Обзорная статья
УДК 004.056
DOI: 10.26583/bit.2025.1.11

ПОВЫШЕНИЕ ТОЧНОСТИ ВЫЯВЛЕНИЯ АНОМАЛИЙ ДЛЯ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЯ С ПОМОЩЬЮ АНСАМБЛЕВОГО ОБУЧЕНИЯ

Алексей В. Балыбердин[1], Григорий О. Крылов[2]
Финансовый университет при правительстве РФ, пр–кт Ленинградский, 49/2, Москва, 125167, Россия
[1]balyberdinav@gmail.com, https://orcid.org/0009-0005-1264-9290
[2]op50@mail.ru, https://orcid.org/0000-0001-8145-1994

Аннотация. Выявление аномалий системой обнаружения вторжений (СОВ) является сложной задачей. Значительное количество ошибок детектирования аномалий снижает эффективность применения СОВ. Повышение точности СОВ рассматривается как решение задачи классификации. Для решения задачи классификации применяют нейронные сети, методы глубокого обучения, статистические модели машинного обучения и многое другое. Одним из способов решения данной задачи является применение ансамблевого обучения для алгоритмов классификации. Широкое применение ансамблевого обучения в различных областях подтверждает эффективность ансамблей. Целью статьи является систематизация знаний по методам ансамблевого обучения, способах их применения для построения современных СОВ и формулировка задач для будущих исследований. В статье используется метод сравнительного анализа при рассмотрении различных исследований. Описана методология выбора работ. В соответствии с методологией были выбраны двенадцать работ. Рассмотрены широко используемые ансамбли обучения и их классификация, приводятся результаты исследования современных методов и алгоритмов СОВ с применением ансамблей. Ансамбли решают различные проблемы классификации, показаны оптимальные алгоритмы ансамблей для решения задачи классификации. Для СОВ выделены базовые метрики оценки и наборы данных, которые предлагается использовать при разработке методов. Метаэвристичекие и генетические алгоритмы применяются не только для решения задач выбора признаков, но и для генерации базовых классификаторов. Сформулированы задачи, которые решают ансамбли, и предложено направление для будущих исследований с применением ансамблевого обучения.

Ключевые слова: *система обнаружения вторжений, аномалия, ансамблевое обучение, нейронная сеть, обнаружение аномалий, базовые классификаторы, алгоритм.*

Для цитирования: *Балыбердин, Алексей В.; Крылов, Григорий О. Повышение точности выявления аномалий для систем обнаружения вторжения с помощью ансамблевого обучения. Безопасность информационных технологий, [S.l.], т. 32, № 1, с. 153–171, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1753. DOI: http://dx.doi.org/10.26583/bit.2025.1.11.*

Review article

ENHANCING ANOMALY DETECTION ACCURACY FOR INTRUSION DETECTION SYSTEMS USING ENSEMBLE LEARNING

Aleksei V. Balyberdin[1], Grigory O. Krylov[2]
Financial University under the Government of the Russian Federation,
Leningradsky Ave., 49/2, Moscow, 125993, Russia
[1]balyberdinav@gmail.com, https://orcid.org/0009-0005-1264-9290
[2]op50@mail.ru, https://orcid.org/0000-0001-8145-1994

Abstract. Anomaly detection by an intrusion detection system (IDS) is a difficult task. A significant number of anomaly detection errors reduces the effectiveness of IDS. Improving the accuracy of IDS is

considered as a solution to the classification problem with a teacher. A solving the classification problem, neural networks, deep learning models, statistical models of machine learning and many others are studied. One of the ways for solving this problem is to use ensemble learning for classification algorithms. The widespread use of ensemble learning in various fields confirms the effectiveness of ensembles. The aim of the work is to systematize knowledge on ensemble learning methods, how to use them to build modern IDS and formulate problems for future research. The paper uses the comparative analysis method when considering various studies. The methodology for selecting the work is described in Chapter 3. Based on the methodology, twelve works were selected. The paper considers widely used learning ensembles and their classification. In the course of the work, a study is conducted on modern IDS methods and algorithms using ensembles. Ensembles solve various classification problems. The study shows the optimal ensemble algorithms for solving the classification problem. Basic evaluation metrics and data sets are identified for the IDS, which are proposed to be used in the development of methods. Metaheuristic and genetic algorithms are used not only to solve feature selection problems, but also to generate basic classifiers. In conclusion, the paper formulates the problems that ensembles solve, and also suggests a direction for future research using ensemble learning.

Keywords: *intrusion detection system, anomaly, ensemble learning, neural networks, anomaly detection, base learning, algorithm.*

For citation: *Balyberdin, Aleksei V.; Krylov, Grigory O. Enhancing anomaly detection accuracy for intrusion detection systems using ensemble learning. IT Security (Russia), [S.l.], v. 32, no. 1, p. 153–171, 2025. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1753. DOI: http://dx.doi.org/10.26583/bit.2025.1.11.*

Введение

С развитие информационных систем, технологий, средств вычислительной техники появляются новые угрозы информационной безопасности. Реализация кибератак может привести к значительным финансовым и репутационным потерям в организации. В настоящее время особенно остро стоят задачи по обеспечению информационной безопасности на объектах критичной инфраструктуры (КИИ) и в финансовых организациях. Для решения данных задач ведутся работы по совершенствованию способов защиты информации. Разрабатываются и внедряются новые средства защиты информации (СЗИ). Одним из таких СЗИ являются системы обнаружения вторжений (СОВ), предназначенные для обнаружения несанкционированных действий злоумышленника в сети. В зависимости от способа детектирования кибератак и злонамеренных действий, системы обнаружения вторжений можно разделить на следующие типы систем: системы сигнатурного анализа (СА), системы обнаружения аномалий (СОА) и гибридные системы.

Наибольшее распространение получили системы сигнатурного анализа, которые на основе имеющейся базы знаний способны выявлять атаки по заранее подготовленным паттернам, правилам и сигнатурам. Данная категория СОВ позволят с высокой точностью выявлять известные кибератаки. Постоянный рост кибератак ставит невозможность выполнить описание всех кибератак и оперативно поддерживать актуальное состояние базы знаний СОВ. Для решения данной проблемы подходят системы обнаружения аномалий, которые выявляют неизвестные атаки на сетевом трафике [1]. Несмотря на большое количество академических исследований, СОА не получило широкого распространения в связи с низкой точностью обнаружения аномалий и интерпретируемости результатов работы системы. Для повышения точности СОА исследователи решают следующие задачи:

- Дисбаланс классов в наборе данных [2].
- Оптимизация признакового пространства [3].
- Избыточность, нормализация и фильтрация данных [4].
- Разработка новых архитектур и алгоритмом классификации [5].
- Объяснение и интерпретация результатов работы методов [6].
- Оценка точности методов обнаружения аномалий [7].
- Дрифт концепций [8].

В данной работе исследованы алгоритмы ансамблевого обучения, в том числе ансамбль классификаторов, как один из способов повышения эффективности классификации для СОВ.

1. Постановка задачи

Для повышения точности классификации СОА применяют алгоритмы глубокого машинного обучения, совершенствуют методики обнаружения аномалий, применяют гибридные подходы к решению подобных задач [9].

В исследовании рассматривается ансамблевое обучение как способ повышения точности классификации СОВ. Основная идея ансамбля заключается в объединении или выборе комбинации базовых классификаторов в общий классификатор, содержащий более точный прогноз в отличии от отдельных независимых классификаторов. Считается, что алгоритм классификации для многоклассового набора данных не может обеспечить точный прогноз по всем классам набора данных [10–11].

Основной мотивацией написания данной статьи заключается в систематизации современных подходов для решения задачи классификации с помощью ансамблевого обучения, оценки эффективности предложенных решений, а также формулировке задач и проблем для дальнейших исследований.

Основной вклад авторов заключается в следующем:

- Выполнена систематизация известных методов ансамблевого обучения.
- Проведен сравнительный анализ современных подходов для решения проблем точности и надежности методов СОВ с помощью ансамблевого обучения.
- Предложены алгоритмы ансамблевого обучения для оптимального решения задач классификации.
- Сформулированы задачи для дальнейших исследований с применение ансамблей обучения.

2. Особенности ансамблевого обучения

Под ансамблевым обучением (Ensemble Learning) понимается комбинация различных алгоритмов, объединяющихся в один, который является более эффективным и точным алгоритмом [12]. Ансамбль классификаторов является частным случаем ансамблевого обучения. Ансамбль классификаторов разделен на отдельные базовые классификаторы. В [12] представлена методика с базовыми классификаторами с применением интеграционного метода ансамбля голосования Voting. Увеличение количества классификаторов в методе привело к возрастанию вычислительной нагрузке на СОВ. Современные СОВ обладают необходимыми ресурсами для практической реализации алгоритмов ансамблевого обучения для обнаружения аномалий, поэтому алгоритмы ансамблей применимы для СОВ [13].

В исследованиях показано, что ансамблевое обучение повышает точность классификатора [14]. Однако, ансамбль и комбинация классификаторов не всегда повышают эффективность модели [15]. К факторам, влияющим на ансамбль классификаторов относят разнообразие ошибок [16], методы классификации [17] и интеграции [13].

Для ансамбля классификаторов можно выделить следующие проблемы, влияющие на точность классификатора:

- Агрегация базовых классификаторов.
- Интеграция или объединение результатов работы классификаторов.
- Генерация разнообразия набора базовых классификаторов.
- Формирование качественного набора данных.

Ансамблевое обучение можно представить в виде процесса, который состоит из трех этапов:

– *Генерация разнообразия наборов базовых классификаторов*. На данном этапе формируется набор базовых классификаторов с различными параметрами.

– *Выбор базовых классификаторов*. При выборе классификаторов применяют различные алгоритмы объединения (используют все базовые классификаторы или их подмножество).

– *Интеграция или объединение результатов прогноза классификаторов*. Для интеграции применяют различные алгоритмы объединения результатов работы отдельных классификаторов.

Как выше отмечено ансамбль обучения широко применяется для решения различных задач. В особенности алгоритмы применяются для задач классификации в качестве создания ансамбля классификаторов [18]. В данной работе ансамбль классификаторов используется для объединения результатов в отдельный классификатор, тем самым повышается прогноз классификации. Объединение результатов базовых классификаторов является основной задачей применение ансамблей.

В [19] с помощью ансамбля обучения решается проблема дрифта концепций. Дрифт концепций возникает во времени при изменении статистических свойств целевой переменной, которую предсказывает модель. Данная проблема особенно проявляется при работе с потоком данных в режиме реального времени.

Для решения рассмотренных задач применяют различные алгоритмы ансамбля обучения. На рис. 1 представлена классификация основных алгоритмов ансамблевого обучения в соответствии с процессом их обучения. Алгоритмы ансамблей разделены на три группы: селективные ансамбли обучения (Selective Ensemble Learning), общие методы ансамблевого обучения (Ensemble learning methods) и интеграционные или объединяющие ансамбли (Integration Ensemble Learning).

Селективные ансамбли на основе различных алгоритмов выбирают подмножество базовых классификаторов для повышения эффективности модели [20]. К данной группе относятся кластерные (Clustering-based methods), упорядоченные (ordering-based methods) и оптимизационные методы (optimization-based methods).

Кластерные методы используются на начальном этапе для необработанных данных, когда отсутствуют необходимые знания для классификации [21]. Основная идея кластерных методов – объединение в группы схожих между собой данных. Метод эффективен для необработанных данных, когда необходимо упорядочить данные по группам и определить наборы данных для дальнейшей их классификации.

Упорядоченные методы или методы сокращения [22] выполняют упорядочивание и отбрасывание не подходящих базовых классификаторов для повышения эффективности модели.

Оптимизационные методы [23] в отличии от упорядоченных методов не сокращают, а повышают разнообразие базовых классификаторов для выбора оптимальной комбинации с наилучшим результатом классификации. Метаэвристические методы являются оптимизационными методами и широко используются для разработки методов выявления аномалий для систем обнаружения вторжений [24].

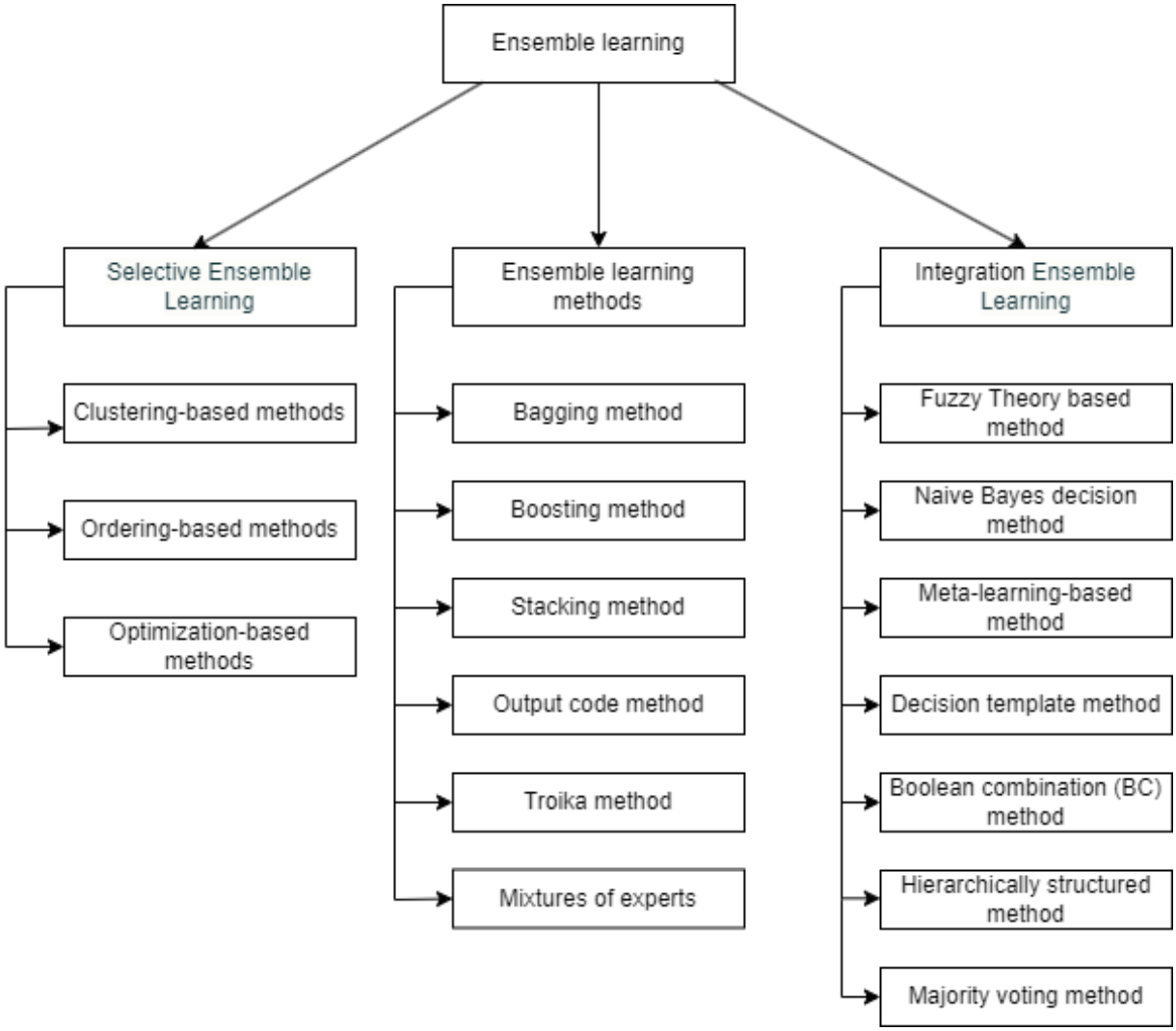

Рис. 1. Классификация ансамблей обучения

Методы ансамблевого обучения (Ensemble learning methods) в отличии от селективного ансамбля используют все базовые классификаторы для повышения эффективности модели. К данной группе методов относятся bagging, boosting, stacking и другие методы.

Метод bagging первоначально был предложен в [25]. Данный метод был разработан для обеспечения стабильности набора классификаторов. Для метода классификаторы обучаются на различных подмножествах исходного набора данных. Подмножество данных формируется случайным распределением исходного набора данных. Отметим, что обобщение базовых классификаторов выполняется с помощью метода голосования [26]. Наиболее известные алгоритмы: Random forest и Wagging метод.

Метод boosting впервые предложен в [27]. В работе показан метод, в котором последовательность слабых алгоритмов преобразуется в сильный классификатор. Бустинг предполагает повторное использование набора данных с последующим объединение результатов с помощью голосования. Развитием данного метода стал популярный алгоритм AdaBoost, который применяется в том числе в СОВ.

Метод stacking используется для стекированного обобщения разнородных алгоритмов в метаобучающегося (meta-learner) [29]. Стекирование выполняет поиск наиболее подходящих базовых классификаторов для дальнейшего обучения

метаклассификатора meta-learner. Данный алгоритм не так широко применяется в отличии от bagging и boosting. Разнородность базовых классификаторов приводится к нелинейному обучению метаклассификатора. Одной из проблем считается, что различие моделей базовых классификаторов может приводить к снижению эффективности метаклассификатора.

Метод Output code method выполняет манипуляции с кодированием классов для задачи классификации [30]. Данный метод выполняет генерацию классификатора с исправлением ошибок базовых классификаторов. Задачи многоклассовой классификации разбиваются на двухклассовую классификацию и агрегируются результаты для меток классов.

Метод troika улучшает эффективность и решает проблемы алгоритма stacking [31]. Универсальность метода заключается в возможности объединения любых типов базовых классификаторов, обученных на любой выборке класса набора данных.

Метод Mixtures of experts (смесь экспертов) выполняет повторную агрегацию базовых классификаторов под наблюдение монитора. Монитор выбирает лучшие базовые классификаторы на основе входных данных [32].

Для выявления аномалий на сетевом трафике наиболее широко используемыми методами являются алгоритмы bagging, boosting и stacking. Данные методы имеют различные архитектуры и выбор алгоритма зависит от используемых базовых классификаторов.

Группа методов Integration Ensemble Learning это алгоритмы объединения результатов базовых классификаторов.

Метод Fuzzy Theory основан на теории нечетких множеств. Результирующий классификатор формируется на основе нечетких агрегационных связей [33].

Метод Naive Bayes decision базовые классификаторы рассматриваются как независимые и классификатор выбирает максимальную вероятность базового классификатора рассчитанного по теореме Байеса [34].

Метод Meta-learning-based использует более высокий уровень классификации, которые также необходимо обучать на основе выходных данных базовых классификаторов [35]. Примером является рассмотренный выше метод stacking.

Метод Decision template method основан на сходстве прототипных ответов с экземплярами данных [36].

Метод Boolean combination (BC) используется для вычисления булевой функции с использованием методов ANR, OR и т.п. [37]. Простота вычислений позволяет снизить вычисления для задач классификации.

Метод Hierarchically structured представляет собой различные этапы классификации. На первом этапе базовые классификаторы рассматривают как независимые классификаторы. На втором этапе применяются алгоритмы для объединения базовых классификаторов [38].

Метод Majority voting каждому базовому классификатору назначает определенный голос. Метод выбирает соответствующий класс на основе максимального количества голосов [39].

Интеграционные методы важны и широко используются при разработке моделей классификации для выявления аномалий. Методы направлены на повышение эффективности классификации. Выбор интеграционного метода зависит от решаемой задачи. К примеру, метод голосования эффективен для объединения базовых классификаторов. Для задач дисбаланса данных оптимально применять методы бэггинга и бустинга.

3. Описание методики анализа работ ансамбля классификаторов

В данной работе представлен сравнительный анализ современных исследований с использование ансамблей классификаторов. В анализе были выбраны различные архитектуры для построения ансамблей классификаторов: последовательные и параллельные архитектуры. Ансамбли классификаторов применялись для выявления аномалий в системах обнаружения вторжений. Область исследования в работах являются события сетевого трафика, события IoT и события облачных систем.

В ходе работы было рассмотрено значительное количество исследований, но для сравнительного анализа было выбрано двенадцать работ [40–51]. В данной работе рассматривались научные статьи и конференции. Доклады и презентации коммерческих организаций не рассматривались. Основной задачей исследования является анализ подходов применения ансамбля классификаторов для СОВ.

Для анализа были сформулированы следующие вопросы:

1) Какие методы и архитектуры ансамблей наиболее широко используются?
2) Какие задачи решают методы ансамбли классификаторов?
3) Какие наборы данных используются для обучения и тестирования?
4) Какие оценки используются для анализа эффективности метода?
5) Какие алгоритмы используются совместно с ансамблями для повышения точности методов?

Выбор работ выполнялся по следующей методике:

– Индекс цитируемости статьи и квартиль журнала (Q1, Q2). Квартиль журналов определялся из базы рейтинга журналов SJR (Scimago Journal & Country Rank).

– Полнота описания исследования. Структурность исследования и проводимого эксперимента.

– Дата публикации не более четырех лет.

– Методы и алгоритмы ансамблей рассматривались для систем обнаружения вторжений.

Для поиска работ использовались следующие база данных: elibrary.ru, springer nature link, science direct, scopus и scholar.

Отметим, что в научной электронной библиотеке elibrary.ru отсутствуют работы по ансамблевому обучению для систем обнаружения вторжений.

4. Анализ методов ансамблей классификаторов для СОВ

Ансамбль классификаторов широко используется для повышения эффективности классификации. В табл. 1 представлен список выбранных работ для сравнительного анализа.

Наиболее цитируемым источником является [40] от 2020 г., наименее цитируемый [41], так как статья вышла совсем недавно. Отметим, что наибольшее количество исследования проводится в Китае, а в западных странах исследования для системы обнаружения вторжения с применением ансамбля классификаторов не так актуально. Несмотря на это, актуальность темы выявления аномалий СОВ подтверждается регулярными обзорными статьями в ведущих научных журналах [52, 53].

Рассматривая процессы предобработки и наборы данных можно заметить, что для сетевого трафика наиболее популярные являются наборы данных UNSW-NB15 и CICIDS-2017, для IoT трафика различная модификация x-IoT наборов данных. Популярность наборов данных UNSW-NB15 и CICIDS-2017 обсуждается в [54]. Основная причина является то, что наборы UNSW-NB15 и CICIDS-2017 имеют лучшую разметку данных, достаточно полное описание данных и необходимое количество данных для обучения алгоритмов. Собственный набор данных [41] используется достаточно редко, так как

возникают проблемы с получением реальных данных, а также с необходимостью формирования наборов данных для обучения, валидации и тестирования.

Таблица 1. Список работ для сравнительного анализа

№	Статья	Год публи-кации	Авторы публикаций	Страна	Цити-рование	База поиска	Журнал
1	[40]	2020	Yuyang Zhou, Guang Cheng, Shanqing Jiang, Mian Dai	Китай	413	Science Direct	Computer Networks
2	[41]	2024	Han, M., Li, C., Meng, F.	Китай	0	Springer	Knowledge and Information Systems
3	[42]	2024	Liu, Y.,Zhu, L.,Ding, L.	Китай	2	Springer	Scientifc Reports
4	[43]	2024	Ali Mohammed Alsafar, Mostafa Nouri-Baygi, Hamed M. Zolbanin	Иран, Ирак, США	1	Springer	Journal of Big Data
5	[44]	2022	Vinayakumar Ravi, Rajasekhar Chaganti, Mamoun Alazab	Саудовская Аравия, США, Австралия	110	Science Direct	Computers and Electrical Engineering
6	[45]	2023	Ruyue Xin, Hongyun Liu & Zhiming Zhao	Нидерланды	27	Science Direct	Journal of Cloud Computing
7	[46]	2024	Amru, M., Jagadeesh Kannan, R., Narasimhan Ganesh, E., Muthumarilakshmi, S., Padmanaban, K., Jeyapriya, J., & Murugan, S.	Индия	39	Scholar	International Journal of Electrical and Computer Engineering (IJECE)
8	[47]	2024	Yakub Kayode Saheed Sanjay Misra	Норвегия, Испания	18	Springer	International Journal of Information Security
9	[48]	2023	Thockchom, N., Singh, M.M. & Nandi, U.	Индия	36	Springer	Complex & Intelligent Systems
10	[49]	2023	M. M. Shtayat, M. K. Hasan, R. Sulaiman, S. Islam and A. U. R. Khan	Малайзия, Бангладеш, Оман	15	IEEE	IEEE Access
11	[50]	2023	Ali, M., Haque, Mu., Durad, M.H.	Пакистан, Исламабад, Англия, Саудовская Аравия	14	Springer	International Journal of Information Security
12	[51]	2023	Ankit Thakka Ritika Lohiya	Индия	58	IEEE	IEEE internet of things journal

Для этапа предобработки выделяют следующие операции, выполняемые с данными: преобразование данных, нормализация и фильтрация данных. Наиболее популярный метод SMOTE используется для решения задач дисбаланса данных. Отметим, что большинство исследований направлено на совершенствование алгоритмов классификации данных, поэтому для дальнейшего улучшения методов можно сфокусироваться на решении проблем дисбаланса классов данных. В [48] обсуждается о необходимости синтетической генерации событий для меньших классов. Проблему дисбаланса данных предлагают решить с помощь ансамбля обучения [51]. Отметим, что LLM для генерации синтетических данных показывает достаточно хорошие результаты [55]. Поэтому применение генеративных

алгоритмов для подготовки обучающихся наборов данных является перспективным направлением для решения задач дисбаланса в наборах данных (табл. 2).

Таблица 2. Наборы данных и предобработка

№	Статья	DataSet	Предобработка	Методы выбора признаков	Тип классификации трафика	Область применения
1	[40]	NSL-KDD, AWID, CIC-IDS2017	Фильтрация, преобразование в числовые значения и нормализация	Metaheuristic optimization algorithm CFS-BA	Многоклассовая (многомерная)	Сетевой трафик
2	[41]	Синтетические и реальные данные	SMOTE для дисбаланса данных	–	Многоклассовая	Сетевой трафик
3	[42]	Page blocks, Satimage-2, KDDCUP99, BATADAL, SWaT, Power	Сэмплирования данных	–	Многоклассовая	Сетевой трафик и UCI database
4	[43]	UNSW-NB15, CICIDS2017	Фильтрация данных, Преобразование данных в значения, Нормализация данных	Гибридный метод MI-Boruta	Многоклассовая, бинарная	Сетевой трафик
5	[44]	SDN-IoT, KDD-Cup-1999, UNSW-NB15, WSN-DS, and CICIDS-2017	Нет	KPCA	Многоклассовая	Сетевой трафик: CPS + SDN
6	[45]	DApp monitoring data, SMD data, Vichalana data Метрики мониторинга инфраструктуры	Нет	PCA	Бинарная	Облачная платформа
7	[46]	IoT-NI	Нет	–	Многоклассовая	IoT
8	[47]	BoT-IoT and UNSW-NB15	Нормализация данных, SMOTE для дисбаланса данных	IG + PCA	Многоклассовая, бинарная	IoT
9	[48]	KDD Cup 1999, UNSW-NB15 and CIC-IDS2017	Нормализация данных, преобразование данных в числовые значения, удаление неполных данных	Chi-Square test	Многоклассовая, бинарная	Сетевой трафик
10	[49]	ToN-IoT	Нормализация данных, преобразование данных в числовые значения, удаление неполных данных	–	Многоклассовая, бинарная	IoT
11	[50]	CIPMAIDS2023-1	Нормализация данных, преобразование данных в числовые значения, удаление неполных данных Smote для дисбаланса данных	Cicflowmeter	Многоклассовая	Сетевой трафик
12	[51]	NSL-KDD UNSW_NB-15 CIC-IDS-2017 BoT-IoT	Нормализация данных, преобразование данных в числовые значения, удаление неполных данных	–	Многоклассовая	IoT Сетевой трафик

Для выбора признаков используют два подхода: классический с применение одного алгоритма [45] и гибридизация алгоритмов [43]. В [40] для выбора признаков используют оптимизационный метаэвристический алгоритм CFS-BA. Метаэвристические алгоритмы селективного ансамбля показывают отличные результаты в области информационных технологий, в медицине, в финансовом менеджменте и другие областях [14]. Также метаэвристика показывает отличные результаты при выборе признаков [40, 47]. Широкое применение также получил алгоритм PCA [44, 45, 47]. Это объясняется тем, что алгоритм прост в реализации и достаточно эффективно при выборе признаков. Применение метаэвристических алгоритмов с их гибридизацией недостаточно изучено, поэтому несомненно стоит обратить внимание исследователей на данное направление исследований.

Для классификации событий используется многоклассовая классификация. Несмотря на это, в исследованиях также оценивается бинарная классификация [45, 48, 49]. Ансамбль классификаторов с применением параллельной архитектуры [42] показывает приемлемые результаты для многоклассовой классификации. В [54] для повышения точности классификации автор предлагает использовать один тип аномалии, тем самым подтверждается, что многоклассовая классификация неэффективна при использовании только одного алгоритма классификации в методе. Поэтому применение ансамблей классификаторов для многоклассовой классификации является эффективным решением для задачи классификации.

Для каждой из рассмотренных работ были составлены краткие выводы (табл. 3). Отметим, что ансамбли обучения применяются для решения следующих задач: повышение точности классификация за счет выбора оптимального результата базовых классификаторов [40, 49, 51], решение задач дрифта концепций [41] и задачи дисбаланса данных [42, 50, 51]. Ансамблевое обучение применяется для задачи дисбаланса данных на уровне алгоритмов в отличии от наиболее известного метода SMOTE [41]. Одной из важных проблем является интерпретация получаемых результатов. Для решения данной задачи в [49] применяют метод XAI (генетический алгоритм). Данный метод показал хороший результаты для обобщения и интерпретации результатов классификации.

В табл. 4 представлен сравнительный анализ ансамблей классификаторов. В основном используются две стратегии ансамблей для СОВ: integration (объединение) и ансамблевое обучение. Базовые классификаторы (Base Learning) представлены нейронными сетями. Для ансамблей классификаторов характерно разнообразие используемых алгоритмов в качестве базовых. В результате предлагаемые фреймворки являются более устойчивыми, но повышая количество base learning алгоритмов увеличиваются вычислительные ресурсы для СОВ. В ансамблевом обучении (Ensemble Learning) широко используются следующие методы: бэггинговые алгоритмы [41, 51], бустинговый XGBOOST [50] и метаобучающийся (MLP) [43]. Отдельно отметим параллельные алгоритмы SEAD-PL [42]. Как отмечалось ранее, параллельные архитектуры алгоритмов с использованием ансамблей классификаторов повышают эффективность алгоритмов и снижают время вычисления. Рассматривая интеграционные методы ансамблей, отметим применение нескольких стратегий [41]. В [41] применение двух стратегий для решения задач дрейфа концепции и дисбаланса данных в сравнении с другими методами показывают лучший результат. В данном случае ансамбль выступает в качестве связки двух различных задач классификации. Интеграционные методы voting [40], stacking [43] и boosting [46] являются наиболее широко используемыми методами. Простота реализации и качество получаемых результатов, несомненно, являются одними из главных критериев популярности данных методов.

Таблица 3. Краткие выводы по статьям

№	Статья	Краткие выводы	Решаемая задача
1	[40]	Предлагаемые методы сравниваются на трех наборах данных. В работе представлены отличные результаты метода в сравнении с другими алгоритмами. Отсутствует информация по редким атакам.	Повышение точности классификации за счёт алгоритмов оптимизации признаков и ансамбля классификаторов
2	[41]	Предлагаемый метод повысил эффективность классификации в несбалансированных классах. Метод требует значительные вычислительные ресурсы и обладает низкой устойчивостью.	Взаимосвязь двух задач дрифта концепций и дисбаланса данных повышает эффективность классификации
3	[42]	Применение параллельного обучения с последующей классификацией событий снижают время вычисления, но увеличивают вычислительные ресурсы. Селективный ансамбль выбора базовых классификаторов повысил эффективность классификации. В работе не представлены результаты оценок по классам.	Решение проблемы дисбаланса набора данных, снижения времени на вычисления
4	[43]	Для решения проблемы классификации применяется алгоритм ансамбля stacking. Данный метод показал низкие результаты классификации для малых классов. Отмечается трудность в интерпретации аномалий.	Решение проблемы избыточности данных и проблемы выбора признаков. Ансамбль для решения проблемы классификации трафика
5	[44]	Для извлечения признаков применяется гибридизация нейронных сетей и алгоритма KPCA. Набор данных поступает на вход базовых классификаторов с последующим обучением метаклассификатора.	Повышение точности классификации решается с помощью гибридизации алгоритмов для признакового пространства с обучением метаклассифактора
6	[45]	Оценка нового метода ELBD выполнена по трем метрикам: точность, надежность и прогнозируемость. Выполнено сравнение на трех наборах данных.	Повышается точность метода с помощью разработки нового фреймворка
7	[46]	В работе показано сравнение XGBoosting с другими алгоритмами для IoT трафика. XGBoosting показал лучший результат на IoT.	Повышение точности классификации за счет использования метода XGBoosting
8	[47]	Для повышения точности классификации используется метаэвристический алгоритм GWO для настройки гиперпараметров алгоритмов. Выполнено сравнение точности модели с другими методами. Алгоритмы метаэвристики помогают оптимизировать гиперпараметры алгоритмов, повышая эффективность классификации.	Повышение точности с помощью ансамбля классификаторов и метаэвристического алгоритма подбора гиперпараметров для базовых классификаторов.
9	[48]	В работе не рассматривается проблема дисбаланса данных, что приводит в низкой точности детектирования малых классов. Предложенный метод показывает хорошие результаты для бинарной классификации. В работе рассматривается только оценка точности классификации.	Для улучшения классификации применяют стекирование отдельных базовых классификаторов
10	[49]	Применение ансамбля классификаторов для бинарной и многоклассовой классификации повысило точность выявления атак. Методы XAI необходимы для повышения уровня интерпретации результатов.	Улучшение классификации за счет применения ансамбля. Задача интерпретации результатов решается с помощью методов XAI
11	[50]	Для повышения точности используется метод stacking ансамблевого обучения. Необходима оценка устойчивости метода.	Повышение точности за счет применения ансамблевого обучения
12	[51]	В работе применяют метода bagging ансамблевого обучения для решения проблемы несбалансированность данных. Дисбаланс данных предлагают решать на уровне алгоритмов, которые не зависят от входных данных.	Решение проблемы дисбаланса данных с помощью ансамблевого обучения

Таблица 4. Ансамбли классификаторов

№	Статья	Стратегия ансамбля	Base Learning	Ensemble Learning	Integration method	Тип классификации	Метод оценки
1	[40]	Integration	C4.5, RF, ForestPA		vote classifier	Много-классовая (много-мерная)	Acc, Precision, DR, F-Measure, ADR, FAR, MBT
2	[41]	Integration	Random Subspace Hoeffding tree (Random Subspace HT). Количество 10	Adaptive online bagging (AdaOB) ensemble	стратегии: 1) combining two ensemble update strategies 2) weighted ensemble strategy	Много-классовая	TPR, TNR, Precision, Recall, G-mean, F1-score
3	[42]	Clustering-based ensemble selection strategy	Back Propagation (BP) Neural Network Algorithm	Parallel learning (SEAD-PL)	clustering-based ensemble selection strategy	Много-классовая	AUC, ROC
4	[43]	Integration	Random forest (RF), Catboost, XGBoost	Multilayer perceptron (MLP) as the meta-learner	stacked ensemble learning - meta learner	Много-классовая, бинарная	accuracy, recall, precision, F1-Score, false positive rate, true positive rate, error rate
5	[44]	Ensemble learning	RNN, GRU, LSTM, KPCA, random forest, SVM		stacked ensemble learning	Много-классовая	Accuracy Precision Recall F1 score
6	[45]	Ensemble learning	IForest, KNN, LOF, OCSVM		Linear ensemble methods and deep ensemble method	Бинарная	Accuracy, Prediction, Robustness, F1-score
7	[46]	Ensemble learning	XGBoosting		boosting	Много-классовая	Precision, Recall F1-Score, support
8	[47]	Integration	RF, DT, MLP, and KNN		voting ensemble	Много-классовая, бинарная	Accuracy, DR Precision, ROC FAR
9	[48]	Ensemble learning	Gaussian naive Bayes (GNB), decision tree (DT), logistic regression (LR)	Stacking ensemble: meta-classifier stochastic gradient descent (SGD)	stacking ensemble	Много-классовая, бинарная	Precision Recall F1 score Accuracy
10	[49]	Integration	CNN (3 сети) ELM model Shapley Additive explanations (SHAP), Local Interpretable Model-Agnostic Explanations (LIME)	Hard voting	voting ensemble	Много-классовая, бинарная	Accuracy Precision Recall F-Score Error Sensitivity Specificity
11	[50]	Ensemble learning	SVM (Linear) SVM (RBF); KNN RF; Logistic Regression	Meta learner: XGBOOST	stacking ensemble	Много-классовая	Precision Recall Weighted F1-score
12	[51]	Ensemble learning	DNN с классом весов	Bagging	bagging ensemble	Много-классовая	accuracy, precision, recall, and f-score FPR

В качестве основных способов оценки методов можно выделить следующие метрики: Accuracy, Precision, Recall, F1 score. Интерпретация метрик и оценка результатов значительного количества исследований приводит к необходимости руководствоваться данными метриками при разработке новых моделей. Использование данных метрик носит рекомендательный характер.

Алгоритмы ансамблей обучения являются одними из способов повышения точности классификации. Генерация базовых классификаторов тоже является важной задачей на пути к повышению эффективности методов. Каждый базовый классификатор содержит начальное состояние, которое определяется значениями гиперпараметров. В [47] используется метаэвристический алгоритм GWO для определения базовых классификаторов. Подбор гиперпараметров влияет на точность классификации. Эффективность представленного способа также обсуждается в [57], в которой настройка базовых классификаторов выполняется с помощью генетического алгоритма GA. Гибридизация методов ансамбля классификаторов и подбор гиперпараметров базовых классификаторов повышает эффективность метода.

Заключение

Ансамблевое обучение применяется в различных областях для решения задач классификации. Ансамбли также широко используются при разработке методов СОВ. Для СОВ ансамбли помогают решать следующие задачи: дисбаланс классов данных, генерация базовых классификаторов, дрифт концепций, повышение точности классификации с помощью объединения и селективности базовых классификаторов.

Дисбаланс классов данных эффективно решать с помощью ансамблевого обучения bagging. Для генерации базовых классификаторов выделяют оптимизационные метаэвртистические алгоритмы селективного ансамбля GWO и генетического алгоритма GA. Дрифт концепций можно снизить с помощью bagging метода. Наиболее популярные методы объединения считаются метаклассификтор и голосование. Двухуровневая ансамблевая стратегия показывает хорошие результаты для классификации в режиме реального времени. В связи с развитием вычислительных ресурсов широкое распространение получило построение параллельных архитектур базовых классификаторов для которых применяются селективные стратегии ансамблей.

Ансамбли классификаторов повышают эффективность многоклассовой классификации и являются оптимальным решением. Базовыми оценками методов можно считать следующие метрики: Accuracy, Precision, Recall, F1 score. Самые популярные наборы данных являются UNSW-NB15 и CICIDS-2017. Базовые метрики и эталонные наборы данных можно рассматривать в качестве сравнения результатов при разработке новых методов СОВ.

В рассмотренных исследованиях ансамбли используются для решения одной выбранной задачи. Применение ансамблей для решения связанных между собой задач в настоящее время недостаточно изучен. Влияние алгоритмов и ансамблей, а также их гибридизация является на наш взгляд перспективным направлением исследований для решения задач классификации применительно к СОВ.

СПИСОК ЛИТЕРАТУРЫ

1. Шелухин, О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. М.: Горячая линия-Телеком, 2019. – 447 с.: ил. ISBN 978-5-9912-0756-0.
2. Neha Gupta, Vinita Jindal, Punam Bedi, LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system, Computer Networks, Volume 192, 2021, 108076, ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.108076.

3. 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). DOI: https://doi.org/10.1007/s13369-024-08949-z.
4. 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. V.137, 2024, 103644, ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2023.103644.
5. 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.DOI: https://doi.org/10.31854/1813-324X-2023-9-4-97-113.
6. Tarek Ali and Panos Kostakos. 2023. HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs). arXiv:2309.16021 [cs.CR]. DOI: https://doi.org/10.48550/arXiv.2309.16021.
7. Sommer R. and Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, Oakland, CA, USA. 2010, p. 305–316. DOI: 10.1109/SP.2010.25.
8. Lu J., Liu A., Dong F., Gu F., Gama J. and Zhang G. Learning under Concept Drift: A Review. IEEE Transactions on Knowledge and Data Engineering, v. 31, no. 12, p. 2346-2363, 1 Dec. 2019. DOI: 10.1109/TKDE.2018.2876857.
9. Pu G., Wang L., Shen J. and Dong F. A hybrid unsupervised clustering-based anomaly detection method. Tsinghua Science and Technology, v. 26, no. 2, p. 146–153, April 2021. DOI: 10.26599/TST.2019.9010051.
10. Rob McKay, Brian Pendleton, James Britt, and Ben Nakhavanit. 2019. Machine Learning Algorithms on Botnet Traffic: Ensemble and Simple Algorithms. In Proceedings of the 2019 3rd International Conference on Compute and Data Analysis (ICCDA '19). Association for Computing Machinery, New York, NY, USA, 31–35. DOI: https://doi.org/10.1145/3314545.3314569.
11. Chand N., Mishra P., Krishna C.R., Pilli E.S. and Govil M.C. A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection. 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), Dehradun, India. 2016, p. 1–6. DOI: 10.1109/ICACCA.2016.7578859.
12. Yuyang Zhou, Guang Cheng, Shanqing Jiang, Mian Dai, Building an efficient intrusion detection system based on feature selection and ensemble classifier, Computer Networks. 2020, v. 174, 107247, ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2020.107247.
13. Rezk, S.S., Selim, K.S. Metaheuristic-based ensemble learning: an extensive review of methods and applications. Neural Comput & Applic 36, 17931–17959 (2024). DOI: https://doi.org/10.1007/s00521-024-10203-4.
14. Jinping Liu, Jiezhou He, Wuxia Zhang, Tianyu Ma, Zhaohui Tang, Jean Paul Niyoyita, Weihua Gui, ANID-SEoKELM: Adaptive network intrusion detection based on selective ensemble of kernel ELMs with random features, Knowledge-Based Systems. 2019, v. 177, p. 104–116. ISSN 0950-7051. DOI: https://doi.org/10.1016/j.knosys.2019.04.008.
15. Kuncheva, L.I., Whitaker, C.J. Measures of Diversity in Classifier Ensembles and Their Relationship with the Ensemble Accuracy. Machine Learning 51, 181–207 (2003). DOI: https://doi.org/10.1023/A:1022859003006.
16. Gavin Brown, Jeremy Wyatt, Rachel Harris, Xin Yao, Diversity creation methods: a survey and categorisation,Information Fusion. 2005, v. 6, Issue 1, p. 5–20, ISSN 1566-2535. DOI: https://doi.org/10.1016/j.inffus.2004.04.004.
17. Alpaydin E. ombining Pattern Classifiers: Methods and Algorithms (Kuncheva, L.I.; 2004) [book review]. IEEE Transactions on Neural Networks, v. 18, no. 3, p. 964–964, May 2007. DOI: 10.1109/TNN.2007.897478.
18. Yuyang Zhou, Guang Cheng, Shanqing Jiang, Mian Dai. Building an efficient intrusion detection system based on feature selection and ensemble classifier, Computer Networks. 2020, v. 174, 107247, ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2020.107247.
19. Minku L.L. and Yao X. DDD: A New Ensemble Approach for Dealing with Concept Drift. IEEE Transactions on Knowledge and Data Engineering, v. 24, no. 4, p. 619–633, April 2012. DOI: 10.1109/TKDE.2011.58.
20. Sagi, O., & Rokach, L. (2018). Ensemble learning: A survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 8(4), e1249. DOI: 10.1002/widm.1249.
21. Tossapon Boongoen, Natthakan Iam-On, Cluster ensembles: A survey of approaches with recent extensions and applications, Computer Science Review. 2018, v. 28, p. 1–25, ISSN 1574-0137. DOI: https://doi.org/10.1016/j.cosrev.2018.01.003.
22. Gonzalo Martínez-Muñoz and Alberto Suárez. 2006. Pruning in ordered bagging ensembles. In Proceedings of the 23rd international conference on Machine learning (ICML '06). Association for Computing Machinery, New York, NY, USA, 609–616. DOI: https://doi.org/10.1145/1143844.1143921.

23. Amgad M. Mohammed, Enrique Onieva, Michał Woźniak. Selective ensemble of classifiers trained on selective samples. Neurocomputing. 2022, v. 482, p. 197–211, ISSN 0925-2312. DOI: https://doi.org/10.1016/j.neucom.2021.11.045.
24. 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). DOI: https://doi.org/10.1007/s12652-023-04571-3.
25. Breiman L (1996) Bias, variance, and arcing classifers (technical report 460). Department of Statistics. University of California at Berkeley. URL: http://digicoll.lib.berkeley.edu/record/86021 (дата обращения: 10.11.2024).
26. Wenyu Zhang, Dongqi Yang, Shuai Zhang, A new hybrid ensemble model with voting-based outlier detection and balanced sampling for credit scoring, Expert Systems with Applications. V. 174, 2021, 114744, ISSN 0957-4174. DOI: https://doi.org/10.1016/j.eswa.2021.114744.
27. Schapire, R.E. The strength of weak learnability. Mach Learn 5, 197–227 (1990). DOI: https://doi.org/10.1007/BF00116037.
28. Xu M., Baraldi P., Lu X. and Zio E. Generative Adversarial Networks With AdaBoost Ensemble Learning for Anomaly Detection in High-Speed Train Automatic Doors. IEEE Transactions on Intelligent Transportation Systems. V. 23, no. 12, p. 23408–23421, Dec. 2022. DOI: 10.1109/TITS.2022.3203871.
29. David H. Wolpert, Stacked generalization, Neural Networks 1992, v. 5, Issue 2, p. 241–259, ISSN 0893-6080. DOI: https://doi.org/10.1016/S0893-6080(05)80023-1.
30. Kumar G, Kumar K (2012) The use of artifcial-intelligence-based ensembles for intrusion detection: a review. Appl Comput Intell Soft Comput 2012:1–20. DOI: https://doi.org/10.1155/2012/850160.
31. Eitan Menahem, Lior Rokach, Yuval Elovici, Troika – An improved stacking schema for classification tasks,Information Sciences. 2009, v. 179, Issue 24, p. 4097–4122, ISSN 0020-0255. DOI: https://doi.org/10.1016/j.ins.2009.08.025.
32. Yao X. and Islam M.M. Evolving artificial neural network ensembles. IEEE Computational Intelligence Magazine, v. 3, no. 1, p. 31–42, February 2008. DOI: 10.1109/MCI.2007.913386.
33. Awotunde, J.B., Ayo, F.E., Panigrahi, R. et al. A Multi-level Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks. Int J Comput Intell Syst 16, 31 (2023). DOI: https://doi.org/10.1007/s44196-023-00205-w.
34. Wang, S., Jiang, L. & Li, C. Adapting naive Bayes tree for text classification. Knowl Inf Syst 44, 77–89 (2015). DOI: https://doi.org/10.1007/s10115-014-0746-y.
35. Vettoruzzo A., Bouguelia M.-R., Vanschoren J., Rögnvaldsson T. and Santosh K. Advances and Challenges in Meta-Learning: A Technical Review. IEEE Transactions on Pattern Analysis and Machine Intelligence. V. 46, no. 7, p. 4763–4779, July 2024. DOI: 10.1109/TPAMI.2024.3357847.
36. Matteo Re, Giorgio Valentini. Integration of heterogeneous data sources for gene function prediction using decision templates and ensembles of learning machines. Neurocomputing. 2010, v. 73, Issues 7–9, p. 1533–1537, ISSN 0925-2312. DOI: https://doi.org/10.1016/j.neucom.2009.12.012.
37. Wael Khreich, Eric Granger, Ali Miri, Robert Sabourin. Iterative Boolean combination of classifiers in the ROC space: An application to anomaly detection with HMMs Pattern Recognition. 2010, v. 43, Issue 8, p. 2732–2752, ISSN 0031-3203. DOI: https://doi.org/10.1016/j.patcog.2010.03.006.
38. Guan, Y., Myers, C.L., Hess, D.C. et al. Predicting gene function in a hierarchical context with an ensemble of classifiers. Genome Biol 9 (Suppl 1), S3 (2008). DOI: https://doi.org/10.1186/gb-2008-9-s1-s3.
39. Aeeneh S., Zlatanov N. and Yu J. New Bounds on the Accuracy of Majority Voting for Multiclass Classification. IEEE Transactions on Neural Networks and Learning Systems. DOI: 10.1109/TNNLS.2024.3387544.
40. Yuyang Zhou, Guang Cheng, Shanqing Jiang, Mian Dai, Building an efficient intrusion detection system based on feature selection and ensemble classifier, Computer Networks. V. 174, 2020, 107247, ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2020.107247.
41. Han, M., Li, C., Meng, F. et al. An online ensemble classification algorithm for multi-class imbalanced data stream. Knowl Inf Syst 66, 6845–6880 (2024). URL: https://ezpro.fa.ru:2117/10.1007/s10115-024-02184-6 (дата обращения: 10.11.2024).
42. Liu, Y., Zhu, L., Ding, L. et al. Selective ensemble method for anomaly detection based on parallel learning. Sci Rep 14, 1420 (2024). DOI: https://doi.org/10.1038/s41598-024-51849-3.
43. Alsaffar, A.M., Nouri-Baygi, M. & Zolbanin, H.M. Shielding networks: enhancing intrusion detection with hybrid feature selection and stack ensemble learning. J Big Data 11, 133 (2024). URL: https://ezpro.fa.ru:2117/10.1186/s40537-024-00994-7 (дата обращения: 10.11.2024).
44. Vinayakumar Ravi, Rajasekhar Chaganti, Mamoun Alazab, Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system, Computers and Electrical Engineering. V. 102, 2022, 108156, ISSN 0045-7906. DOI: https://doi.org/10.1016/j.compeleceng.2022.108156.

45. Xin, R., Liu, H., Chen, P. et al. Robust and accurate performance anomaly detection and prediction for cloud applications: a novel ensemble learning-based framework. J Cloud Comp 12, 7 (2023). DOI: https://doi.org/10.1186/s13677-022-00383-6.
46. Amru, M., Jagadeesh Kannan, R., Narasimhan Ganesh, E., Muthumarilakshmi, S., Padmanaban, K., Jeyapriya, J., & Murugan, S. (2024). Network intrusion detection system by applying ensemble model for smart home. International Journal of Electrical and Computer Engineering (IJECE), 14(3), 3485-3494. DOI: http://doi.org/10.11591/ijece.v14i3.pp3485-3494.
47. Saheed, Y.K., Misra, S. A voting gray wolf optimizer-based ensemble learning models for intrusion detection in the Internet of Things. Int. J. Inf. Secur. 23, 1557–1581 (2024). URL: https://ezpro.fa.ru:2117/10.1007/s10207-023-00803-x (дата обращения: 10.11.2024).
48. Thockchom, N., Singh, M.M. & Nandi, U. A novel ensemble learning-based model for network intrusion detection. Complex Intell. Syst. 9, 5693–5714 (2023). DOI: https://doi.org/10.1007/s40747-023-01013-7.
49. Shtayat M.M., Hasan M.K., Sulaiman R., Islam S. and Khan A.U.R. An Explainable Ensemble Deep Learning Approach for Intrusion Detection in Industrial Internet of Things. IEEE Access. 2023, v. 11, p. 115047–115061. DOI: 10.1109/ACCESS.2023.3323573.
50. Ali, M., Haque, Mu., Durad, M.H. et al. Effective network intrusion detection using stacking-based ensemble approach. Int. J. Inf. Secur. 22, 1781–1798 (2023). DOI: https://doi.org/10.1007/s10207-023-00718-7.
51. Thakkar A. and Lohiya R. Attack Classification of Imbalanced Intrusion Data for IoT Network Using Ensemble-Learning-Based Deep Neural Network. IEEE Internet of Things Journal. V. 10, no. 13, p. 11888–11895, 1 July1, 2023. DOI: 10.1109/JIOT.2023.3244810.
52. Abdulganiyu, O.H., Ait Tchakoucht, T. & Saheed, Y.K. A systematic literature review for network intrusion detection system (IDS). Int. J. Inf. Secur. 22, 1125–1162 (2023). DOI: https://doi.org/10.1007/s10207-023-00682-2.
53. Zahra Zamanzadeh Darban, Geoffrey I. Webb, Shirui Pan, Charu Aggarwal, and Mahsa Salehi. 2024. Deep Learning for Time Series Anomaly Detection: A Survey. ACM Comput. Surv. 57, 1, Article 15 (January 2025), 42 p. DOI: https://doi.org/10.1145/3691338.
54. Балыбердин, А.В. Особенности общедоступных наборов данных сетевого трафика для обнаружения аномалий. Телекоммуникации и информационные технологии. 2024, т. 11, № 1, с. 24–30. – EDN: NRDQHO.
55. Gopali S., Abri F., Siami Namin A. and Jones K.S. The Applicability of LLMs in Generating Textual Samples for Analysis of Imbalanced Dataset. IEEE Access, v. 12, p. 136451–136465, 2024. DOI: 10.1109/ACCESS.2024.3463400.
56. Горюнов М.Н., Мацкевич А.Г., Рыболовлев Д.А. Синтез модели машинного обучения для обнаружения компьютерных атак на основе набора данных CICIDS2017. Труды Института системного программирования РАН. 2020;32(5):81-94. DOI: https://doi.org/10.15514/ISPRAS-2020-32(5)-6.
57. 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). DOI: https://doi.org/10.1007/s13369-024-08949-z.

REFERENCES:

[1] Sheluxin, O.I. Setevy`e anomalii. Obnaruzhenie, lokalizaciya, prognozirovanie. M.: Goryachaya liniya-Telekom, 2019. – 447 s. ISBN 978-5-9912-0756-0 (in Russian).
[2] Neha Gupta, Vinita Jindal, Punam Bedi, LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system, Computer Networks, Volume 192, 2021, 108076, ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2021.108076.
[3] 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). DOI: https://doi.org/10.1007/s13369-024-08949-z.
[4] 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. V.137, 2024, 103644, ISSN 0167-4048. DOI: https://doi.org/10.1016/j.cose.2023.103644.
[5] Shelukhin O., Rakovsky D. Multivalued Classification of Computer Attacks Using Artificial Neural Networks with Multiple Outputs. Proceedings of Telecommunication Universities. 2023;9(4):97-113. DOI: https://doi.org/10.31854/1813-324X-2023-9-4-97-113 (in Russian).
[6] Tarek Ali and Panos Kostakos. 2023. HuntGPT: Integrating Machine Learning-Based Anomaly Detection and Explainable AI with Large Language Models (LLMs). arXiv:2309.16021 [cs.CR]. DOI: https://doi.org/10.48550/arXiv.2309.16021.

[7] Sommer R. and Paxson V. Outside the Closed World: On Using Machine Learning for Network Intrusion Detection. IEEE Symposium on Security and Privacy, Oakland, CA, USA. 2010, p. 305–316. DOI: 10.1109/SP.2010.25.

[8] Lu J., Liu A., Dong F., Gu F., Gama J. and Zhang G. Learning under Concept Drift: A Review. IEEE Transactions on Knowledge and Data Engineering, v. 31, no. 12, p. 2346-2363, 1 Dec. 2019. DOI: 10.1109/TKDE.2018.2876857.

[9] Pu G., Wang L., Shen J. and Dong F. A hybrid unsupervised clustering-based anomaly detection method. Tsinghua Science and Technology, v. 26, no. 2, p. 146–153, April 2021. DOI: 10.26599/TST.2019.9010051.

[10] Rob McKay, Brian Pendleton, James Britt, and Ben Nakhavanit. 2019. Machine Learning Algorithms on Botnet Traffic: Ensemble and Simple Algorithms. In Proceedings of the 2019 3rd International Conference on Compute and Data Analysis (ICCDA '19). Association for Computing Machinery, New York, NY, USA, 31–35. DOI: https://doi.org/10.1145/3314545.3314569.

[11] Chand N., Mishra P., Krishna C.R., Pilli E.S. and Govil M.C. A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection. 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), Dehradun, India. 2016, p. 1–6. DOI: 10.1109/ICACCA.2016.7578859.

[12] Yuyang Zhou, Guang Cheng, Shanqing Jiang, Mian Dai, Building an efficient intrusion detection system based on feature selection and ensemble classifier, Computer Networks. 2020, v. 174, 107247, ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2020.107247.

[13] Rezk, S.S., Selim, K.S. Metaheuristic-based ensemble learning: an extensive review of methods and applications. Neural Comput & Applic 36, 17931–17959 (2024). DOI: https://doi.org/10.1007/s00521-024-10203-4.

[14] Jinping Liu, Jiezhou He, Wuxia Zhang, Tianyu Ma, Zhaohui Tang, Jean Paul Niyoyita, Weihua Gui, ANID-SEoKELM: Adaptive network intrusion detection based on selective ensemble of kernel ELMs with random features, Knowledge-Based Systems. 2019, v. 177, p. 104–116. ISSN 0950-7051. DOI: https://doi.org/10.1016/j.knosys.2019.04.008.

[15] Kuncheva, L.I., Whitaker, C.J. Measures of Diversity in Classifier Ensembles and Their Relationship with the Ensemble Accuracy. Machine Learning 51, 181–207 (2003). DOI: https://doi.org/10.1023/A:1022859003006.

[16] Gavin Brown, Jeremy Wyatt, Rachel Harris, Xin Yao, Diversity creation methods: a survey and categorisation,Information Fusion. 2005, v. 6, Issue 1, p. 5–20, ISSN 1566-2535. DOI: https://doi.org/10.1016/j.inffus.2004.04.004.

[17] Alpaydin E. ombining Pattern Classifiers: Methods and Algorithms (Kuncheva, L.I.; 2004) [book review]. IEEE Transactions on Neural Networks, v. 18, no. 3, p. 964–964, May 2007. DOI: 10.1109/TNN.2007.897478.

[18] Yuyang Zhou, Guang Cheng, Shanqing Jiang, Mian Dai. Building an efficient intrusion detection system based on feature selection and ensemble classifier, Computer Networks. 2020, v. 174, 107247, ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2020.107247.

[19] Minku L.L. and Yao X. DDD: A New Ensemble Approach for Dealing with Concept Drift. IEEE Transactions on Knowledge and Data Engineering, v. 24, no. 4, p. 619–633, April 2012. DOI: 10.1109/TKDE.2011.58.

[20] Sagi, O., & Rokach, L. (2018). Ensemble learning: A survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 8(4), e1249. DOI: 10.1002/widm.1249.

[21] Tossapon Boongoen, Natthakan Iam-On, Cluster ensembles: A survey of approaches with recent extensions and applications, Computer Science Review. 2018, v. 28, p. 1–25, ISSN 1574-0137. DOI: https://doi.org/10.1016/j.cosrev.2018.01.003.

[22] Gonzalo Martínez-Muñoz and Alberto Suárez. 2006. Pruning in ordered bagging ensembles. In Proceedings of the 23rd international conference on Machine learning (ICML '06). Association for Computing Machinery, New York, NY, USA, 609–616. DOI: https://doi.org/10.1145/1143844.1143921.

[23] Amgad M. Mohammed, Enrique Onieva, Michał Woźniak. Selective ensemble of classifiers trained on selective samples. Neurocomputing. 2022, v. 482, p. 197–211, ISSN 0925-2312. DOI: https://doi.org/10.1016/j.neucom.2021.11.045.

[24] 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). DOI: https://doi.org/10.1007/s12652-023-04571-3.

[25] Breiman L (1996) Bias, variance, and arcing classifers (technical report 460). Department of Statistics. University of California at Berkeley. URL: http://digicoll.lib.berkeley.edu/record/86021 (accessed: 10.11.2024).

[26] Wenyu Zhang, Dongqi Yang, Shuai Zhang, A new hybrid ensemble model with voting-based outlier detection and balanced sampling for credit scoring, Expert Systems with Applications. V. 174, 2021, 114744, ISSN 0957-4174. DOI: https://doi.org/10.1016/j.eswa.2021.114744.

[27] Schapire, R.E. The strength of weak learnability. Mach Learn 5, 197–227 (1990). DOI: https://doi.org/10.1007/BF00116037.

[28] Xu M., Baraldi P., Lu X. and Zio E. Generative Adversarial Networks With AdaBoost Ensemble Learning for Anomaly Detection in High-Speed Train Automatic Doors. IEEE Transactions on Intelligent Transportation Systems. V. 23, no. 12, p. 23408–23421, Dec. 2022. DOI: 10.1109/TITS.2022.3203871.
[29] David H. Wolpert, Stacked generalization, Neural Networks 1992, v. 5, Issue 2, p. 241–259, ISSN 0893-6080. DOI: https://doi.org/10.1016/S0893-6080(05)80023-1.
[30] Kumar G, Kumar K (2012) The use of artifcial-intelligence-based ensembles for intrusion detection: a review. Appl Comput Intell Soft Comput 2012:1–20. DOI: https://doi.org/10.1155/2012/850160.
[31] Eitan Menahem, Lior Rokach, Yuval Elovici, Troika – An improved stacking schema for classification tasks,Information Sciences. 2009, v. 179, Issue 24, p. 4097–4122, ISSN 0020-0255. DOI: https://doi.org/10.1016/j.ins.2009.08.025.
[32] Yao X. and Islam M.M. Evolving artificial neural network ensembles. IEEE Computational Intelligence Magazine, v. 3, no. 1, p. 31–42, February 2008. DOI: 10.1109/MCI.2007.913386.
[33] Awotunde, J.B., Ayo, F.E., Panigrahi, R. et al. A Multi-level Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks. Int J Comput Intell Syst 16, 31 (2023). DOI: https://doi.org/10.1007/s44196-023-00205-w.
[34] Wang, S., Jiang, L. & Li, C. Adapting naive Bayes tree for text classification. Knowl Inf Syst 44, 77–89 (2015). DOI: https://doi.org/10.1007/s10115-014-0746-y.
[35] Vettoruzzo A., Bouguelia M.-R., Vanschoren J., Rögnvaldsson T. and Santosh K. Advances and Challenges in Meta-Learning: A Technical Review. IEEE Transactions on Pattern Analysis and Machine Intelligence. V. 46, no. 7, p. 4763–4779, July 2024. DOI: 10.1109/TPAMI.2024.3357847.
[36] Matteo Re, Giorgio Valentini. Integration of heterogeneous data sources for gene function prediction using decision templates and ensembles of learning machines. Neurocomputing. 2010, v. 73, Issues 7–9, p. 1533–1537, ISSN 0925-2312. DOI: https://doi.org/10.1016/j.neucom.2009.12.012.
[37] Wael Khreich, Eric Granger, Ali Miri, Robert Sabourin. Iterative Boolean combination of classifiers in the ROC space: An application to anomaly detection with HMMs Pattern Recognition. 2010, v. 43, Issue 8, p. 2732–2752, ISSN 0031-3203. DOI: https://doi.org/10.1016/j.patcog.2010.03.006.
[38] Guan, Y., Myers, C.L., Hess, D.C. et al. Predicting gene function in a hierarchical context with an ensemble of classifiers. Genome Biol 9 (Suppl 1), S3 (2008). DOI: https://doi.org/10.1186/gb-2008-9-s1-s3.
[39] Aeeneh S., Zlatanov N. and Yu J. New Bounds on the Accuracy of Majority Voting for Multiclass Classification. IEEE Transactions on Neural Networks and Learning Systems. DOI: 10.1109/TNNLS.2024.3387544.
[40] Yuyang Zhou, Guang Cheng, Shanqing Jiang, Mian Dai, Building an efficient intrusion detection system based on feature selection and ensemble classifier, Computer Networks. V. 174, 2020, 107247, ISSN 1389-1286. DOI: https://doi.org/10.1016/j.comnet.2020.107247.
[41] Han, M., Li, C., Meng, F. et al. An online ensemble classification algorithm for multi-class imbalanced data stream. Knowl Inf Syst 66, 6845–6880 (2024). URL: https://ezpro.fa.ru:2117/10.1007/s10115-024-02184-6 (accessed: 10.11.2024).
[42] Liu, Y., Zhu, L., Ding, L. et al. Selective ensemble method for anomaly detection based on parallel learning. Sci Rep 14, 1420 (2024). DOI: https://doi.org/10.1038/s41598-024-51849-3.
[43] Alsaffar, A.M., Nouri-Baygi, M. & Zolbanin, H.M. Shielding networks: enhancing intrusion detection with hybrid feature selection and stack ensemble learning. J Big Data 11, 133 (2024). URL: https://ezpro.fa.ru:2117/10.1186/s40537-024-00994-7 (accessed: 10.11.2024).
[44] Vinayakumar Ravi, Rajasekhar Chaganti, Mamoun Alazab, Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system, Computers and Electrical Engineering. V. 102, 2022, 108156, ISSN 0045-7906. DOI: https://doi.org/10.1016/j.compeleceng.2022.108156.
[45] Xin, R., Liu, H., Chen, P. et al. Robust and accurate performance anomaly detection and prediction for cloud applications: a novel ensemble learning-based framework. J Cloud Comp 12, 7 (2023). DOI: https://doi.org/10.1186/s13677-022-00383-6.
[46] Amru, M., Jagadeesh Kannan, R., Narasimhan Ganesh, E., Muthumarilakshmi, S., Padmanaban, K., Jeyapriya, J., & Murugan, S. (2024). Network intrusion detection system by applying ensemble model for smart home. International Journal of Electrical and Computer Engineering (IJECE), 14(3), 3485-3494. DOI: http://doi.org/10.11591/ijece.v14i3.pp3485-3494.
[47] Saheed, Y.K., Misra, S. A voting gray wolf optimizer-based ensemble learning models for intrusion detection in the Internet of Things. Int. J. Inf. Secur. 23, 1557–1581 (2024). URL: https://ezpro.fa.ru:2117/10.1007/s10207-023-00803-x (accessed: 10.11.2024).
[48] Thockchom, N., Singh, M.M. & Nandi, U. A novel ensemble learning-based model for network intrusion detection. Complex Intell. Syst. 9, 5693–5714 (2023). DOI: https://doi.org/10.1007/s40747-023-01013-7.

[49] Shtayat M.M., Hasan M.K., Sulaiman R., Islam S. and Khan A.U.R. An Explainable Ensemble Deep Learning Approach for Intrusion Detection in Industrial Internet of Things. IEEE Access. 2023, v. 11, p. 115047–115061. DOI: 10.1109/ACCESS.2023.3323573.

[50] Ali, M., Haque, Mu., Durad, M.H. et al. Effective network intrusion detection using stacking-based ensemble approach. Int. J. Inf. Secur. 22, 1781–1798 (2023). DOI: https://doi.org/10.1007/s10207-023-00718-7.

[51] Thakkar A. and Lohiya R. Attack Classification of Imbalanced Intrusion Data for IoT Network Using Ensemble-Learning-Based Deep Neural Network. IEEE Internet of Things Journal. V. 10, no. 13, p. 11888–11895, 1 July1, 2023. DOI: 10.1109/JIOT.2023.3244810.

[52] Abdulganiyu, O.H., Ait Tchakoucht, T. & Saheed, Y.K. A systematic literature review for network intrusion detection system (IDS). Int. J. Inf. Secur. 22, 1125–1162 (2023). DOI: https://doi.org/10.1007/s10207-023-00682-2.

[53] Zahra Zamanzadeh Darban, Geoffrey I. Webb, Shirui Pan, Charu Aggarwal, and Mahsa Salehi. 2024. Deep Learning for Time Series Anomaly Detection: A Survey. ACM Comput. Surv. 57, 1, Article 15 (January 2025), 42 p. DOI: https://doi.org/10.1145/3691338.

[54] Balyberdin, A. V. Specifics public datasets of network traffic for anomaly detection. Telekommunikacii i informacionnye tekhnologii. 2024, v. 11, no. 1, p. 24–30. – EDN: NRDQHO (in Russian).

[55] Gopali S., Abri F., Siami Namin A. and Jones K.S. The Applicability of LLMs in Generating Textual Samples for Analysis of Imbalanced Dataset. IEEE Access, v. 12, p. 136451–136465, 2024. DOI: 10.1109/ACCESS.2024.3463400.

[56] Goryunov M.N., Matskevich A.G., Rybolovlev D.A. Synthesis of a Machine Learning Model for Detecting Computer Attacks Based on the CICIDS2017 Dataset. Proceedings of the Institute for System Programming of the RAS (Proceedings of ISP RAS). 2020;32(5):81-94. DOI: https://doi.org/10.15514/ISPRAS-2020-32(5)-6 (in Russian).

[57] 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). DOI: https://doi.org/10.1007/s13369-024-08949-z.

Статья поступила в редакцию 20.11.2024; одобрена после рецензирования 10.01.2025;
принята к публикации 22.01.2025
The article was submitted 20.11.2024; approved after reviewing 10.01.2025;
accepted fo publication 22.01.2025