DOI 10.37882/2223-2966.2024.11-2.38

АНАЛИЗ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ В СИСТЕМАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

ANALYSIS OF MACHINE LEARNING METHODS FOR ANOMALY DETECTION IN INTRUSION DETECTION SYSTEMS

A. Balyberdin

Summary. Intrusion Detection Systems are widely used to detect cyberattacks on corporate data transmission network. Detecting new and unknown cyberattacks on CDTN is an important task of IDS. Anomaly detection methods are used to detect such cyberattacks.

The article presents a comparative analysis of machine learning methods used to detect anomalies in IDS. The purpose of this article is to systematize knowledge and formalize problems related to solving the problem of detecting anomalies in corporate data transmission networks (CDTN).

The analysis of scientific papers on IDS anomaly detection methods was carried out according to the following parameters: year of publication of the article, name of the methods, data set, dimension of the feature space, types of anomalies, detection accuracy, environment of use and brief conclusions. The studied anomaly detection methods were divided into two categories: classical machine learning methods and hybrid methods. For each category, seven scientific papers were selected for analysis. The criteria for selecting these papers were the completeness of the description of the studies, the date of publication, the authority of the journal and the number of publications by the author.

The result of the work is the systematization of existing knowledge, the formulation of problems and directions for further research of anomaly detection systems. The conclusions of the scientific article can be used for future research in this area.

Keywords: intrusion detection system, anomaly, machine learning methods, hybrid methods, data set, feature of data set, corporate data transmission networks, cyberattack.

Балыбердин Алексей Викторович
Аспирант, Финансовый университет при правительстве РФ, г. Москва
balyberdinav@gmail.com

Аннотация. Системы обнаружения вторжений (СОВ) широко применяются для выявления кибератак на корпоративную сеть передачи данных (КСПД). Выявление новых и неизвестных кибератак в КСПД является важной задачей СОВ. Для выявления подобных кибератак используют методы обнаружения аномалий для СОВ.

В работе выполнен сравнительный анализ методов машинного обучения, применяемых для выявления аномалий с помощью СОВ. Целью данной статьи является систематизация знаний и формализация проблем, связанных с решением задачи выявления аномалий в корпоративных сетях передачи данных (КСПД). Анализ научных работ по методам обнаружения аномалий СОВ проводился по следующим параметрам: год издания статьи, название методов, набор данных, размерность признакового пространства, типы аномалий, точность выявления, среда использования и краткие выводы. Исследуемые методы обнаружения аномалий были разделены на две категории: классические методы машинного обучения и гибридные методы. Для каждой категории были отобраны для анализа по семь научных работ. Критерием выбора данных работ была полнота описания исследований, дата публикации, авторитетность журнала и количество публикаций автора. Результатом работы является систематизация имеющихся знаний, постановка проблем и направления дальнейших исследований систем обнаружения аномалий. Выводы научной статьи могут быть использованы для будущих исследований в данной области.

Ключевые слова: система обнаружения вторжений, аномалия, методы машинного обучения, гибридные методы, набор данных, признаки набора данных, корпоративная сеть передачи данных, кибератака.

Введение

Системы обнаружения вторжений (СОВ) предназначены для выявления несанкционированных действий или вирусной активности на корпоративную сеть. В зависимости от способа выявления угроз СОВ бывают двух видов: системы сигнатурного анализа и системы обнаружения аномалий. Сигнатурный анализ СОВ выявляет злонамеренные активности на основании заранее сформированной базы знаний о кибератаках. Базы знаний представляют собой набор шаблонов и регулярных выражений известных кибератак. Для данного метода характерна точность выявления угроз. Недостатком является невозможность идентифицировать новые кибератаки. Для устранения данного недостатка активно развиваются системы обнаружения аномалий. Системы обнаружения аномалий (СОА) предназначены для выявления новых, заранее неизвестных кибератак на корпоративную сеть. Несмотря на то, что в академической сфере проведено большое количество исследований по сетевым аномалиям, на практике данные системы не получили широкого применения. Значительное количество ошибок первого и второго рода СОВ является основным ограничивающим фактором применения в реальной сети. Выделяют следующие проблемы, влияющие на точность работы СОА:

— Разнообразие и постоянные изменения признакового пространства сетевого трафика. Диверсификация и большие объемы сетевого трафика приводят к невозможности обнаружения редких сетевых аномалий.
— Интерпретация выявленных аномалий. Не каждая сетевая аномалия может рассматриваться как кибератака, поэтому необходима дополнительная их интерпретация и классификация.
— Высокая стоимость ошибки. Аналитики кибербезопасности тратят значительное время на обработку событий от СОВ, которые в большинстве случаев не является инцидентами кибербезопасности.

1. Постановка задачи

Как ранее отмечалось, что основной проблемой ограничения использования систем обнаружения аномалий (СОА) на практике является низкая точность, а также сложность интерпретации их результатов. Для повышения точности СОА применяют методы машинного обучения. В нашем исследовании, на основании сравнительного анализа различных академических работ, сделана попытка составить основные проблемы применения методов машинного обучения для выявления аномалий, а также показать актуальные и перспективные направления исследований в данной области.

2. Аномалии в сетевом трафике

Термин аномалии может быть представлен как в математическом виде [3], так и иметь точную формулировку [2].

В общем понимании, аномалия — это отклонение от нормы, от общей закономерности, которое характеризует неправильное поведение [1].

В математическом виде аномалия представляет собой отклонение от эталонных значений функции $f(t)$ характеризующей изменение сетевого трафика в любой момент времени t.

Классификация аномалий [3] представлена на рисунке 1.

В представленной классификации на рис. 1 можно отметить, что аномалии могут быть вполне легитимными и не относящимися к действиям, направленным на нарушение безопасности. Исходя из рассмотренных классификаций сделаем вывод о том, что выявленные аномалии СОА необходимо правильно классифицировать и интерпретировать как несанкционированные действия на корпоративную сеть.

3. Классификация методов обнаружения атак

Методы обнаружения атак СОВ принято разделять на следующие группы: методы злоупотреблений, методы обнаружения аномалий и гибридные методы [4].

Методы злоупотреблений (misuse detection) предназначены для обнаружения несанкционированных действий в сети с помощью базы знаний известных атак [5]. База знаний представляет собой набор шаблонов и регулярных выражения, описывающих атаки. Источником данных для базы знаний является сетевой трафик [6].

Методы обнаружения аномалий (anomaly detection) выявляют нетипичное поведение сетевого трафика. Классический способ обнаружения аномалий считается построение профиля на основе нормального поведения сетевого трафика, а отклонение от порогового значения профиля принимается за аномалию [7].

В последнее время активно проводятся исследования по обнаружению аномалий с применением методов машинного обучения. В работах [8–10] рассматриваются новые методы машинного обучения, их классификация и отмечается, что данные алгоритмы повышают точность обнаружения аномалий для СОВ.

На основании выше рассмотренных классификаций была актуализирована классификация методов обнаружения атак для СОВ. Общая классификация методов для СОВ представлена на рисунке 2.

4. Методика анализа методов обнаружения аномалий

В нашей работе проведен сравнительный анализ классических методов обнаружения аномалий с применением алгоритмов машинного обучения и гибридных методов. Гибридные методы представляют собой использование двух и более методов для обнаружения аномалий СОВ. В работе рассматриваются гибридные методы на основе алгоритмов машинного обучения.

В рамках проводимого исследования было проанализировано значительное количество работ по методам обнаружения аномалий. В рамках работы рассматривались следующие группы методов: классические методы машинного обучения и гибридные методы.

Для каждой группы были отобраны по семь исследовательских актуальных работ. Выбор работ был сделан по следующим критериям:
— Дата публикации не должна быть позднее 2019 года.
— Количество публикаций автора.
— Авторитетность журнала.

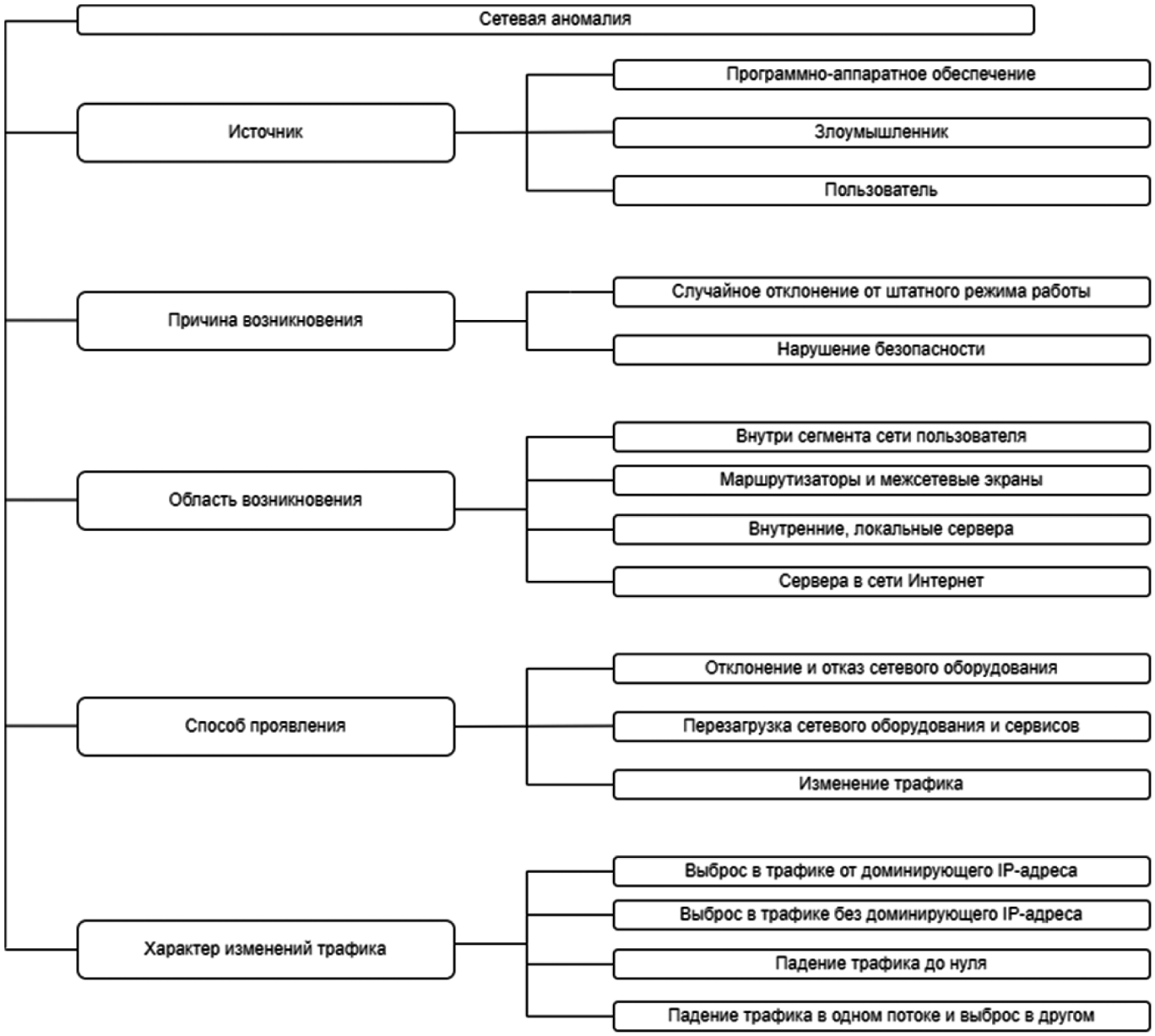

Рис. 1. Классификация аномалий

— Полнота и описание проводимых исследований и результатов.

Для анализа работ были выбраны следующие характеристики: год издания статьи, название методов, наборы данных, размерность признакового пространства, типы аномалий, точность выявления, среда применения и краткие выводы.

5. Анализ методов обнаружения аномалий на основе машинного обучения

В таблице 1 представлен сравнительный анализ методов обнаружения аномалий на основе машинного обучения. Как видно из таблицы 1, в исследованиях достаточно часто применяют эталонные наборы данных. В исследуемых работах отмечается, что полнота описания и качество разметки наборов данных, применяемых при обучении метода влияют на точность классификации. Наиболее популярными являются методы глубокого обучения, которые показывают более высокую точность классификатора. Методы машинного обучения СОВ также подвержены состязательным атакам [12]. Устойчивость методов машинного обучения СОВ к состязательным атакам недостаточно изучен и требует дополнительных исследований. Особое внимание уделяется предобработке и выборе признакового пространства, а также оптимизации гиперпараметров искусственной нейронной сети (ИНС). Следует обратить внимание, что незначительное количество исследований проведено по методам глубокого обучения с подкреплением для СОВ. Вероятно данное направление исследований бу-

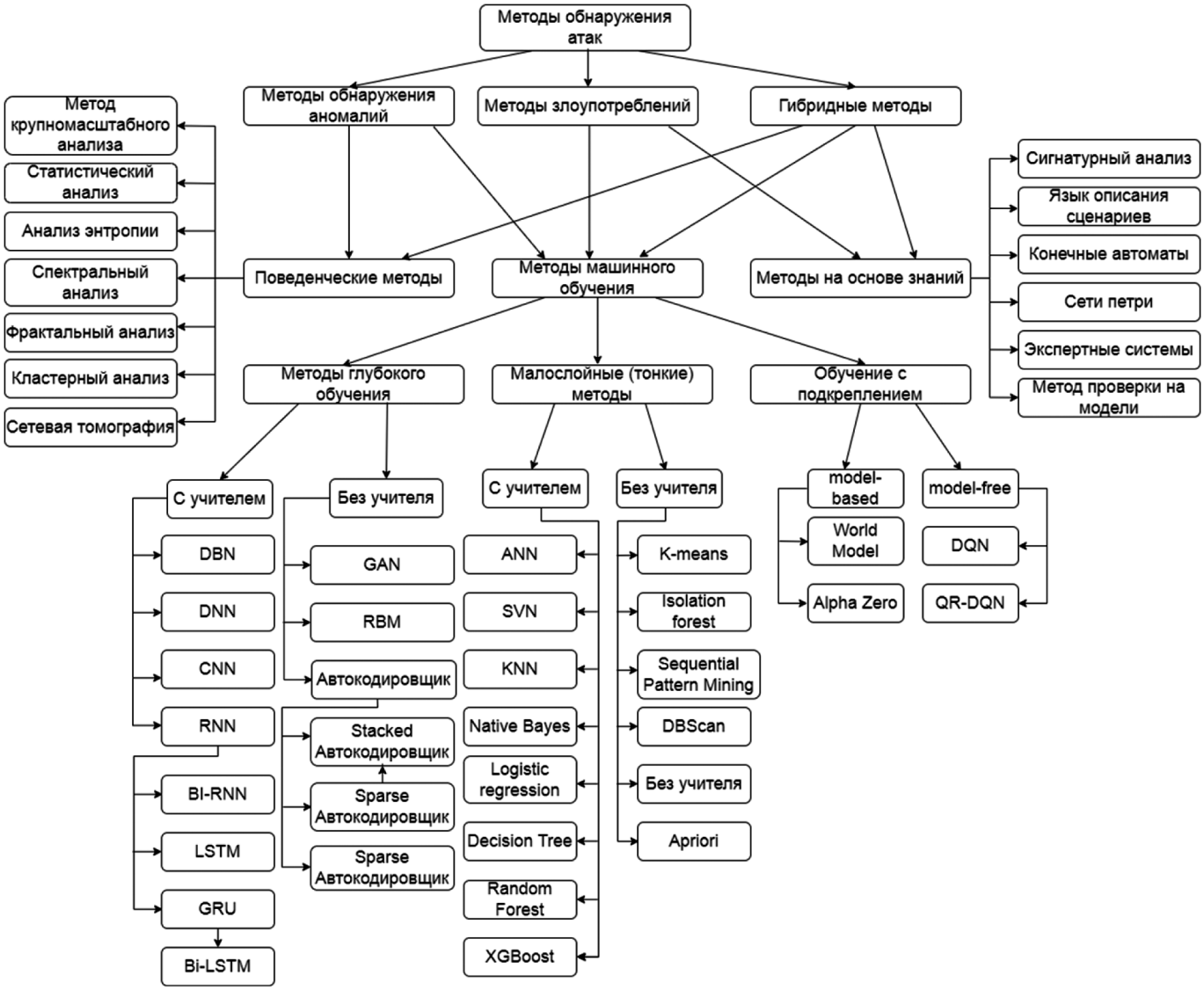

Рис. 2. Классификация методов обнаружения атак

дет боле активно развиваться для решения задач СОВ. При разработке СОВ в основном применяют следующие сетевые аномалии: DoS, Probe, Web атаки и Bruteforce.

Отметим также ряд проблем, выявленных в ходе анализа:

— Обучение методов происходит на устаревших наборах данных, тем самым наблюдается не соответствие данных реальной сети [19].
— Результаты тестирования методов показаны на одном наборе данных. В реальной сети трафик в значительной степени диверсифицирован и признаковое пространство не статично.
— Рассмотренные исследования направлены на точность классификации аномалий. Отсутствует оценка сложности алгоритмов и вычислительных ресурсов, что может влиять на практическую ценность разрабатываемых моделей.
— Отсутствует единый подход к оценке методов, что приводит в сложности проведения сравнительного анализа разрабатываемых методов.

6. Анализ гибридные методы обнаружения аномалий на основе машинного обучения

Анализ гибридных методов показал, что значительная часть исследований направлена на использование нейронных сетей в методах обнаружения аномалий. Авторы работ подчеркивают необходимость оценки методов на различных наборах данных и применением обязательной оптимизации признакового пространства. Отметим, что исследователи адаптируют методы из других сфер применения, к примеру, используют метаэвристические методы и алгоритмы распознавания текста и картинок для СОВ. Гибридный подход устраняет недостатки отдельно взятых алгоритмов, повышая тем самым точность СОВ. Анализируя даты публикации работ, можно сделать вывод, что наблюдается рост исследований гибридных

Таблица 1.

Методы обнаружения аномалий с применением машинного обучения

Название статьи	Год издания	Методы	Входные данные (дата сеты)	Количество признаков	Тип аномалий	Точность выявления	Среда	Краткие выводы
Random Forest-Based NIDS: Advancing Network Threat Detection [11]	2024	Random Forest	CICIDS-2017	5, 15, 25, 36, 46, 57	DoS Portscan Bruteforce Web Attack Bot Infiltration	Precision Accuracy Recall F1-score	network traffic	Точность классификации зависит от предобработки набора данных и от выбора признакового пространства. Несбалансированность атак в наборе данных приводит к снижению точности классификации.
Состязательные атаки против системы обнаружения вторжений, основанной на применении методов машинного обучения [12]	2023	Random Forest	CICIDS2017	Выбраны 10	Состязательные атаки HSJA Leaf Tuple ZOO Sign-OPT	Precision Accuracy Recall F1-score	network traffic	СОВ является уязвима для состязательных атак на методы машинного обучения. Мера защиты представляет собой включение в обучающийся набор состязательные атаки. Необходимо дополнительные меры защиты.
Deep Q-Learning Based Reinforcement Learning Approach for Network Intrusion Detection [13]	2022	Deep Q-Learning (DQL)	NSL-KDD	41 (выделили 4 признака)	DoS Probe U2R R2L	Precision Accuracy Recall F1-score	network traffic	Классификация с помощью DQL модели с подбором гиперпараметров показывает отличные результаты. Применение данных без предобработки (несбалансированность данных) значительно снижает точность классификации (R2L атаки).
Применение нейронных сетей в системах обеспечения информационной безопасности [14]	2021	Новая модель стохастической нейронной сети	Синтетический набор данных	-	Вредоносная активность	ROC AUC	События с инфраструктурных источников, а также события СЗИ	Выявление вредоносной активности по неструктурированным данным. Выявлена зависимость время обучения от количества нейронов. Приемлемая точность достигается за счет увеличения количества нейронов в сети (60<N<70).
Многозначная классификация компьютерных атак с использованием искусственных нейронных сетей с множественным выходом [15]	2023	Новая ANN with Multiple Output	Экспериментальный набор данных	115 признаков из них 20 вторичных и 95 первичный атрибутов	OS Scan	Precision Recall F1-score ROC AUC	Компьютерная сеть IoT	Исследована ИНС со множественными выходами при бинарной и многозначной классификации для ЭД компьютерной сети. Данная классификация показала наилучший результат. Недостатком является увеличение вычислительных ресурсов.

Окончание табл. 1

Название статьи	Год издания	Методы	Входные данные (дата сеты)	Количество признаков	Тип аномалий	Точность выявления	Среда	Краткие выводы
Синтез модели машинного обучения для обнаружения компьютерных атак на основе набора данных CICIDS2017 [16]	2020	RF (random forest)	CICIDS2017 Набор данных реальной сети	Из 84 признаков Выбрано 10	Веб-атаки (Brute Force, XSS, SQL Injection)	Accuracy Precision Recall F1	network traffic	Физические признаки сети в наборе данных значительно влияют на точность классификации. Предлагается отказаться от данных признаков с помощью методов глубокого обучения.
Artificial Intelligence based Network Intrusion Detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing [17]	2019	Artificial Neural Networks (ANN)	CSE-CIC-IDS2018	80 признаков	Brute-force Heartbleed Botnet DoS DDoS Web attacks Infiltration	Accuracy Precision Recall F1 AUC	network traffic	Выявление аномалий с помощью ИНС ANN бинарной классификации без предобработки и выбора признакового пространства набора данных.

Таблица 2.

Гибридные методы обнаружения аномалий с применением машинного обучения

Название статьи	Год издания	Методы	Входные данные (дата сеты)	Количество признаков	Тип аномалий	Точность выявления	Среда	Краткие выводы
Empirical Enhancement of Intrusion Detection Systems: A Comprehensive Approach with Genetic Algorithm-based Hyperparameter Tuning and Hybrid Feature Selection [20]	2024	XGBoost random forest, decision tree, bagging, and extra tree. Для моделей XGBoost RFгиперпараметры подбираются с помощью GA	CICIDS2017 CSECIC 2018	80 признаков (выбрали 6 для бинарной и многоклассовой моделях)	Brute Force DoS PortScan DDoS attacks	Accuracy F1 score	network traffic	Оптимизация гиперпарметров классификации привело к снижению времени обучения.
A simple framework to enhance the adversarial robustness of deep learning-based intrusion detection system [21]	2024	DLL-IDS: адаптация FNN и CNN. AE detector: local intrinsic dimensionality (LID)	CICIDS201 NSL-KDD	78 и 41 (6 статических и 35 динамических)	Состязательные атаки: CLEAN FGSM BIM DEEPFOOL CW	Precision Accuracy Recall F1-score	network traffic	Для гибридного метода получена оценка точности классификации. В исследовании применялись 5 атак. Обнаружение атаки CW выросло до 71,7% (более чем в 6 раз).
A novel network intrusion detection method based on metaheuristic optimisation algorithms [22]	2023	KNN, для выбора признаков используется MQBHOA	CSE-CIC-IDS2018 NSL-KDD	41 (выбор признаков с помощью алгоритма MQBHOA в зависимости от категории трафика)	DoS Probe U2R R2L (22 категории атак)	Precision Accuracy Recall F1-score	network traffic	Гибридизация адаптированного метаэвристического алгоритма HAO для выбора признаков в сочетании с классификацией KNN повысила точность СОВ.
A novel optimized probabilistic neural network approach for intrusion detection and categorization [23]	2023	Firefly Optimization (FFO) и Probabilistic Neural Network (PNN)	KDD-CUP 99	41	Не указаны какие атаки детектировались	Accuracy Precision Recall F1-Score Sensitivity Specificity	network traffic	Гибридизация FFO и PNN повысили точность СОВ. Тестирование на неактуальном наборе данных требуется дополнительной оценки нового метода.

Окончание табл. 2

Название статьи	Год издания	Методы	Входные данные (дата сеты)	Количество признаков	Тип аномалий	Точность выявления	Среда	Краткие выводы
Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks [24]	2023	Enhanced long-short term memory (ELSTM) Recurrent neural network (RNN)	UNSW-NB15 (KDD TEST PLUS and KDD TEST21)	38 признаков	DoS Probe R2L U2R (39 подтипов атак)	Accuracy Precision Recall F1-Score Sensitivity Specificity FAR FNR Negative presition Error rate BDR BTNR MCC Tranning time Testing time	network traffic	Гибридный метод ELSTM-RNN повышает точность СОВ и снижает время обучения классификации. Данная мотод решает проблему затухающего градиента (vanishing gradient).
Deep Learning for Intrusion Detection Systems (IDSs) in Time Series Data. [25]	2024	CNN + LSTM + ATT	UNSW-NB15	49 признаков (выбрали 44 признака)	fuzzers analysis backdoors DoS	F1-score AUC	network traffic	Набор данных преобразуется во временные ряды и поступает на вход модели состоящей из нескольких нейронных сетей CNN, LSTM и ATT.
A Hybrid Unsupervised Clustering-Based Anomaly Detection Method [26]	2021	Sub-Space Clustering (SSC) One Class Support Vector Machine (OCSVM)	NSL-KDD	41 (нет информации о выбо)	DoS Probe U2R R2L	Sensitivity Recall Detection Rate (DR) False Alarm Rate (FAR)	network traffic	Объединение кластерных алгоритма SSC и OCSVM повысила точность классификации. Данный метод имеет низкую точность выявления редких атак (U2R и R2L).

методов. В работах выделяют дополнительную оценку эффективности метода — время обучения алгоритма. Рассмотрение проблемы выявления аномалий СОВ как задачи прогнозирования временных рядов позволяет как обнаруживать аномалии, так и проактивно детектировать угрозы, поэтому несомненно стоит обратить внимание на данный подход. Для повышения точности СОВ исследования направлены на оптимизацию признаков набора данных, улучшение характеристик классификации, за счет внедрения новых алгоритмов и методик, а также подбор оптимальных параметров для ИНС.

Отметим также ряд проблем, выявленных в ходе анализа:

- Для оценки метода применяются один или два неактуальных набора данных.
- В исследованиях отсутствует информация об ограничениях и возможных проблем в работе предлагаемых методах.
- В исследованиях отсутствует единый подход к оценке эффективности методов.
- Предлагаемые методы не решают проблему низкой точности выявления редких атак и аномалий на сетевом трафике.
- Недостаточно исследований в области быстрой адаптации методов к изменяющимся параметрам среды.
- Отсутствует оценка требуемых вычислительных ресурсов для предлагаемых методов. Сложность алгоритмов и объем данных для анализа повышают требования к комплексу технических средств.

Заключение

В данной работе выполнен сравнительный анализ последних исследований в области обнаружения аномалий СОВ. В настоящее время для решения задачи выявления аномалий широко применяют гибридные методы машинного обучения, которые устраняют недостатки отдельных методов. Анализ работ показывает, что методы глубокого обучения показывают более высокую точность СОВ в отличии от других методов. Для обнаружения аномалий исследуются новые виды классификации: многозначные и прогнозирование временных рядов. Для более точной оценки методов необходимо использовать разные наборы данных в сочетании с данными реальной сети. Адаптивность методов, оптимизация признакового пространства, новые алгоритмы классификации повышают эффективность методов обнаружения аномалий. Отметим, что выявление аномалий является сложной задачей для решения которой необходимо решить следующие проблемы:

- Необходим единый подход к оценке методов.
- Низкая точность обнаружения редких атак и аномалий.
- Для практического применение методов необходима оценка вычислительных ресурсов.
- Отсутствуют данные по адаптации методов при изменении параметров среды.
- Необходим механизм принятия решений о необходимости переобучения метода или автономного изменения их параметров обучения.
- Сложность интерпретации полученных результатов от методов обнаружения аномалий СОВ.

Дальнейшие исследования будут направлены на применение новых гибридных методов машинного обучения. Усовершенствование процессов формирования, предобработки и оптимизации признакового пространства наборов данных является важной задачей для получения высокой точности классификации.

ЛИТЕРАТУРА

1. Шелухин, О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование: [текст] / О.И. Шелухин. — Москва: Горячая линия-Телеком, 2019. — 447 с.: ил. — Библиогр. в конце гл. — ISBN 978-5-9912-0756-0: Б. ц.
2. Шелухин, О.И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учебное пособие / О.И. Шелухин, Д.Ж. Сакалема, А.С. Филинова; под редакцией О.И. Шелухина. — Москва: Горячая линия-Телеком, 2018. — 220 с. — ISBN 978-5-9912-0323-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/111119.
3. Карачанская, Е.В. Метод выявления аномалий сетевого трафика, основанный на его самоподобной структуре / Е.В. Карачанская, Н.И. Соседова // Безопасность информационных технологий. — 2019. — Т. 26, № 1. — С. 98–110. — EDN YZELNB.
4. Mouhammd A., Sherenaz A.B., Intrusion Detection Systems: A State-of-the-Art Taxonomy and Survey, Arabian Journal for Science and Engineering, 2022, pp. 1–45, https://doi.org/10.1007/s13369-022-07412-1.
5. Kumar S., Spafford E.H. A Pattern Matching Model for Misuse Intrusion Detection // Proceedings of the 17th National Computer Security Conference, 1994. pp. 11–21. URL: https://www.researchgate.net/publication/2595618_A_Pattern_Matching_Model_For_Misuse_Intrusion_Detection.
6. Браницкий, А.А. Analysis and Classification of Methods for Network Attack Detection / А.А. Браницкий, И. В. Котенко // SPIIRAS Proceedings. — 2016. — No. 2(45). — P. 207–244. — DOI 10.15622/SP.45.13. — EDN VVFUQV.
7. Robin S., Vern P., Outside the Closed World: On Using Machine Learning For Network Intrusion Detection, 31st IEEE Symposium on Security and Privacy, 2010, pp. 1–12. URL: https://ieeexplore.ieee.org/document/5504793/. DOI: 10.1109/SP.2010.25.
8. Mouhammd A., Sherenaz A. B., Intrusion Detection Systems: A State-of-the-Art Taxonomy and Survey, Arabian Journal for Science and Engineering, 2022, pp. 1–45, https://doi.org/10.1007/s13369-022-07412-1.

9. Ansam K., Iqbal G., Peter V., Joarder K., Survey of intrusion detection systems: techniques, datasets and challenges, 2019, pp. 1–22, https://doi.org/10.1186/s42400-019-0038-7.
10. Barrish D. van Vuuren J.H., A Taxonomy Of Univariate Anomaly Detection Algorithms For Predictive Maintenance, South African Journal of Industrial Engineering November 2023 Vol 34(3), pp 28–42. DOI:10.7166/34-3-2943.
11. Mohammed Tarek Abdelaziz, Abdelrahman Radwan, Hesham Mamdouh, Adel Saeed Saad, Abdulrahman Salem Abuzaid, Ahmed Ayman AbdElhakeem, Salma Zakzouk, Kareem Moussa and M. Saeed Darweesh, Random Forest-Based NIDS: Advancing Network Threat Detection, Springer Nature, August 2024, pp 1–32, https://doi.org/10.1109/TSMCC.2008.923876.
12. Состязательные атаки против системы обнаружения вторжений, основанной на применении методов машинного обучения / А.И. Гетьман, М.Н. Горюнов, А.Г. Мацкевич [и др.] // Проблемы информационной безопасности. Компьютерные системы. — 2023. — № 4(57). — С. 156–190. — DOI 10.48612/jisp/eatr-5pxb-akt8. — EDN XTMDJV.
13. Hooman Alavizadeh, Julian Jang-Jaccard, Hootan Alavizadeh, Deep Q-Learning based Reinforcement Learning Approach for Network Intrusion Detection, Computers 2022, 11, 41, https://doi.org/10.3390/computers11030041.
14. Применение нейронных сетей в системах обеспечения информационной безопасности / А.В. Плугатарев, А.Л. Марухленко, М.А. Бугорский [и др.] // Безопасность информационных технологий. — 2021. — Т. 28, № 3. — С. 73–80. — DOI 10.26583/bit.2021.3.06. — EDN UQKGHV.
15. Шелухин О.И., Раковский Д.И. Многозначная классификация компьютерных атак с использованием искусственных нейронных сетей с множественным выходом. Труды учебных заведений связи. 2023;9(4):97–113. https://doi.org/10.31854/1813-324X-2023-9-4-97-113.
16. Горюнов, М.Н. Синтез модели машинного обучения для обнаружения компьютерных атак на основе набора данных CICIDS2017 / М.Н. Горюнов, А.Г. Мацкевич, Д.А. Рыболовлев // Труды Института системного программирования РАН. — 2020. — Т. 32, № 5. — С. 81–94. — DOI 10.15514/ISPRAS-2020-32(5)-6. — EDN FFAPFH.
17. V. Kanimozhi and T.P. Jacob, «Artificial Intelligence based Network Intrusion Detection with Hyper-Parameter Optimization Tuning on the Realistic Cyber Dataset CSE-CIC-IDS2018 using Cloud Computing,» 2019 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2019, pp. 0033–0036, doi: 10.1109/ICCSP.2019.8698029.
18. G. Pu, L. Wang, J. Shen and F. Dong, «A hybrid unsupervised clustering-based anomaly detection method,» in Tsinghua Science and Technology, vol. 26, no. 2, pp. 146–153, April 2021, doi: 10.26599/TST.2019.9010051.
19. Балыбердин, А.В. Особенности общедоступных наборов данных сетевого трафика для обнаружения аномалий / А.В. Балыбердин // Телекоммуникации и информационные технологии. — 2024. — Т. 11, № 1. — С. 24–30. — EDN NRDQHO.
20. Bakır, H., Ceviz, Ö. Empirical Enhancement of Intrusion Detection Systems: A Comprehensive Approach with Genetic Algorithm-based Hyperparameter Tuning and Hybrid Feature Selection. Arab J Sci Eng 49, 13025–13043 (2024). https://doi.org/10.1007/s13369-024-08949-z.
21. Xinwei Yuan, Shu Han, Wei Huang, Hongliang Ye, Xianglong Kong, Fan Zhang, A simple framework to enhance the adversarial robustness of deep learning-based intrusion detection system, Computers & Security, Volume 137, 2024, 103644, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2023.103644.
22. Ghanbarzadeh, R., Hosseinalipour, A. & Ghaffari, A. A novel network intrusion detection method based on metaheuristic optimisation algorithms. J Ambient Intell Human Comput 14, 7575–7592 (2023). https://doi.org/10.1007/s12652-023-04571-3.
23. Nadir Omer, Ahmed H. Samak, Ahmed I. Taloba, Rasha M. Abd El-Aziz, A novel optimized probabilistic neural network approach for intrusion detection and categorization, Alexandria Engineering Journal, Volume 72, 2023, Pages 351–361, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2023.03.093.
24. A.A. E.-B. Donkol, A.G. Hafez, A.I. Hussein and M.M. Mabrook, «Optimization of Intrusion Detection Using Likely Point PSO and Enhanced LSTM-RNN Hybrid Technique in Communication Networks», in IEEE Access, vol. 11, pp. 9469–9482, 2023, doi: 10.1109/ACCESS.2023.3240109.
25. Psychogyios, K.; Papadakis, A.; Bourou, S.; Nikolaou, N.; Maniatis, A.; Zahariadis, T. Deep Learning for Intrusion Detection Systems (IDSs) in Time Series Data. Future Internet 2024, 16, 73. https://doi.org/10.3390/ fi16030073.
26. G. Pu, L. Wang, J. Shen and F. Dong, «A hybrid unsupervised clustering-based anomaly detection method,» in Tsinghua Science and Technology, vol. 26, no. 2, pp. 146–153, April 2021, doi: 10.26599/TST.2019.9010051.