УДК 004.056.5 + 004.8 URL: https://ptsj.bmstu.ru/catalog/icec/insec/1051.html

МЕТОД ЗАЩИТЫ СЕРВЕРНОЙ ИНФРАСТРУКТУРЫ ОТ РАСПРЕДЕЛЕННОЙ АТАКИ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ» С ИСПОЛЬЗОВАНИЕМ РЕКУРРЕНТНОЙ НЕЙРОННОЙ СЕТИ

А.А. Сёмина anna290303@yandex.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Современные статистические данные ведущих компаний в области кибербезопасности (Лаборатория Касперского, Cloudflare, Statista) свидетельствуют о 63%-ном росте количества DDoS-атак в 2023–2024 гг. В данной статье рассмотрен инновационный метод противодействия этим угрозам, основанный на применении рекуррентных нейронных сетей (RNN). Разработанное решение обеспечивает автоматизированное обнаружение атак в реальном времени с возможностью мгновенного реагирования, демонстрируя при этом точность классификации на уровне 99,14 % на тестовой выборке из набора NSL-KDD и время предсказания всего 70,12 мс. Особенностью предложенного подхода является адаптивность к новым типам угроз благодаря механизму дообучения модели. Система может быть интегрирована в существующую инфраструктуру клиента без нарушения работы сервисов. Проведенные исследования различных конфигураций RNN (включая анализ влияния длины последовательности, количества нейронов и эпох обучения) позволили достичь оптимального баланса между точностью и производительностью.

Ключевые слова: DDoS-атаки, кибербезопасность, рекуррентные нейронные сети, машинное обучение, защита серверов, NSL-KDD, автоматическое обнаружение атак

Введение. Распределенная атака типа «отказ в обслуживании» (DDoS-атака) относится к типу кибератак, при котором злоумышленники стремятся нарушить работу серверной инфраструктуры, отправляя огромный поток запросов с распределенных источников [1, 2]. Эти атаки нацелены на исчерпание вычислительных и сетевых ресурсов серверной инфраструктуры, что приводит к недоступности сервисов для легитимных пользователей. Три крупнейших компании в области статистики в сфере кибербезопасности (Лаборатория Касперского [3], Cloudflare [4], Statista [5]) отметили увеличение количества DDoS-атак в 2023–2024 гг. как минимум на 63 %.

Таким образом, целью работы является разработка метода защиты серверной инфраструктуры от распределенной атаки типа «отказ в обслуживании» с использованием рекуррентной нейронной сети.

Анализ методов защиты от DDoS-атак. Существующие методы защиты имеют разное время применения, уровень воздействия, разное расположение

 ISSN 2541-8009

механизма в сети [1, 5, 6]. Они включают различные механизмы фильтрации, методы углубленного анализа содержимого, нейронные сети и распределение нагрузки [1, 2, 5, 6]. Однако не все методы защищают от всех типов атак и способны адаптироваться (табл. 1).

Таблица 1. **Сравнение существующих методов защиты от DDoS-атак**

Метод	Преимущества	Недостатки	Расположение механизма	Время применения	Тип атаки	Уровень воздействия	Адаптивность
IP-фильтрация	Простота реализации, подходит для фильтрации атак с небольшим количеством источников	Неэффективен против распределенных атак. Вероятность обхода фильтрации злоумышленником	У источника	После обнаружения атаки	UDP flood	Сетевой уровень	–
Фильтрация по протоколам	Эффективен для защиты от атак, использующих конкретные протоколы	Может блокировать легитимные запросы. Вероятность обхода фильтрации злоумышленником	На промежуточных узлах	После обнаружения атаки	UDP flood, TCP flood	Сетевой и транспортный уровень	–
DPI	Высокая точность фильтрации и возможность выявления сложных атак	Высокие вычислительные затраты и задержки. Вероятность обхода фильтрации злоумышленником	На стороне жертвы	Во время атаки	HTTP flood	Уровень приложений	+
IDS Сигнатурные	Обнаруживает известные атаки с низкой частотой ложных срабатываний	Неэффективен против новых типов атак, ресурсоемкий	На стороне жертвы	Во время атаки	Известные DDoS-атаки	Все уровни	–

Окончание табл. 1

Метод	Преимущества	Недостатки	Расположение механизма	Время применения	Тип атаки	Уровень воздействия	Адаптивность
IDS аномалии	Может выявлять неизвестные атаки	Высокий риск ложных срабатываний	На стороне жертвы	Во время атаки	Любые DDoS-атаки	Все уровни	+
Нейронные сети	Обнаруживает известные и новые атаки с низкой частотой ложных срабатываний	Требует большого объема данных для обучения	На стороне жертвы	До атаки и во время атаки	Любые DDoS-атаки	Все уровни	+
Anycast-сети	Распределение нагрузки на инфраструктуру, высокая отказоустойчивость	Сложная и дорогостоящая инфраструктура	На промежуточных узлах	До атаки	Любые DDoS-атаки	Все уровни	–

На основе данных сравнительной таблицы (табл. 1) можно сделать вывод, что нейросетевой метод оптимален для достижения поставленной цели, поскольку он демонстрирует адаптивность, универсальность для различных типов атак и уровней воздействия, снижает количество ложных срабатываний и не требует значительных финансовых вложений в инфраструктуру по сравнению с другими методами. Это метод также предоставляет возможность не только обнаружения, но и прогнозирования атак.

Решения для защиты от DDoS-атак. Для противодействия DDoS-атакам в 2025 г. применяют несколько решений [8–14]. Недостатки существующих решений в сравнительной таблице (табл. 2) отмечены красным. На общем фоне положительно выделяется решение Касперского. Рост числа атак делает необходимым использование автоматизированных систем. К сожалению, у решения Касперского не предусмотрена возможность автоматизированной реакции на атаку, необходимо круглосуточно доступное лицо или группа лиц клиента. Также допустимое время реакции на атаку любого масштаба составляет не менее 15 мин, что не подходит для некоторых систем: банки, платежные системы, биржи, системы управления воздушным движением, автономные транспортные средства и др.

Приведенные решения являются коммерческими и не предоставляют в полной мере данные об эффективности и задержках при использовании.

 ISSN 2541-8009

Таким образом, необходимо решение с известным уровнем эффективности и временем задержки при использовании, предоставляющее возможность для мгновенной автоматизированной реакции на атаку с возможностью адаптации к новым типам атак.

Таблица 2. **Сравнение существующих решений для защиты от DDoS-атак**

Решение	Защищают от всех типов DDoS-атак	Сертифицировано в России	Эффективность	Есть решение, защищающее только от DDoS	Задержка при анализе	Метод
Kaspersky DDoS Protection	+	+	Не указана	+	Не указана	Анализ аномалий + Экспертная группа
DDoS-GUARD	+	+	Не указана	+	Не указана	Фильтрация трафика
StormWall	Не защищают от атак на уровне приложения	+	Не указана	+	Не указана	Анализ аномалий + фильтрация трафика
bunny.net	+	–	Не указана	–	Не указана	Фильтрация трафика
Cloud4Y	Не защищают от атак на транспортном уровне	–	99,982 %	+	Не указана	Фильтрация трафика + межсетевой экран уровня приложения
NDENIX	+	+	Не указана	–	Время отклика < 20 мс	Фильтрация трафика + анализ HTTP-запросов
Yandex DDoS Protection	+	+	Не указана	–	Не указана	Анализ аномалий

Конфигурация разработанной нейронной сети. Для предсказания атак используются данные сетевого трафика и параметры нормализации — это статистические данные для масштабирования метрик. На выходе получаем ответ на вопрос, есть DDoS-атака или нет. Для работы используется предобученная нейронная сеть, в качестве параметров нормализации использовались данные трафика, помеченные как нормальные.

Рекуррентная нейронная сеть состоит из трех слоев (рис. 1).

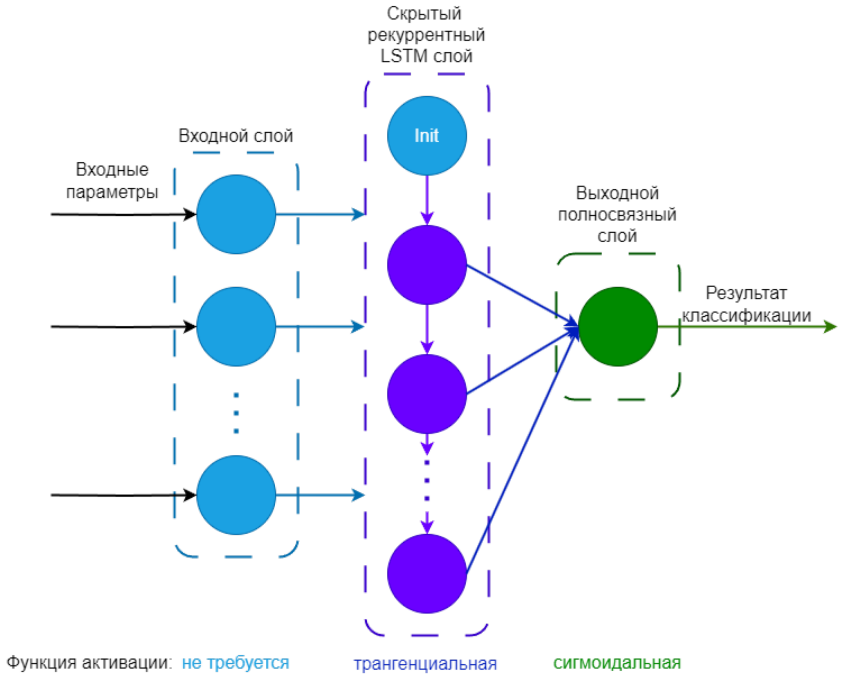

Рис. 1. Конфигурация разработанной рекуррентной нейронной сети

1. Входной слой — принимает сжатый набор входных параметров из выборки NSL-KDD [15]: protocol_type, flag, src_bytes, dst_bytes, count, srv_count, serror_rate, srv_serror_rate, same_srv_rate, dst_host_count, dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_srv_diff_host_rate, dst_host_serror_rate, dst_host_srv_serror_rate, duration, service, rerror_rate, dst_host_rerror_rate, dst_host_srv_rerror_rate, функция активации не требуется.

2. Скрытый слой — рекуррентный слой с тангенциальной функцией активации, 38 нейронов.

3. Выходной слой — полносвязный слой с сигмоидальной функцией активации с одним нейроном.

В качестве метода обучения выбрано обучение с учителем с использованием оптимизации Adam. Для такого метода обучения необходимы тренировочная и тестовая выборки [16], данные для которых были взяты из набора NSL-KDD. Начальные веса нейронов выбираются случайным образом. Количество эпох обучения определяется с помощью метода ранней остановки — во время обучения проверяется, как меняется функция потерь на валидационной выборке. Если показатели ухудшаются в течение нескольких эпох, это

 ISSN 2541-8009

значит, что нейросеть начала переобучаться; процесс обучения автоматически завершается с восстановлением лучших весов. В качестве функции потерь выбрана бинарная кросс-энтропия.

Рекуррентная нейронная сеть работает с последовательностями данных, оптимальная длина последовательности 10. Оптимальный набор входных параметров, количество нейронов в скрытом слое и длина последовательности определялись с помощью исследования.

Программная реализация разработанного метода. Реализованное программное обеспечение (ПО) имеет два варианта использования. Первый — с использованием графического интерфейса (рис. 2) для удобного ознакомления с методом защиты, изучения его возможностей, наглядной демонстрации работы программы, возможности тестирования и дообучения выбранной модели без привлечения дополнительных специалистов. В самом графическом интерфейсе не предусмотрена возможность выбора модели для работы. Но, при необходимости, используя файл конфигурации, можно изменить соответствующие настройки, и работа приложения будет осуществляться с другой моделью или для тестирования будет использоваться другой набор данных.

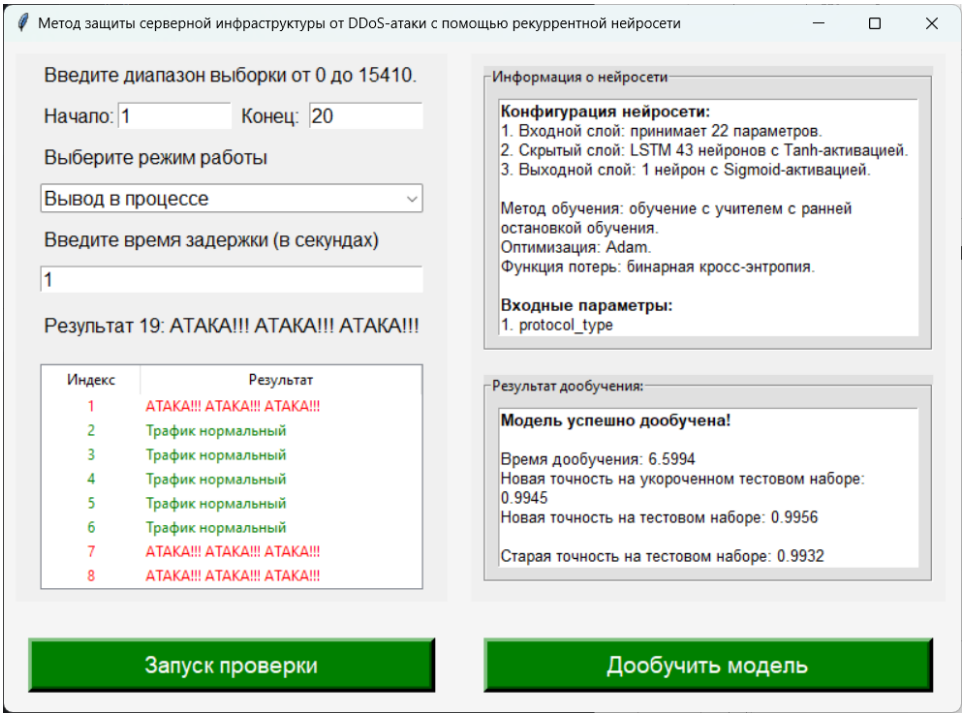

Рис. 2. Графический интерфейс реализованного ПО

Второй вариант использования тесно связан с первым — это подключение защиты непосредственно серверной инфраструктуры.

Код графического интерфейса является открытым, представляя собой вспомогательную инструкцию для интеграции функций разработанного метода в мультисервисную инфраструктуру клиента. Предполагается, что решение будет внедряться рядом со сбором статистических данных, поскольку обработку группы запросов необходимо выполнять каждый раз. При такой интеграции время ответа пользователю клиента не изменяется, поскольку получение результата по запросу и анализ запроса — две независимые операции. Такая организация взаимодействия предполагает корректную работу приложения клиента даже при дообучении модели и ее замене.

Разработанное решение поддерживает возможность масштабирования производительности двумя способами: использование ресурсов более мощного сервера для работы с модулем или использование нескольких серверов с запущенными нейросетями на каждом, поскольку анализируемая последовательность передается полностью и результат не зависит от результата предыдущего анализа, т. е. используя балансировщик нагрузки можно равномерно распределить ее между ними.

Решение позволяет обеспечение защиты сразу после подключения, при наличии статистики нормального трафика или определении специалистом параметров нормализации.

Дообучение модели на новых данных позволяет адаптировать систему к изменяющимся условиям и повышать точность классификации. Дообученная модель заменяет предыдущую версию и используется для дальнейшей работы. Это делает систему более гибкой и эффективной в долгосрочной перспективе. Дообученная модель показывает более высокие результаты по сравнению с первоначальной.

Результаты исследования. Было проведено исследование моделей с различной конфигурацией. Изменялась длина последовательности данных (1, 5, 10, 15, 20), набор входных параметров (127 комбинаций) и количество нейронов в скрытом слое (от n до $2n + 1$ с шагом 5, где n — количество входных параметров.

Исследование времени предсказания показало, что различия в конфигурациях моделей оказывают значительно меньшее влияние на время анализа, чем использование ресурсов процессора фоновыми процессами.

Тестовая точность не является строго зависимой от количества нейронов или количества эпох обучения. На нее оказывает влияние комбинация начальных весов, количества эпох, нейронов, но наиболее важным составляющим является набор входных параметров и длина анализируемой последо-

 ISSN 2541-8009

вательности. Точность модели увеличивается до тех пор, пока не появляются лишние параметры, способные спутать модель. Графики результатов исследования точности при длине последовательности 10 приведены на рис. 3 и 4. Конфигурация нейросети с самой высокой точность была приведена выше.

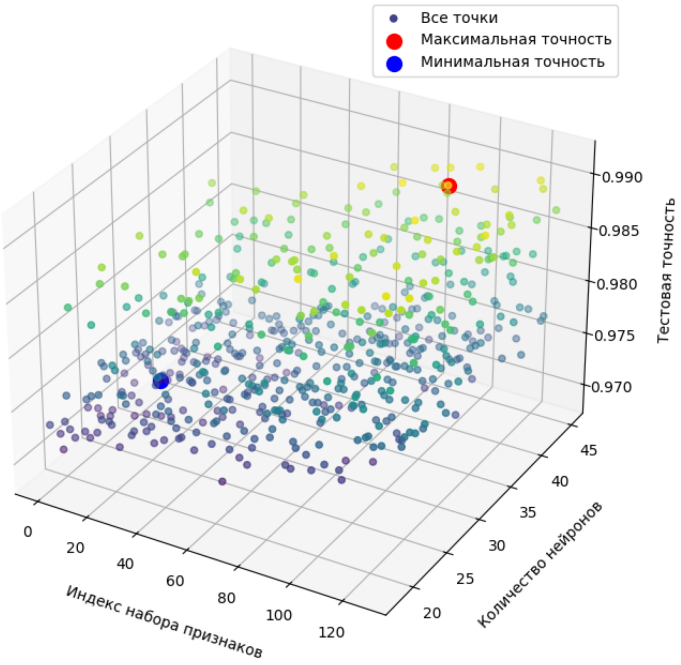

Рис. 3. Зависимость точности модели от набора параметров при длине последовательности 10

Количество эпох обучения для одинаковых конфигураций нейронных сетей и для разных невозможно предугадать, так как этот параметр зависит от случайных начальных весов. Зависимость от комбинаций набора входных данных и количества нейронов не прослеживается.

Время обучения модели значительно увеличивается в зависимости от длины последовательности. При длине последовательности 1 среднее время обучения составляет 54 с, а при длине 20 среднее время обучения равно 147 с. Это обусловлено увеличением количества весов в модели, которые необходимо постоянно корректировать. Время обучения модели не представляется в виде линейной зависимости, поскольку имеет также второй параметр, влияющий на длительность, — количество эпох, поэтому имеет аналогичные зависимости от других параметров.

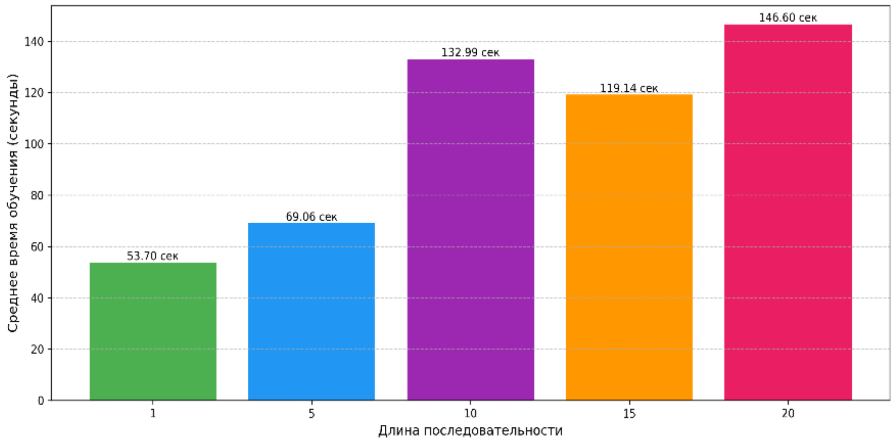

Рис. 4. Исследование точности модели при длине последовательности 10

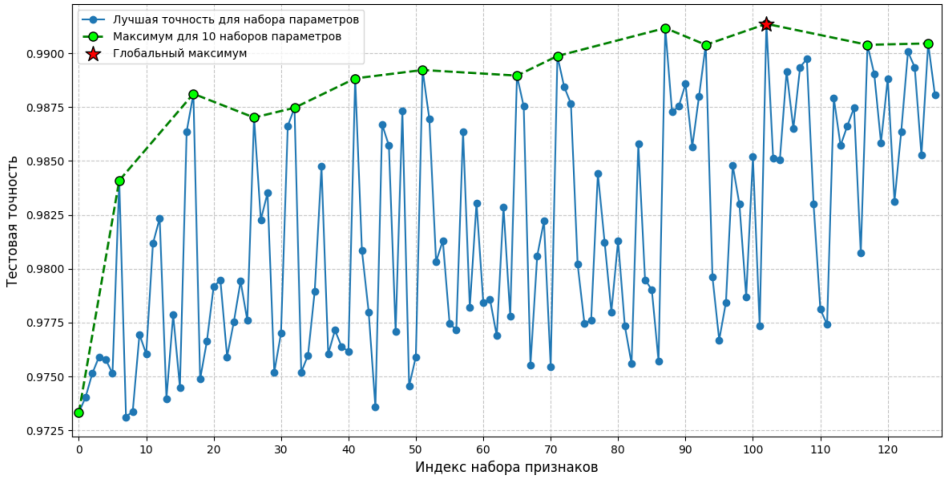

Рис. 5. Зависимость среднего времени обучения от длины последовательности данных

Заключение. Разработан метод защиты серверной инфраструктуры от распределенной атаки типа «отказ в обслуживании» с использованием рекуррентной нейронной сети. Программное обеспечение демонстрирует идеальный баланс: высокую точность (99,14 %) и скорость анализа данных (70,12 мс), возможность автоматизированной реакции и адаптации модели, что подтверждается результатами дообучения.

Проведенный анализ гиперпараметров модели показал константное время предсказания для различных конфигураций, непрогнозируемое количе-

 ISSN 2541-8009

ство эпох обучения, прямую зависимость времени обучения от длины последовательности и количества эпох, сложную зависимость точности от длины последовательности и набора входных параметров, достигающую пикового значения при конфигурации разработанной нейронной сети.

Литература

[1] Чичков С.Н. Методы защиты от DDOS-атак. *Цифровая экономика: проблемы и перспективы развития*, 2022, с. 571–574.

[2] Мусиенко С.С. Использование нейронных сетей для прогнозирования угроз информационной безопасности на примере DDoS-атак. *Инновационные научные исследования: сетевой журнал*, 2021, № 2–3 (4), с. 178–185. https://doi.org/10.5281/zenodo.4604863

[3] *Лаборатория Касперского. Как меняется ландшафт DDoS-атак в России*. URL: https://www.kaspersky.ru/about/press-releases/laboratoriya-kasperskogo-kak-menyaetsya-landshaft-ddos-atak-v-rossii (дата обращения 07.11.2024).

[4] *Cloudflare. Quarterly DDoS Attack Trends for Q1 2024*. URL: https://blog.cloudflare.com/ddos-threat-report-for-2024-q1/ (accessed 19.11.2024).

[5] *2023: годовой отчет StormWall о DDoS-атаках*. URL: https://stormwall.pro/resources/blog/ddos-ataki-2023-otchet-za-god (дата обращения 19.11.2024).

[6] Бачманов Д.А., Очередько А.Р., Путято М.М., Макарян А.С. Исследование вопросов совершенствования систем защиты от DDOS-атак на основе комплексного анализа современных механизмов противодействия. *Прикаспийский журнал: управление и высокие технологии*, 2021, № 1 (53), с. 63–74.

[7] Медведев М., Рева И. Анализ подходов к фильтрации трафика и эффективность применения черных и белых списков. *Вестник СибГУТИ*, 2023, т. 17, № 1, с. 107–116.

[8] *Kaspersky DDoS Protection.* URL: https://www.kaspersky.ru/enterprise-security/ddos-protection (дата обращения 19.01.2025).

[9] [*NDENIX*. URL: https://ngenix.net/ecp/ddos-protection/ (дата обращения 25.01.2025).

[10] *Yandex DDoS Protection в Virtual Private Cloud*. URL: https://yandex.cloud/ru/docs/vpc/ddos-protection/ (дата обращения 18.01.2025).

[11] *DDoS-GUARD*. URL: https://ddos-guard.ru/ (дата обращения 19.01.2025).

[12] *StormWall.* URL: https://stormwall.pro/ (дата обращения 21.01.2025).

[13] *Bunny.net.* URL: https://bunny.net/ (accessed 21.01.2025).

[14] *Cloud4Y*. URL: https://www.cloud4y.ru/ (дата обращения 24.01.2025).

[15] *NSL-KDD. Network Security, Information Security, Cyber Security*. URL: https://www.kaggle.com/datasets/hassan06/nslkdd (accessed 16.02.2025).

[16] Калугин Ю.А., Рудаков И.В. Выделение источника звука при помощи сверточных нейронных сетей с полносвязными слоями. *Modern Science*, 2021, № 4–3, с. 535–539.

Поступила в редакцию 09.04.2025

Сёмина Анна Алексеевна — студентка кафедры «Программное обеспечение ЭВМ и информационные технологии», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Рудаков Игорь Владимирович, кандидат технических наук, доцент, заведующий кафедрой «Программное обеспечение ЭВМ и информационные технологии», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Сёмина А.А. Метод защиты серверной инфраструктуры от распределенной атаки типа «отказ в обслуживании» с использованием рекуррентной нейронной сети. *Политехнический молодежный журнал*, 2025, № 05 (100). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1051.html

 ISSN 2541-8009

METHOD OF PROTECTING SERVER INFRASTRUCTURE FROM DISTRIBUTED DENIAL OF SERVICE ATTACK USING A RECURRENT NEURAL NETWORK

A.A. Semina anna290303@yandex.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Modern statistics from leading cybersecurity companies (Kaspersky Lab, Cloudflare, Statista) indicate a 63 % increase in the number of DDoS attacks in 2023–2024. This article discusses an innovative method for countering these threats based on the use of recurrent neural networks (RNN). The developed solution provides automated detection of attacks in real time with the ability to respond instantly, demonstrating classification accuracy at the level of 99.14 % and analysis time of only 70.12 ms on a test sample from the NSL-KDD set. A special feature of the proposed approach is adaptability to new types of threats due to the mechanism of additional training of the model. The system can be integrated into the existing client infrastructure without disrupting the operation of services. The conducted studies of various RNN configurations (including analysis of the influence of the sequence length, the number of neurons and training epochs) made it possible to achieve an optimal balance between accuracy and performance.

Keywords: DDoS attacks, cybersecurity, recurrent neural networks, machine learning, server protection, NSL-KDD, automatic attack detection

Received 09.04.2025

Semina A.A. — Student of Department of Computer Software and Information Technology, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Rudakov I.V., Ph. D. (Eng.), Associate Professor, Head of the Department of Computer Software and Information Technology, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Semina A.A. Method of protecting server infrastructure from distributed denial of service attack using a recurrent neural network. *Politekhnicheskiy molodezhnyy zhurnal*, 2025, no. 05 (100). (In Russ.). URL: https://ptsj.bmstu.ru/catalog/icec/insec/1051.html

