Научная статья
УДК 004.85
https://doi.org/10.31854/1813-324X-2025-11-3-87-96
EDN:EDKHNU

Применение адаптивной нейро-нечеткой системы вывода для обнаружения DDoS-атак на основе набора данных CIC-DDoS-2019

Николай Николаевич Васин[1], vasin-nn@psuti.ru
Карен Сергеевич Какабьян[2] ✉, and4r1lh0@yandex.ru

[1]Поволжский государственный университет телекоммуникаций и информатики,
Самара, 443010, Российская Федерация
[2]ООО «Яндекс Облако»,
Москва, 119021, Российская Федерация

Аннотация

Актуальность. *Распределенные атаки типа «отказ в обслуживании» (DDoS) остаются значительной угрозой для доступности онлайн-сервисов. Традиционные системы обнаружения вторжений, основанные на сигнатурах или анализе аномалий, сталкиваются с ограничениями при обнаружении новых и сложных атак, в то время как подходы на основе машинного обучения, демонстрируя высокий потенциал, часто лишены интерпретируемости. Гибридные системы, такие как адаптивная нейро-нечеткая система вывода (ANFIS), объединяют преимущества нейронных сетей и нечеткой логики, предлагая как точность, так и возможность интерпретации. Однако их эффективность применительно к современным наборам данных с разнообразными векторами атак, таким как CIC-DDoS-2019, требует изучения.*

Цель. *Исследование направлено на оценку эффективности и применимости системы ANFIS для задачи обнаружения DDoS-атак с использованием актуального и сложного набора данных CIC-DDoS-2019. В работе* ***использовалась*** *модель ANFIS. Исследование проводилось на репрезентативной подвыборке из набора данных CIC-DDoS-2019. Методология включала тщательную предварительную обработку данных, отбор наиболее релевантных признаков и экспертных знаний, нормализацию признаков. Модель ANFIS с гауссовыми функциями принадлежности обучалась с использованием гибридного алгоритма оптимизации (градиентный спуск и метод наименьших квадратов) на 80 % данных. Эффективность оценивалась на оставшихся 20 % тестовых данных с использованием стандартных метрик классификации: Accuracy, Precision, Recall, F1-Score, а также анализа матрицы ошибок.*

Результаты. *Эксперименты показали высокую производительность модели ANFIS. Были достигнуты следующие показатели: доля правильно классифицированных объектов (Accuracy) – 97,82 %, точность (Precision) – 99,52 %, полнота (Recall) – 85,95 % и F1-мера – 92,24 %. Результаты указывают на очень низкий уровень ложных срабатываний, при некотором количестве пропущенных атак.*

Научная новизна. *Работа демонстрирует применение и оценку эффективности ANFIS на современном и сложном наборе данных CIC-DDoS-2019, содержащем актуальные типы атак. Исследование подтверждает* ***теоретическую применимость*** *гибридных нейро-нечетких моделей для решения актуальных задач кибербезопасности.* ***Практическая значимость*** *состоит в демонстрации того, что ANFIS может служить основой для разработки эффективных систем обнаружения DDoS-атак, обеспечивая высокий уровень точности и приемлемую полноту обнаружения. Возможность анализа функций принадлежности и правил реализует интерпретируемость, что важно для понимания работы системы и анализа угроз. Результаты предоставляют эталонные показатели для ANFIS на данном наборе данных.*

Ключевые слова: *DDoS-атаки, обнаружение вторжений, нейро-нечеткие системы, ANFIS, машинное обучение, анализ сетевого трафика*

Ссылка для цитирования: Васин Н.Н., Какабьян К.С. Применение адаптивной нейро-нечеткой системы вывода для обнаружения DDoS-атак на основе набора данных CIC-DDoS-2019 // Труды учебных заведений связи. 2025. Т. 11. № 3. С. 87–96. (in Russ.) DOI:10.31854/1813-324X-2025-11-3-87-96. EDN:EDKHNU

Original research
https://doi.org/10.31854/1813-324X-2025-11-3-87-96
EDN:EDKHNU

Application of Adaptive Neuro-Fuzzy Inference System for DDoS Attack Detection Based on CIC-DDoS-2019 Dataset

Nikolay N. Vasin[1], vasin-nn@psuti.ru
Karen S. Kakabian[2] ✉, and4r1lh0@yandex.ru

[1]Povolzhskiy State University of Telecommunications and Informatics,
Samara, 443010, Russian Federation
[2]Yandex Cloud, LLC,
Moscow, 119021, Russian Federation

Annotation

The relevance. *Distributed Denial of Service (DDoS) attacks remain a significant threat to the availability of online services. Traditional intrusion detection systems based on signatures or anomaly analysis face limitations in detecting new and complex attacks, while machine learning-based approaches, while showing high potential, often lack interpretability. Hybrid systems, such as the Adaptive Neuro-Fuzzy Inference System (ANFIS), combine the advantages of neural networks and fuzzy logic, offering both accuracy and interpretability. However, their effectiveness with respect to modern datasets with diverse attack vectors, such as CIC-DDoS-2019, needs to be investigated.*

Objective. *The study aims to evaluate the performance and applicability of ANFIS for the task of DDoS attack detection using the current and challenging CIC-DDoS-2019 dataset. The ANFIS model was* ***used*** *in this work. The study was conducted on a representative subsample of the CIC-DDoS-2019 dataset. The methodology included careful data preprocessing, selection of the most relevant features and expert knowledge, and feature normalisation. The ANFIS model with Gaussian membership functions was trained using a hybrid optimisation algorithm (gradient descent and least squares method) on 80 % of the data. Performance was evaluated on the remaining 20 % of the test data using standard classification metrics: Accuracy, Precision, Recall, F1-Score, and error matrix analysis.*

Results. *The experiments showed high performance of the ANFIS model. The following metrics were achieved: proportion of correctly classified objects (Accuracy) – 97.82 %, accuracy (Precision) – 99.52 %, completeness (Recall) – 85.95 % and F1-measure – 92.24 %. The results indicate a very low false positive rate, with some number of missed attacks.*

Novelty. *The work demonstrates the application and performance evaluation of ANFIS on a modern and complex CIC-DDoS-2019 dataset containing relevant attack types.*
The study confirms the theoretical applicability of hybrid neuro-fuzzy models to solve current cybersecurity problems.

The practical significance *consists in demonstrating that ANFIS can serve as a basis for the development of effective DDoS attack detection systems, providing a high level of accuracy and acceptable detection completeness. The ability to analyze membership functions and rules implements interpretability, which is important for understanding system performance and threat analysis. The results provide benchmarks for ANFIS on this dataset.*

Keywords: *DDoS attacks, intrusion detection, neuro-fuzzy systems, ANFIS, machine learning, network traffic analysis*

For citation: Vasin N.N., Kakabian K.S. Application of Adaptive Neuro-Fuzzy Inference System for DDoS Attack Detection Based on CIC-DDoS-2019 Dataset. *Proceedings of Telecommunication Universities.* 2025;11(3):87–96. DOI:10.31854/1813-324X-2025-11-3-87-96. EDN:EDKHNU

Введение

Повсеместное распространение интернет-сервисов сделало их доступность критически важным фактором для современной экономики и общества. Распределенные атаки типа «отказ в обслуживании» (DDoS, *аббр. от англ.* Distributed Denial of Service) направлены на нарушение этой доступности путем перегрузки целевых систем или сетевых

каналов огромным потоком вредоносного трафика, генерируемого с множества скомпрометированных устройств [1]. Последствия успешных DDoS-атак варьируются от временной недоступности сервисов до значительных финансовых и репутационных потерь.

Масштабы DDoS-атак постоянно растут. Злоумышленники используют все более сложные методы, включая атаки на уровне приложений, атаки с амплификацией и отражением, а также атаки, имитирующие легитимный трафик, что значительно усложняет их обнаружение традиционными методами [2]. Классические подходы, такие как системы обнаружения вторжений на основе сигнатур, эффективны против известных атак, но уязвимы перед новыми или модифицированными вариантами. Системы обнаружения вторжений, основанные на обнаружении аномалий, способны выявлять ранее неизвестные атаки, но зачастую подвержены высокому уровню ложных срабатываний [3].

В последние годы методы машинного обучения (ML, *аббр. от англ.* Machine Learning) продемонстрировали большой потенциал в области обнаружения DDoS-атак [4, 5]. Эти подходы позволяют автоматически извлекать сложные закономерности из сетевого трафика и строить модели для классификации потоков на легитимные и вредоносные. Однако многие модели ML функционируют как «черные ящики», что затрудняет интерпретацию их решений и настройку.

В этом контексте перспективным направлением является использование гибридных интеллектуальных систем, объединяющих сильные стороны различных подходов. Нейро-нечеткие системы, в частности адаптивные нейро-нечеткие системы вывода (ANFIS, *аббр. от англ.* Adaptive Neuro-Fuzzy Inference System) [6], представляют собой такой гибридный подход. ANFIS интегрирует способность нейронных сетей к обучению на данных со способностью систем нечеткой логики оперировать неточными, неопределенными данными и представлять знания в виде интерпретируемых правил. Это позволяет создавать системы обнаружения DDoS, которые не только точны, но и потенциально более прозрачны и устойчивы к зашумленным данным.

Целью данной работы является оценка эффективности применения ANFIS для обнаружения DDoS-атак на основе набора данных CIC-DDoS-2019 [7]. Набор данных CIC-DDoS-2019 содержит большой объем трафика (более 430 000 сетевых пакетов), включая как нормальную активность, так и широкий спектр новейших DDoS-атак (DNS, LDAP, MSSQL, NTP, SNMP, SSDP, SYN, TFTP, UDP, UDP-Lag, WebDDoS), что делает его релевантным для оценки современных систем обнаружения.

С развитием ML появилось множество работ, применяющих различные классификаторы для обнаружения DDoS. Среди них Support Vector Machines (SVM), Decision Trees (DT), Random Forest (RF), Naive Bayes (NB) и K-Nearest Neighbors (KNN) [8]. Эти методы часто показывают хорошую производительность, но требуют тщательного отбора признаков и настройки гиперпараметров. Работы [9, 10] предоставляют сравнительный анализ различных ML-алгоритмов на всякого рода наборах данных, включая унаследованные (KDD Cup 99, NSL-KDD) и современные (CICIDS2017, CIC-DDoS-2019).

В последнее время активно применяются методы глубокого обучения (DL, *аббр. от англ.* Deep Learning), такие как сверточные нейронные сети (CNN, *аббр. от англ.* Convolutional Neural Network) и рекуррентные нейронные сети (RNN, *аббр. от англ.* Recurrent Neural Network) – LSTM, GRU. DL-модели способны автоматически извлекать высокоуровневые признаки из сырых данных трафика, что потенциально улучшает точность обнаружения сложных атак. Однако они требуют больших объемов данных для обучения, значительных вычислительных ресурсов и часто страдают от недостатка интерпретируемости.

Применение нейро-нечетких систем для обнаружения вторжений, включая DDoS, также исследовалось, хотя и в меньшей степени по сравнению с чистыми ML/DL-подходами. В работе [11] предлагается использование ANFIS для обнаружения аномалий в сетевом трафике. Авторы [12] применяют ANFIS в сочетании с генетическими алгоритмами для оптимизации параметров системы обнаружения DDoS-атак. В [13] ANFIS используют для классификации атак на наборе данных KDD Cup 99, демонстрируя хорошие результаты. Однако применение ANFIS к новейшим и более сложным наборам данных, таким как CIC-DDoS-2019, содержащим современные векторы атак, остается менее изученной областью.

Методология

ANFIS представляет собой многослойную адаптивную сеть, функционально эквивалентную системе нечеткого вывода типа Сугено. Ее структура позволяет использовать алгоритмы обучения нейронных сетей для настройки параметров системы нечеткого вывода на основе обучающих данных [14]. Типичная архитектура ANFIS для системы с двумя входами и одним выходом показана на рисунке 1 и состоит из пяти слоев.

Слой 1 – слой фаззификации. Каждый узел в этом слое является адаптивным и вычисляет степень принадлежности входного значения к нечеткому множеству. При этом он соответствует одной нечеткой функции принадлежности (ФП).

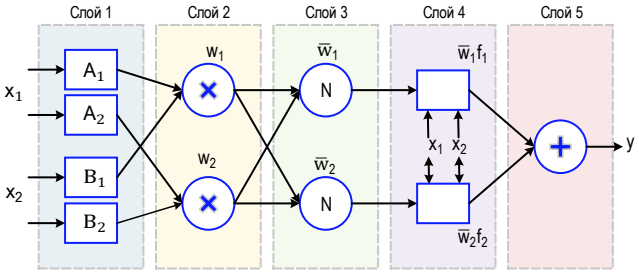

Рис. 1. Архитектура ANFIS для системы с двумя входами и одним выходом

Fig. 1. ANFIS Architecture for a System with Two Inputs and One Output

В данной реализации для каждого из входов используется две гауссовых ФП. Гауссова ФП определяется двумя параметрами – центром c и шириной σ:

$$\mu_{ij}(x_i) = e^{-\frac{1}{2}\left(\frac{x_i - c_{ij}}{\sigma_{ij}}\right)^2}, \quad (1)$$

где $\mu_{ij}(x_i)$ – степень принадлежности входного значения x_i к j-му нечеткому множеству для i-го входа; c_{ij} – центр (среднее значение) j-й гауссовой ФП для i-го входа; σ_{ij} – ширина (стандартное отклонение) j-й гауссовой ФП для i-го входа; x_i – нормализованное входное значение.

Начальные параметры c и σ инициализируются равномерно в диапазоне [0, 1] (после нормализации данных) с добавлением небольшого случайного шума. Сигма ограничивается снизу малым положительным значением $(1 \cdot 10^{-6})$ для стабильности.

Слой 2 – слой правил. Каждый узел соответствует одному нечеткому правилу. В данной реализации, с 10 входами и 2 ФП на вход, система оперирует 1024 правилами. Каждое правило неявно определяется уникальной комбинацией ФП (по одной от каждого входа).

Выход узла r (сила срабатывания правила w_r) вычисляется как произведение степеней принадлежности из Слоя 1, соответствующих данному правилу r:

$$w_r = \mu_{1,k_1}(x_1) \cdot \mu_{2,k_2}(x_2) \cdot \ldots \cdot \mu_{10,k_{10}}(x_{10}), \quad (2)$$

где k_i – индекс ФП для i-го входа в правиле r; $\mu_{i,k_i}(x_i)$ – степень принадлежности x_i к выбранной ФП для i-го входа.

Слой 3 – слой нормализации. Узлы этого слоя вычисляют нормализованную силу срабатывания каждого правила как отношение силы срабатывания правила r к сумме сил срабатывания всех правил:

$$\overline{w}_r = \frac{w_r}{\sum_{k=1}^{N} w_k}, \quad (3)$$

где $\overline{w}_r$ – нормализованная сила срабатывания правила r; w_r – исходная сила срабатывания правила r; N – общее количество правил в системе.

Слой 4 – слой дефаззификации. Каждый узел является адаптивным. Выход узла вычисляется как произведение нормализованной силы срабатывания правила на выход этого правила (линейную комбинацию входов для системы Сугено первого порядка).

Для модели Сугено нулевого порядка выход каждого правила является константой C_r (обучаемый параметр заключения). Выход узла r в этом слое равен произведению нормализованной силы срабатывания на константу этого правила.

Вектор параметров заключения $C = [C_1, C_2 \ldots C_N]$ инициализируется случайными малыми значениями.

Слой 5 – выходной слой. Единственный узел в этом слое вычисляет итоговый выход системы y как сумму выходов всех узлов предыдущего слоя:

$$y = \sum_{r=1}^{N} \overline{w}_r \cdot C_r, \quad (4)$$

где y – итоговый выход системы; $\overline{w}_r$ – нормализованная сила срабатывания правила r; C_r – параметр заключения правила r.

Обучение ANFIS обычно происходит с использованием гибридного алгоритма: параметры предпосылки (в слое 1) настраиваются методом градиентного спуска, а параметры заключения (в слое 4) вычисляются методом наименьших квадратов на прямом проходе. Это позволяет ANFIS эффективно настраивать как ФП, так и параметры выходных функций правил для аппроксимации заданной зависимости между входами и выходами.

Набор данных CIC-DDoS-2019

Для обучения и оценки модели ANFIS был выбран набор данных CIC-DDoS-2019, разработанный канадским университетом Нью–Брансуика. Представленный набор данных является одним из наиболее актуальных и комплексных общедоступных датасетов, специально сфокусированных на современных DDoS-атаках, что делает его референтным для оценки систем их обнаружения. В отличие от наборов, полученных ранее, таких как, CIC-IDS2017, который шире и ориентирован на различные типы вторжений в информационные системы, а не только DDoS [15], CIC-DDoS-2019 включает 16 типов современных DDoS-атак, включая атаки на уровне приложений и атаки с использованием механизмов амплификации. Фокус данного исследования направлен именно на обнаружение DDoS-атак, что делает специализированный набор CIC-DDoS-2019 наиболее подходящим для поставленной задачи. Он был создан путем захвата и анализа реального сетевого трафика в контролируемой среде.

Основные характеристики CIC-DDoS-2019:

– содержит как фоновый легитимный трафик, сгенерированный на основе профилей [16], так и трафик реальных DDoS-атак;

– включает 16 различных типов DDoS-атак, использующих протоколы TCP (SYN), UDP (DNS, LDAP, MSSQL, NetBIOS, NTP, SNMP, SSDP, TFTP, UDP, UDP-Lag) и HTTP (WebDDoS); атаки охватывают как методы отражения / амплификации, так и атаки на уровне приложений и на транспортном уровне;

– содержит значительный объем данных, представленных в виде двунаправленных потоков;

– для каждого потока извлечено более 75 статистических признаков с использованием инструмента CICFlowMeter [17]; данные признаки включают информацию о длительности потока, количестве пакетов, размерах пакетов, временны́х интервалах между пакетами (IAT), флагах TCP и т. д.

Использование CIC-DDoS-2019 позволяет оценить способность ANFIS обнаруживать широкий спектр современных DDoS-угроз в условиях, приближенных к реальным.

Хотя в данном исследовании используется репрезентативная выборка, она была сформирована таким образом, чтобы сохранить разнообразие представленных в исходном наборе типов атак и обеспечить возможность проведения экспериментов на оборудовании с ограниченными ресурсами, не теряя при этом общности выводов.

Предварительная обработка данных

Качество данных имеет решающее значение для построения эффективной модели ML. Данные CIC-DDoS-2019, представленные в формате CSV-файлов, требуют тщательной предварительной обработки.

Ввиду значительного размера полного набора данных (~50 Гб), для исследования была использована репрезентативная выборка, включающая легитимный трафик и несколько характерных типов DDoS-атак. Такой подход позволил провести эксперименты на оборудовании с ограниченными ресурсами, сохранив при этом разнообразие данных.

Признаки, не несущие полезной информации для классификации, были удалены. IP-адреса и порты могут быть полезны для анализа конкретной атаки, но для построения общей модели обнаружения их часто исключают, чтобы избежать переобучения на конкретные адреса. Также была проведена проверка на наличие пропущенных значений. Распространенной стратегией является замена значений NaN на медианное или нулевое значение, либо удаление строк с пропусками, если их немного. В данном исследовании строки с NaN также были удалены.

Признаки, являющиеся результатом деления («Flow Bytes/s», «Flow Packets/s»), могут содержать бесконечные значения, если делитель (длительность потока) равен нулю. Такие значения непригодны для большинства алгоритмов ML. Они были заменены на очень большие числа (представляющие максимальное значение для данного типа данных) или удалены / заменены медианой по столбцу. Были проверены и удалены полностью дублирующиеся строки.

Целевой признак «Label» содержит текстовые метки («Benign» и различные типы атак). Для задачи бинарной классификации все метки атак были объединены в один класс «DDoS». Затем метки «Benign» и «DDoS» были преобразованы в числовой формат (0 и 1).

Использование всех признаков набора данных неизбежно приведет к увеличению вычислительной сложности, переобучению и проблеме «проклятия размерности». Соответственно был применен метод отбора признаков на основе их важности, определенной с помощью алгоритма Random Forest, а также на основе корреляции и экспертных знаний о признаках, наиболее релевантных для DDoS-атак. Было выбрано подмножество наиболее информативных признаков («Down/Up Ratio», «URG Flag Count», «Avg Fwd Segment Size», «Fwd Packet Length Mean», «Packet Length Min», «Fwd Packet Length Min», «Packet Length Mean», «Bwd Packet Length Min», «Avg Packet Size», «Protocol»).

Значения признаков в наборе данных имеют различные диапазоны. Для корректной работы ANFIS необходимо привести все признаки к единому масштабу. Была применена нормализация с использованием функции MinMaxScaler [18], которая масштабирует значения в диапазоне [0, 1].

Обработанный набор данных был разделен на обучающую и тестовую выборки в пропорции 80 % / 20 %, соответственно. Разделение производилось стратифицированно для сохранения исходного соотношения классов в обеих выборках.

Реализация модели ANFIS

Для реализации ANFIS использовалась библиотека sklearn, предоставляющая функциональность для создания и обучения подобных систем. Количество входов модели ANFIS соответствует количеству признаков, выбранных на этапе отбора. Для каждого входа было определено два нечетких множества с использованием гауссовых ФП. Параметры функций (центр, ширина) инициализировались на основе распределения данных и затем настраивались в процессе обучения.

Система автоматически генерирует правила, покрывающие все комбинации нечетких множеств входных переменных. Модель имеет один выход,

представляющий степень уверенности в том, что входной поток является DDoS-атакой (значение близкое к 1) или легитимным трафиком (значение близкое к 0).

Модель обучалась на выборке с использованием гибридного алгоритма оптимизации (градиентный спуск + метод наименьших квадратов) в течение заданного числа эпох. Целевой функцией являлась минимизация среднеквадратичной ошибки (MSE, *аббр. от англ.* Mean Squared Error) между выходами модели и истинными метками (0 или 1).

Метрики оценки

Для оценки производительности обученной модели ANFIS на тестовой выборке использовались стандартные метрики бинарной классификации [19]. Матрица ошибок отображает количество истинно положительных (TP), истинно отрицательных (TN), ложно положительных (FP) и ложно отрицательных (FN) срабатываний.

Значения TP, TN, FP и FN, полученные из матрицы ошибок по результатам тестирования модели на отложенной выборке, напрямую используются для расчета метрик:

– Accuracy (доля правильно классифицированных объектов от общего числа объектов):

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}; \quad (5)$$

– Precision (точность – доля истинно положительных срабатываний среди всех примеров, классифицированных моделью как положительные; показывает, насколько можно доверять сигналу «атака»):

$$Precision = \frac{TP}{TP + FP}; \quad (6)$$

– Recall (полнота – доля истинно положительных срабатываний среди всех реально положительных примеров; показывает, какую долю реальных атак модель смогла обнаружить):

$$Recall = \frac{TP}{TP + FN}; \quad (7)$$

– F1-Score (F1-мера – среднее гармоническое точности и полноты; является метрикой для несбалансированных наборов данных, где важны и Precision, и Recall):

$$F_{score} = \frac{2 \cdot TP}{2 \cdot TP + FN + FP}. \quad (8)$$

Наряду с указанными метриками, для оценки точности непрерывных выходных значений ANFIS (представляющих степень уверенности в принадлежности к классу) до их преобразования в бинарные метки используется MSE, которая минимизируется в процессе обучения модели:

$$MSE = \frac{1}{M}\sum_{i=1}^{M}\left(y_{И}^{(i)} - y_{П}^{(i)}\right)^2, \quad (9)$$

где M – количество объектов в тестовой выборке; $y_{И}^{(i)}$ – истинное значение для i-го объекта; $y_{П}^{(i)}$ – предсказанное значение для i-го объекта.

Вышеуказанные показатели позволяют количественно оценить аспекты производительности классификатора. При этом высокие значения метрик Accuracy, Precision, Recall и F1-Score свидетельствуют о хорошей производительности системы обнаружения, в то время как низкое значение MSE указывает на высокую точность предсказаний модели.

Особое внимание в задачах обнаружения DDoS уделяется высокой полноте (минимизация FN, т. е. пропущенных атак) и приемлемой точности (минимизация FP, т. е. ложных тревог).

Проведение экспериментов

Эксперименты проводились с использованием библиотек языка программирования Python 3, а именно NumPy для вычислений, Pandas для обработки данных, Scikit-learn для предобработки, разделения данных и расчета метрик, Matplotlib для построения графиков. Использовалась подвыборка из CIC-DDoS-2019, включающая файл с легитимным трафиком и несколькими типами атак. Общий размер обработанной подвыборки составил 16 071 пакетов.

Параметры обучения:
– количество эпох: 20;
– размер батча: 64;
– скорость обучения: 0,1;
– количество гауссовых ФП на вход: 2;
– количество правил: $2^{10} = 1024$.

Обучающая выборка – 12 856 записей; тестовая выборка – 3 215 записей.

Выход ANFIS представляет собой непрерывное значение. Для бинарной классификации был установлен порог 0,5 (значения $\geq 0{,}5$ классифицировались как DDoS, а – $< 0{,}5$ как нормальная сетевая активность). После обучения модели ANFIS в течение 20 эпох на 80 % данных и тестирования на оставшихся 20 %, были получены следующие функции принадлежности (рисунок 2).

Среднее время обучения одной эпохи составило порядка 5–8 минут.

График ошибки обучения, изображенный на рисунке 3, показал общее снижение при увеличении количества эпох. Определено оптимальное количество эпох равное 4. Матрица ошибок изображена на рисунке 4. Метрики производительности модели представлены в таблице 1.

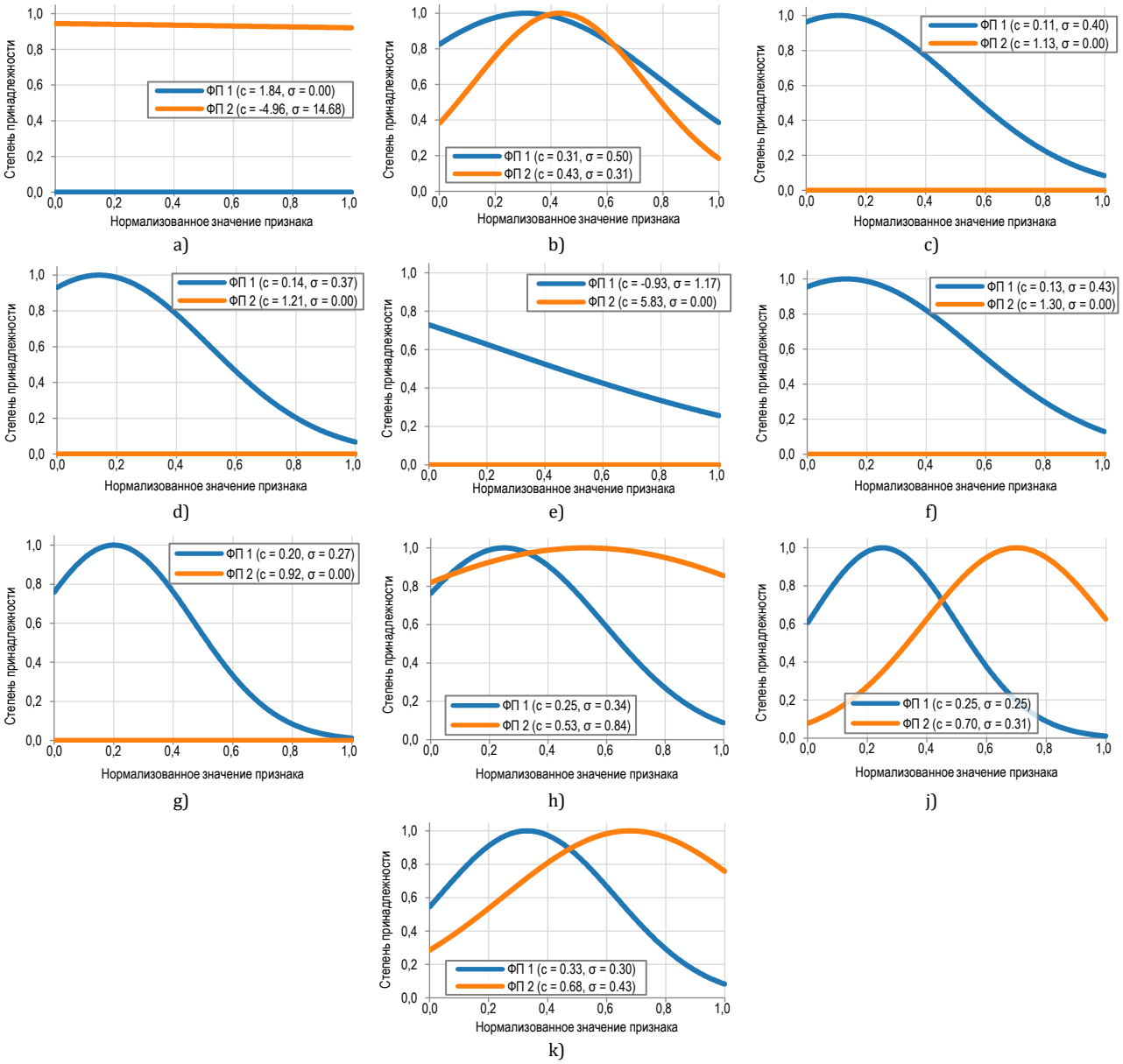

Рис. 2. Функции принадлежности для «Avg Fwd Segment Size» (a), «Avg Packet Size» (b), «Bwd Packet Length Min» (c), «Down/Up Ratio» (e), «Fwd Packet Length Mean» (f), «Fwd Packet Length Min» (g), Packet Length Mean» (h), «Protocol» (j) и «URG Flag Count» (k)

Fig. 2. Accessory Function for «Avg Fwd Segment Size» (a), «Avg Packet Size» (b), «Bwd Packet Length Min» (c), «Down/Up Ratio» (e), «Fwd Packet Length Mean» (f), «Fwd Packet Length Min» (g), Packet Length Mean» (h), «Protocol» (j) and «URG Flag Count» (k)

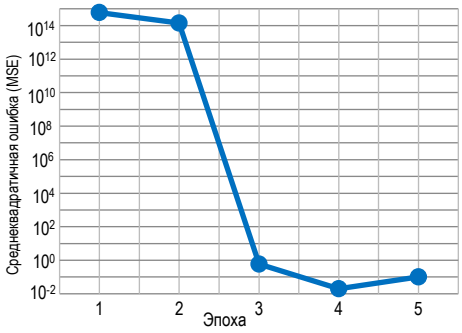

Рис. 3. График ошибки обучения ANFIS (MSE) по эпохам

Fig. 3. Graph of ANFIS Learning Error (MSE) by Epochs

Рис. 4. Матрица ошибок модели ANFIS

Fig. 4. Confusion Matrix for ANFIS

ТАБЛИЦА 1. Метрики производительности ANFIS

TABLE. 1. ANFIS Performance Metrics

Метрика	Значение (%)
Accuracy	97,82
Precision (DDoS)	99,52
Recall (DDoS)	85,95
F1-Score (DDoS)	92,24
MSE	2,46

Результаты свидетельствуют о высокой доле правильно классифицированных объектов. Представленная модель правильно классифицирует подавляющее большинство потоков трафика. Высокий показатель точности (Precision = 99,52 %) является особенно важным результатом, поскольку он указывает на крайне низкий уровень ложных срабатываний (FP = 2 в абсолютных числах из матрицы ошибок на рисунке 4). Это означает, что система редко ошибочно помечает легитимный трафик как атаку, что критично для минимизации перебоев в работе защищаемых сервисов. Полнота (Recall = 85,95 %) несколько ниже, что указывает на пропуск моделью 68 пакетов, относящихся к реальным атакам (FN = 68 на рисунке 4). Достигнутый уровень полноты в сочетании с высокой точностью является значимым для сложных и разнообразных атак, представленных в CIC-DDoS-2019. Высокий показатель F1-меры подтверждает хороший баланс точности и полноты.

Достигнутые метрики сопоставимы с результатами, получаемыми с использованием стандартных библиотек или других методов ML на указанном наборе данных [20], однако предложенный подход на основе ANFIS дополнительно предлагает преимущества в виде интерпретируемости функций принадлежности и правил нечеткого вывода.

Преимущества ANFIS в контексте обнаружения DDoS-атак

Во-первых, возможно дообучение модели на новых данных, что важно для адаптации к изменяющимся тактикам атак.

Во-вторых, в отличие от методов DL, из обученной ANFIS можно извлечь нечеткие правила. Анализ функций принадлежности и их связей может дать представление о том, какие комбинации значений признаков наиболее характерны для атак, что полезно для анализа и понимания угроз и обеспечивает интерпретируемость данного подхода.

В-третьих, нечеткая логика по своей природе хорошо справляется с зашумленными входными данными, что характерно для реального сетевого трафика.

В-четвертых, эксперименты показали, что ANFIS может достигать высоких показателей доли правильно классифицированных объектов, точности и полноты, минимизируя количество пропущенных атак.

Ограничения ANFIS

1) ANFIS, особенно с большим количеством входов и функций принадлежности, может быть вычислительно затратным. Количество правил увеличивается экспоненциально с увеличением числа входов и числа ФП. Это ограничивает количество признаков, которые могут быть эффективно использованы напрямую.

2) Производительность ANFIS зависит от выбора архитектуры (количества и типа ФП, количества входов). Оптимальный выбор параметров требует экспериментов и знаний в предметной области.

3) Применение ANFIS к потокам данных в реальном времени требует оптимизированных реализаций, а также интеграции с аппаратными ускорителями [21].

По сравнению с традиционными ML-алгоритмами (SVM, RF), ANFIS предлагает более удобный способ работы с неопределенностью и потенциально лучшую интерпретируемость правил. По сравнению с DL-моделями, ANFIS может требовать меньше данных для обучения и обеспечивает лучшую прозрачность.

Заключение

В статье было рассмотрено применение адаптивной нейро-нечеткой системы вывода (ANFIS) для задачи обнаружения DDoS-атак на основе набора данных CIC-DDoS-2019. Проведенные эксперименты, включающие этапы предварительной обработки данных, отбора признаков, обучения и тестирования модели ANFIS, продемонстрировали высокую эффективность предложенного подхода. Модель показала отличные результаты по метрикам доли правильно классифицированных объектов, точности, полноты и F1-меры, успешно идентифицируя DDoS-атаки с минимальным количеством ложных срабатываний, что особенно важно для практического применения, и приемлемым уровнем пропущенных атак, учитывая сложность и разнообразие атак, представленных в наборе данных.

Результаты подтверждают, что гибридный подход ANFIS, сочетающая адаптивность нейронных сетей и интерпретируемость нечеткой логики, делает ее мощным инструментом для разработки интеллектуальных систем обнаружения вторжений. Способность ANFIS моделировать границы между нормальным и аномальным поведением является ценным качеством при анализе сетевого трафика.

Список источников

1. Арикова К.Г. Анализ статистических данных по реализации кибератак и их последствий // Всероссийская студенческая научно-практическая конференция «Цифровая экономика и безопасность: вызовы и перспективы» (Москва, Российская Федерация, 21–22 марта 2024 г.). М.: РТУ МИРЭА, 2024. С. 10–14. EDN:DHNDAL

2. Баранов И.А., Кучеренко М.А., Карасев П.И. DDOS атаки и методы защиты от них // I Национальная научно-практическая конференция (Москва, Российская Федерация, 24–26 мая 2023 г.) «Кибербезопасность: технические и правовые аспекты защиты информации». М.: РТУ МИРЭА, 2023. С. 133–136. EDN:BQZKRL

3. Козлова Н.Ш., Довгаль В.А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. 2023. № 3(326). С. 65–72. DOI:10.53598/2410-3225-2023-3-326-65-72. EDN:CYUKLH

4. Лизнева Ю.С., Ростова Е.В. К вопросу о применении машинного обучения для классификации сетевых аномалий // Всероссийская научно-техническая конференция с международным участием «Обработка информации и математическое моделирование» (Новосибирск, Российская Федерация, 19–20 апреля 2023 г.). Новосибирск: СибГУТИ, 2023. С. 58–61. EDN:DILYWD

5. Попов А.С., Константинова А.А. Применение искусственного интеллекта в системах информационной безопасности // Всероссийская студенческая научно-практическая конференция «Математические модели техники, технологий и экономики» (Санкт-Петербург, Российская Федерация, 15 мая 2024 г.). СПб.: СПбГЛТУ, 2024. С. 363–367. EDN:FNVXCM

6. Ростовцев В.С. Искусственные нейронные сети: учебник для вузов. СПб.: Лань, 2025. 216 с.

7. DDoS evaluation dataset (CIC-DDoS2019) // University of New Brunswick. URL: https://www.unb.ca/cic/datasets/ddos-2019.html (Accessed 29.03.2025)

8. Rahman M.A. Detection of distributed denial of service attacks based on machine learning algorithms // International Journal of Smart Home. 2020. Vol. 14. Iss. 2. PP. 15–24. DOI:10.21742/ijsh.2020.14.2.02. EDN:MMRDIG

9. Le D.C., Dao M.H., Nguyen K.L.T. Comparison of Machine Learning Algorithms for DDOS Attack Detection in SDN // Information and Control Systems. 2020. № 3(106). С. 59–70. DOI:10.31799/1684-8853-2020-3-59-70. EDN:GLVTEL

10. Shakya S., Abbas R. Comparative Evaluation of Machine Learning Models for DDoS Detection in IoT Networks. 2024. DOI:10.48550/arXiv.2411.05890

11. Mohamed Y.A., Salih D.A., Khanan A. An Approach to Improving Intrusion Detection System Performance Against Low Frequent Attacks // Journal of Advances in Information Technology. 2023. Vol. 14. Iss. 3. PP. 472–478. DOI:10.12720/jait.14.3.472-478

12. Toosi A.N., Kahani M. A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers // Computer Communications. 2007. Vol. 30. Iss. 10. PP. 2201–2212. DOI:10.1016/j.comcom.2007.05.002

13. Nwasra N., Daoud M., Qaisar Z.H. ANFIS-AMAL: Android Malware Threat Assessment Using Ensemble of ANFIS and GWO // Cybernetics and Information Technologies. 2024. Vol. 24. Iss. 3. PP. 39–58. DOI:10.2478/cait-2024-0024. EDN:EIOXIL

14. Молотникова А.А. Системный анализ. Краткий курс: учебное пособие для вузов. СПб.: Лань, 2021. 212 с.

15. Ahmed A.S., Kurnaz S., Khaleel A.M. Evaluation DDoS Attack Detection Through the Application of Machine Learning Techniques on the CICIDS2017 Dataset in the Field of Information Security // Mathematical Modelling of Engineering Problems. 2023. Vol. 10. Iss. 4. PP. 1125–1134. DOI:10.18280/mmep.100404

16. Копашенко М.А., Поздняк И.С. Нейросети при защите от DDOS атак // XXX Российская научно-техническая конференция «Актуальные проблемы информатики, радиотехники и связи» (Самара, Российская Федерация, 28 февраля – 3 марта 2023 г.). Самара: ПГУТИ, 2023. С. 85–87. EDN: ZWYLIB

17. Ковалев Е.А. Применение искусственных нейронных сетей в системах обеспечения информационной безопасности // Безопасность. Управление. Искусственный интеллект. 2022. Т. 4. № 4(4). С. 26–35. EDN:THNLOH

18. Груздев А.В. Предварительная подготовка данных в Python. Т. 2. План, примеры и метрики качества. М.: ДМК Пресс, 2023. 814 с.

19. Алексейчук А.С. Введение в нейронные сети: модели, методы и программные средства. М.: МАИ, 2023. 105 с.

20. Васин Н.Н., Какабьян К.С. Сравнительный анализ методов машинного обучения для решения задачи бинарной классификации сетевого трафика // Инфокоммуникационные технологии. 2025. Т. 22. № 2. С. 20–25. DOI:10.18469/ikt.2024.22.2.03. EDN:VZCOSB

21. Назаркин О.А., Сараев П.В. Повышение эффективности параллельного обучения ансамблей аппроксиматоров на основе ненормализованного варианта моделей ANFIS // 4-я Всероссийская научно-техническая конференция «Суперкомпьютерные технологии» (СКТ-2016, Дивноморское, Российская Федерация, 19–24 сентября 2016 г.). Ростов-на-Дону: Южный федеральный университет, 2016. С. 184–188. EDN:YQTHCB

References

1. Arikova K.G. Analysis of statistical data on the implementation of cyberattacks and their consequences. *Proceedings of the All-Russian Student Scientific and Practical Conference on Digital Economy and Security, 21–22 March 2024, Moscow, Russian Federation*. Moscow: RTU MIREA Publ.; 2024. p.10–14. (in Russ.) EDN:DHNDAL

2. Baranov I.A., Kucherenko M.A., Karasev P.I. DDoS attacks and methods of protection against them. *Proceedings of the Ist National Scientific and Practical Conference on Cybersecurity: Technical and Legal Aspects of Information Protection, 24–26 May 2023, Moscow, Russian Federation*. Moscow: RTU MIREA Publ.; 2023. p.133–136. (in Russ.) EDN:BQZKRL

3. Kozlova N.Sh., Dovgal V.A. Analysis of the Use of Artificial Intelligence and Machine Learning In Cybersecurity. *Bulletin of the Adyghe State University. Series: Natural, Mathematical and Technical Sciences*. 2023;3(326):65–72. (in Russ.) DOI:10.53598/2410-3225-2023-3-326-65-72. EDN:CYUKLH

4. Lizneva Yu.S., Rostova E.V. On the application of machine learning for network anomaly classification. *Proceedings of the All-Russian Scientific and Technical Conference with International Participation on Information Processing and Mathematical Modeling, 19–20 April 2023, Novosibirsk, Russian Federation*. Novosibirsk: SibSUTI Publ.; 2023. p.58–61. (in Russ.) EDN:DILYWD

5. Popov A.S., Konstantinova A.A. Application of artificial intelligence in information security systems. *Proceedings of the All-Russian Student Scientific and Practical Conference on Mathematical Models of Technology, Techniques, and Economics, 15 May 2024, St. Petersburg, Russian Federation*. St. Petersburg: SPbGLTU Publ.; 2024. p.363–367. (in Russ.) EDN:FNVXCM

6. Rostovtsev V.S. *Artificial Neural Networks*. St. Petersburg: Lan Publ.; 2025. 216 p. (in Russ.)

7. *University of New Brunswick*. DDoS evaluation dataset (CIC-DDoS2019). URL: https://www.unb.ca/cic/datasets/ddos-2019.html [Accessed 29.03.2025]

8. Rahman M.A. Detection of distributed denial of service attacks based on machine learning algorithms. *International Journal of Smart Home*. 2020;14(2):15–24. DOI:10.21742/ijsh.2020.14.2.02. EDN:MMRDIG

9. Le D.C., Dao M.H., Nguyen K.L.T. Comparison of Machine Learning Algorithms for DDOS Attack Detection in SDN. *Information and Control Systems*. 2020;3(106):59–70. DOI:10.31799/1684-8853-2020-3-59-70. EDN:GLVTEL

10. Shakya S., Abbas R. *Comparative Evaluation of Machine Learning Models for DDoS Detection in IoT Networks*. 2024. DOI:10.48550/arXiv.2411.05890

11. Mohamed Y.A., Salih D.A., Khanan A. An Approach to Improving Intrusion Detection System Performance Against Low Frequent Attacks. *Journal of Advances in Information Technology*. 2023;14(3):472–478. DOI:10.12720/jait.14.3.472-478

12. Toosi A.N., Kahani M. A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers. *Computer Communications*. 2007;30(10):2201–2212. DOI:10.1016/j.comcom.2007.05.002

13. Nwasra N., Daoud M., Qaisar Z.H. ANFIS-AMAL: Android Malware Threat Assessment Using Ensemble of ANFIS and GWO. *Cybernetics and Information Technologies*. 2024;24(3):39–58. DOI:10.2478/cait-2024-0024. EDN:EIOXIL

14. Molotnikova A.A. *System Analysis. Short Course*. St. Petersburg: Lan Publ.; 2021. 212 p. (in Russ.)

15. Ahmed A.S., Kurnaz S., Khaleel A.M. Evaluation DDoS Attack Detection Through the Application of Machine Learning Techniques on the CICIDS2017 Dataset in the Field of Information Security. *Mathematical Modelling of Engineering Problems*. 2023;10(4):1125–1134. DOI:10.18280/mmep.100404

16. Kopashenko M.A., Pozdnyak I.S. Neural networks in DDoS attack protection. *Proceedings of the XXX Russian Scientific and Technical Conference on Current Problems of Informatics, Radio Engineering and Communications, 28 February – 3 March 2023, Samara, Russian Federation*. Samara: PSUTI Publ.; 2023. p.85–87. (in Russ.) EDN: ZWYLIB

17. Kovalev E.A. Application of Artificial Neural Networks in Information Security Systems. *Bezopasnost'. Upravlenie. Iskusstvennyj intellekt*. 2022;4(4):26–35. (in Russ.) EDN:THNLOH

18. Gruzdev A.V. *Data Preprocessing in Python. Vol. 2. Plan, Examples, and Quality Metrics*. Moscow: DMK Press Publ.; 2023. 814 p. (in Russ.)

19. Alekseychuk A.S. *Introduction to Neural Networks: Models, Methods, and Software Tools*. Moscow: MAI Publ.; 2023. 105 p. (in Russ.)

20. Vasin N.N., Kakabian K.S. Comparative Analysis of Machine Learning Methods for Network Traffic Binary Classification. *Infocommunication Technologies*. 2025;22(2):20–25. (in Russ.) DOI:10.18469/ikt.2024.22.2.03. EDN:VZCOSB

21. Nazarkin O.A., Saraev P.V. Improving the Efficiency of Parallel Training of Approximator Ensembles Based on the Unnormalized Version of ANFIS Models. *Proceedings of the 4th All-Russian Scientific and Technical Conference on Supercomputer Technologies, SCT-2016, 19–24 September 2016, Divnomorskoye, Russian Federation*. Rostov-on-Don: Southern Federal University Publ.; 2016. p.184–188. (in Russ.) EDN:YQTHCB

Статья поступила в редакцию 13.05.2025; одобрена после рецензирования 27.05.2025; принята к публикации 23.06.2025.
The article was submitted 13.05.2025; approved after reviewing 27.05.2025; accepted for publication 23.06.2025.

Информация об авторах:

ВАСИН Николай Николаевич — доктор технических наук, профессор, профессор кафедры сетей и систем связи Поволжского государственного университета телекоммуникаций и информатики
https://orcid.org/0000-0001-9749-4884

КАКАБЬЯН Карен Сергеевич — инженер технической поддержки ООО «Яндекс Облако»
https://orcid.org/0009-0000-0043-1757

Авторы сообщают об отсутствии конфликтов интересов.
The authors declare no conflicts of interests.