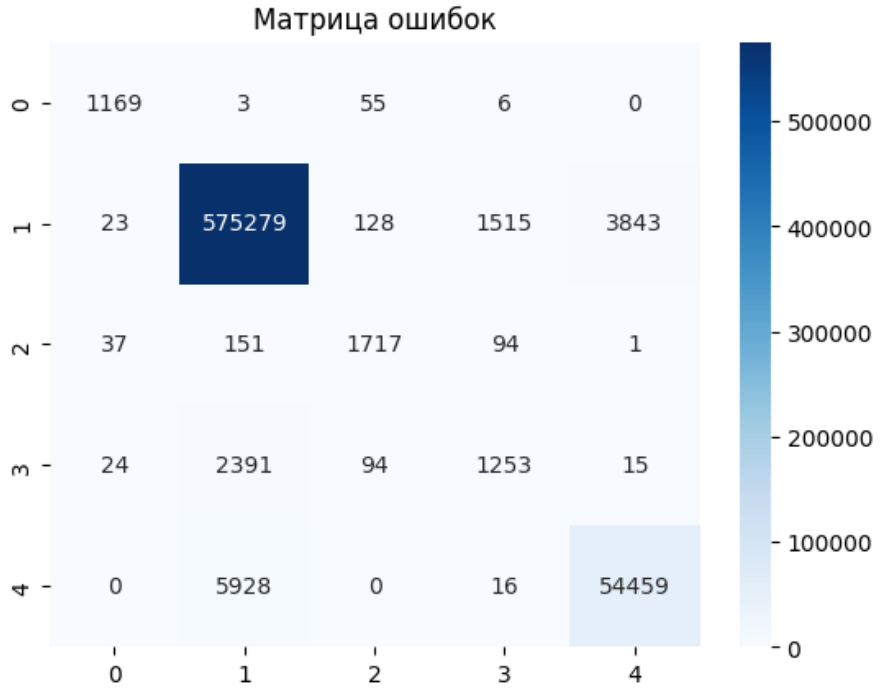

Рис. 4. – ROC-кривая

Заключение

Внедрение технологий машинного обучения для обнаружения DDoS-атак в корпоративной среде существенно повышает уровень безопасности и надежности ИТ-инфраструктуры. В банковском секторе, где безопасность данных имеет первостепенное значение, использование таких моделей позволяет в реальном времени анализировать сетевой трафик и оперативно реагировать на подозрительные активности, предотвращая потенциальные атаки. Аналогично, в телекоммуникационных компаниях машинное обучение помогает обрабатывать огромные объемы данных и быстро идентифицировать аномалии [10], обеспечивая бесперебойное обслуживание клиентов.

В электронной коммерции и государственных учреждениях, где простои и нарушения могут иметь серьезные финансовые и репутационные последствия, системы на основе машинного обучения могут быть интегрированы в существующие средства защиты. Они могут работать в

комплексе с традиционными методами кибербезопасности, такими как брандмауэры или системы обнаружения/предотвращения вторжений.

Внедрение технологий машинного обучения в процесс обеспечения кибербезопасности открывает новые горизонты в области эффективного противодействия атакам отказа в обслуживании. Их важность особенно проявляется в вопросах классификации сетевого трафика и выявления потенциальных угроз.

В процессе выполнения исследования была разработана программа, основанная на технологиях ML для решения задач классификации сетевого трафика, а также выявления атак отказа в обслуживании. Для этого был использован набор данных, который включает в себя различные параметры, собранные при анализе сетевого трафика. На основе результатов и метрик можно сделать вывод о том, что такие модели могут эффективно распознавать аномалии в сетевом трафике, при этом открывая перспективы для их интеграции и внедрения в современные системы обеспечения информационной безопасности.

Литература

1. Brij B. Gupta, Amrita D. Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures // CRC Press, 2021. - 140 с.

2. Гладков А. Н., Горячев С. Н., Кобяков Н. С. Визуализация киберугроз как аспект формирования компетенций в области информационной безопасности // Защита информации. Инсайд. - 2023. - № 1. - С. 32-37.

3. Рыленков Д.А., Карпов Д.С. Разработка интегрального метода оценки уровня защищенности серверной инфраструктуры организации // Инженерный вестник Дона. 2025. №1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9763.

4. DDoS attacks and machine-learning-based detection methods: A survey and taxonomy // Wiley Online Library. URL: onlinelibrary.wiley.com/doi/full/10.1002/eng2.12697 (дата обращения: 30.03.24).

5. Касымов А.А., Лысенко А. Синтез нейронных сетей и системного анализа с применением сократических методов для управления корпоративными ИТ–проектами // Инженерный вестник Дона. 2025. №2. URL: ivdon.ru/ru/magazine/archive/n2y2025/9819.

6. Detecting Denial of Service attacks using machine learning algorithms // SpringerOpen URL: journalofbigdata.springeropen.com/articles/10.1186/s40537-022-00616-0 (дата обращения: 30.03.24).

7. ИИ в кибербезопасности: друг или враг // DDOS-GUARD URL: ddos-guard.ru/blog/ii-v-kiberbezopasnosti (дата обращения: 07.04.24).

8. Что такое DDoS-атака и как от неё защититься? // StormWall URL: stormwall.pro/resources/blog/ddos-ataka-kak-zashchititsya (дата обращения: 08.04.24).

9. Соколов А.С., Шутов В.А. Обеспечение противодействия кибератакам в условиях информационной войны // Информационные системы и технологии. 2023. №№2 2023 (136). С. 122-128.

10. Пучков А. Ю., Соколов А. М., Широков С. С., Прокимнов Н. Н. Алгоритм выявления угроз информационной безопасности в распределенных мультисервисных сетях органов государственного управления // Прикладная информатика. - 2023. - Т. 18, № 2. - С. 85-102.

References

1. Brij B. Gupta, Amrita D. Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures. CRC Press, 2021. 140 p.

2. Gladkov A. N., Gorjachev S. N., Kobjakov N. S. Zashhita informacii. Insajd. 2023. № 1. pp. 32-37.

3. Rylenkov D.A., Karpov D.S. Inzhenernyj vestnik Dona. 2025. №1. URL: ivdon.ru/ru/magazine/archive/n1y2025/9763.

4. DDoS attacks and machine-learning-based detection methods: A survey and taxonomy. Wiley Online Library URL: onlinelibrary.wiley.com/doi/full/10.1002/eng2.12697 (date of reference: 30.03.24).

5. Kasymov A.A., Lysenko A. Inzhenernyj vestnik Dona. 2025. №2. URL: ivdon.ru/ru/magazine/archive/n2y2025/9819.

6. Detecting Denial of Service attacks using machine learning algorithms. SpringerOpen. URL: journalofbigdata.springeropen.com/articles/10.1186/s40537-022-00616-0 (date of reference: 30.03.24).

7. II v kiberbezopasnosti: drug ili vrag [AI in Cybersecurity: Friend or Foe]. DDOS-GUARD. URL: ddos-guard.ru/blog/ii-v-kiberbezopasnosti (date of reference: 07.04.24).

8. Chto takoe DDoS-ataka i kak ot nejo zashhitit'sja? [What is a DDoS attack and how to protect yourself from it?]. URL: stormwall.pro/resources/blog/ddos-ataka-kak-zashchititsya (date of reference: 08.04.24).

9. Sokolov A.S., Shutov V.A. Informacionnye sistemy i tehnologii. 2023. №2 2023 (136). pp. 122-128.

10. Puchkov A. Ju., Sokolov A. M., Shirokov S. S., Prokimnov N. N. Prikladnaja informatika. 2023. T. 18, № 2. pp. 85-102.

Дата поступления: 12.03.2025

Дата публикации: 25.04.2025