Методы обнаружения аномалий в компьютерных сетях

Клочкова Екатерина Николаевна
заместитель начальника кафедры информационной безопасности учебно-научного комплекса информационных технологий, Московский университет МВД России имени В.Я. Кикотя, e_maks2000@mail.ru

Пименова Оксана Владимировна
канд. техн. наук, доцент кафедры информационной безопасности учебно-научного комплекса информационных технологий, Московский университет МВД России имени В.Я. Кикотя, okcana.pimenova@yandex.ru

В статье рассмотрены основные методы обнаружения аномалий в компьютерных сетях, дан их сравнительный анализ, приведены условия их применения, предложен комплексный подход к разработке интегрированной модели выявления аномалий в сети, объединяющий возможности алгоритмов машинного обучения и преимущества архитектуры глубоких нейронных сетей.
Ключевые слова: методы обнаружения аномалий, сетевые аномалии, обнаружение аномалий в сетевом трафике, машинное обучение

Компьютерные сети прочно вошли в жизнь современного общества. Трудно представить себе организацию, которая бы не использовала в своей работе сетевые технологии; человека, который бы не пользовался возможностями, которые предоставляет ему Интернет. При этом одновременно со значительным увеличением объемов сетевого трафика, возрастает количество и разнообразие угроз, которым подвергаются передаваемые данные. Традиционные средства безопасности такие, как межсетевые экраны, системы обнаружения вторжений все чаще не справляются со стоящей перед ними задачей по обеспечению сетевой безопасности, не имея возможности адаптироваться под новые возникающие виды угроз. Для предотвращения сетевых вторжений необходимо внедрять меры безопасности, предназначенные для обнаружения аномалий и способные идентифицировать потенциальные угрозы.

Обнаружение аномалий является универсальной техникой, которая может применяться как для обнаружения сетевых вторжений, так и для идентификации необычной, подозрительной активности. Под аномалиями в сети принято понимать такие события в пределах сети, которые отклоняются от нормального или известного поведения и считаются имеющими значение для безопасности. В большинстве случаев это нетипичные действия, направленные на нарушение работоспособности сети.

Стратегия на основе обнаружения аномалий предполагает, что необходимо сначала оценить модель «нормальной сетевой активности», а затем уже проводить анализ будущей активности в сети, сравнивая ее с эталонной. Такой подход даст возможность различить обычную и потенциально вредоносную сетевую активность.

Рассмотрим существующие методы обнаружения аномалий в сети. Их принято классифицировать на:

1. Методы обнаружение аномалий на основе анализа временных рядов.
2. Методы обнаружение аномалий на основе анализа журналов.
3. Автоматизированное управление сетью и обнаружение неисправностей.
4. Методы обнаружения аномалий на основе машинного обучения.

Методы обнаружение аномалий на основе анализа временных рядов

Методы обнаружение аномалий на основе анализа временных рядов занимают важное место в области обнаружения сетевых атак. Для выявления аномального поведения в этом случае используют временную природу данных.

Одним из распространенных подходов стало использование методов авторегрессии с интегрированным скользящим средним (ARIMA, AutoRegressive Integrated Moving Average) и сезонного разложения для анализа трендов.

ARIMA представляет собой статистический метод моделирования временных рядов, объединяющий три компоненты: авторегрессию, дифференцирование и скользящее среднее. Для эффективной работы алгоритма необходимо, чтобы данные имели хронологический порядок. Подход позволяет выявлять скрытые паттерны и зависимости в данных для формирования прогнозов будущих значений.

К методам сезонного разложения относятся метод центрированных скользящих средних, TRAMO-SEAT, STL (Seasonal-Trend decomposition using LOESS) и т.д. Основ-

ной принцип методов анализа временных рядов заключается в разложении данных на несколько компонентов (тренд, сезонность, нерегулярные колебания), и выявлении на их основе долгосрочных тенденций и закономерностей, исключив регулярные сезонные колебания.

Применительно к сетевой безопасности методы на основе анализа временных рядов используются для выявления снижения производительности сетей, сбоев и аномальных событий.

Еще одной группой методов, которые применяются для обнаружения аномалий в сети, стали методы, основанные на анализе журналов.

Анализ журналов является важной составляющей для обеспечения информационной безопасности и выявления аномалий в сети. Каждый из журналов содержит логи, которые позволяют выявить различные виды отклонений в поведении.

В таблице 1 приведен перечень информации, которая может быть получена из журналов.

Таблица 1

Классификация информации по источникам ее получения

№ п/п	Наименование журнала	Получаемая информация
1	Системные журналы операционной системы Windows	попытки входа/выхода в систему, изменение учетных записей, изменение прав доступа и политик безопасности, информация о доступе к защищенным объектам, об использовании особых привилегий, ошибки системы и приложений, запуск/остановка служб, информация о сбоях драйверов и аппаратных ошибках, о событиях, связанных с ядром ОС.
2	Системные журналы операционной системы Linux	информация об аутентификации пользователей (пользователь, источник подключения, временные метки события, успешные и неудачные попытки входа в систему, используемый механизм аутентификации); о доступе к объектам файловой системы, о выполнении системных вызовов, о изменении прав доступа и политик безопасности; системные сообщения от ядра, от различных компонентов ОС.
3	Системные журналы операционной системы MacOS	информация о действиях брандмауэра (о блокировке соединений, о разрешенных подключениях, о попытках нарушения правил безопасности); о сетевых подключениях, открытых портах, изменениях сетевых настроек; о попытках входа в систему, используемых методах аутентификации; о произведенных изменениях в системе (факты перезагрузки, выключения, обновления прошивок); о действиях приложений (запуск, сбои, подозрительное поведение); данные о сетевых ошибках и сбоях.
4	Журналы сетевых устройств	- для межсетевых экранов: информация о попытках несанкционированного доступа (неудачные попытки аутентификации); о попытках сканирования портов, о разрешенном/заблокированном трафике, о попытках DoS/DDoS-атак, об использовании уязвимых портов, об аномалиях в трафике; - для маршрутизаторов и коммутаторов: информация о событиях, связанных с изменением конфигурации; о сбоях линков; об аномалиях трафика; - для прокси-серверов: информация о запросах, сделанных через прокси-сервер (IP-адрес, запрошенный URL, код статуса HTTP и т.д.), об объемах переданных данных, о подозрительных запросах.
5	Журналы приложений и сервисов	информация об успешных и неудачных попытках входа в систему, включая количество попыток; об изменениях в учетных записях; о попытках доступа к ресурсам с нарушением прав; о необычных паттернах использования ресурсов; о попытках эксплуатации уязвимостей; о попытках чтения, изменения конфиденциальных данных, об ошибках при обработке данных; об отказе в доступе; об изменениях в настройках безопасности.
6	Журналы системы управления доступом и СКУД	информация о событиях, связанных с физическим и цифровым доступом к сети (учетные данные пользователя, тип используемого идентификатора, временные метки, информация о точках и зонах доступа, результат попыток доступа) об одновременном доступе с разных точек, о множественных неудачных попытках аутентификации, о незакрытых сессиях
7	Специализированные журналы учета инцидентов информационной безопасности	зафиксированная информация об инцидентах безопасности (дата, время обнаружения, категория инцидента, описание инцидента, источник угрозы, причины возникновения и т.д.)
8	Журналы сервисов безопасности	информация о работе антивирусных программ, систем обнаружения и предотвращения вторжений и других средств защиты; о выявленных сетевых атаках, вредоносном коде, нарушениях целостности системы, попытках несанкционированного доступа; о событиях, связанных с запуском, остановкой, изменением режимов работы программных модулей, средств защиты; о командах, выполненных с повышенными правами; о действиях с аккаунтами, ключевой информацией; о нетипичных изменениях конфигурации или нарушениях в работе компонентов, связанных с обеспечением информационной безопасности

Из приведенной таблицы видно, что анализ журналов позволяет отслеживать разнообразные события в сети, анализировать угрозы и реагировать на нарушения, предоставляя важную информацию о состоянии системы. Выявление аномалий с использованием анализа журналов имеет существенные недостатки, которые связаны прежде всего с огромным объемом регистрируемой информации. Обработка таких массивов данных требует не только значительных вычислительных ресурсов, но и высокоскоростных каналов передачи данных, распределенных баз данных, как следствие возникают временные задержки между инцидентом и его анализом, снижая оперативность реагирования. Еще одна проблема возникает из-за большого количества разнообразных журналов и несогласованности данных в них, что приводит к сложности или даже невозможности построения единой схемы обработки данных.

На текущий момент существует несколько подходов к анализу данных в журналах. Первый основан на правилах, которые определяются изначально и предназначены для выявления событий, которые им не соответствуют. Другой подход заключается в использовании современных методов обработки естественного языка (технологии NLP) для распознавания ключевой информации. Ни один из подходов не является идеальным решением. Методы на основе правил требуют разработки правил. Не корректная их формулировка может привести к ложным срабатываниям или отсутствию реакции на инцидент. Применение методов на основе технологии NLP очень сильно зависит от датасета, который используется для обучения.

Автоматизированное управление сетью и обнаружение неисправностей

Автоматизированное управление сетью и обнаружение неисправностей является важной задачей, направленной на обеспечение их надежности и производительности. Одним из наиболее распространенных подходов является управление сетью на основе правил. Здесь необходимо заранее сформулировать набор правил для обнаружения аномального поведения или проблем в сети. Их используют для обнаружения необычных шаблонов в сетевом трафике, неисправных устройств, потенциальных атак на сеть, но в любом случае требуется провести большое количество действий в ручном формате. В последние годы все чаще для решения поставленной задачи используются методы машинного обучения.

Методы обнаружения аномалий на основе машинного обучения

Методы обнаружения аномалий на основе традиционного машинного обучения являются наиболее популярными при обеспечении сетевой безопасности. Здесь выделяются несколько подходов.

Один из них основывается на использовании метода опорных векторов (SVM) при построении модели обнаружения аномалий. Основная идея SVM заключается в том, чтобы преобразовать данные в пространство большей размерности, проводя деление на нормальные и аномальные точки данных и находя наилучшую гиперплоскость для данных.

Данный алгоритм машинного обучения предназначен для решения задач линейной и нелинейной классификации, регрессии и обнаружения аномальных данных. SVM показывает хорошие результаты в задачах с большим количеством признаков, а также при обучении на небольшом количестве данных.

Второй подход, который также нашел широкое распространение, основывается на изоляции аномальных данных. Примером такого статического метода является алгоритм Isolation Forest. В его основе лежит принцип того, что аномалии по своей природе более «изолированы» в наборе данных из-за своей редкости и имеющихся отличий от нормальных данных. Поэтому Isolation Forest пытается изолировать выбросы.

Работа алгоритма заключается в построении деревьев. Каждое дерево создается путем случайного разбиения данных. При построении дерева для каждого узла выбирается произвольный признак с некоторым пороговым значением и случайное значение разбиения. Такие деления данных продолжаются рекурсивно, до тех пор, пока дерево не достигнет своей максимальной заранее определенной глубины, или не произойдет изоляции каждой точки данных в уникальный узел.

Эффективность метода достигается за счет использования в качестве критерия оценки аномалии для каждой точки - показателя средней длины пути, ведущего к изоляции. Аномальные точки данных характеризуются значительно более короткими путями, что облегчает их быстрое обнаружение.

Методы обнаружения аномалий на основе машинного обучения традиционно показывают неплохие результаты при решении большинства задач обеспечения сетевой безопасности. Среди основных недостатков можно выделить следующие:

– при обработке сложных сетевых данных с высокой размерностью возникают проблемы;

– эффективность использования методов машинного обучения зависит от качества выбора признаков, что требует от пользователей специальных знаний о структурах сложных сетевых данных;

– могут оказаться недостаточно гибкими, чтобы справляться с появляющимися новыми киберугрозами и меняющимися шаблонами аномалий.

Проведенный нами анализ существующих методов обнаружения аномалий в сети показывает, что каждый из методов обладает недостатками, которые не позволяют их эффективно использовать для решения задач обеспечения сетевой безопасности.

Для повышения эффективности борьбы с возникающими в компьютерных сетях новыми угрозами может быть предложен комплексный подход, который позволит объединить в новую интегрированную модель возможности таких алгоритмов машинного обучения, как GAN (Generative Adversarial Network) и Isolation Forest, и преимущества архитектуры глубоких нейронных сетей Transformer.

Основная идея заключается в следующем. Необработанные данные, полученные из компьютерной сети, поступают в компонент Isolation Forest, основная задача которого заключается в быстрой проверке сетевого трафика и выделения аномальных точек путем построения случайного бинарного дерева. На этом этапе происходит генерация оценки аномалий для каждой точки данных. Признаками потенциально аномальных точек данных выступают полученные высокие значения оценок.

Совместно с Isolation Forest работает алгоритм GAN. Он основан на взаимодействии двух нейронных сетей: генератора и дискриминатора. Задача, стоящая перед генератором, заключается в создании новых данных путем имитации реальных образцов, т.е. похожих на обычный сетевой трафик. Дискриминатор используется для оценки схожести сгенерированных и реальных данных, выступая в качестве классификатора подлинности образца. Полученные оценки передаются генератору, который корректирует свои параметры для повышения качества данных, их достоверности, способствуя выявлению потенциально аномальных характеристик.

Сгенерированные данные и информация из необработанных журналов поступают на вход модели Transformer, которая уже используется для выявления корреляции между событиями из разных источников путем сопоставления временных характеристик данных.

В итоге результаты первоначального отбора, проведенного с применением Isolation Forest, улучшенные с помощью GAN и прошедшие временное моделирование через Transformer используются для комплексного обнаружения сетевых аномалий и анализа логов: сгенерированные и исходные данные можно сравнивать, а оценки аномалий сопоставлять с пороговыми значениями модели для выявления потенциального аномального поведения. Использование такой модели позволяет более точно фиксировать и идентифицировать проявления аномального поведения в компьютерных сетях.

Проведенный анализ методов выявления сетевых аномалий показал, что они могут выступать лишь в качестве одного из инструментов защиты от киберугроз и не служат универсальным решением. Постоянное изменение сетевого трафика, сложность детектирования ранее не встречавшихся атак приводит к неэффективности использования традиционных методов обнаружения аномалий. Наиболее перспективным направлением становится создание гибридов на основе различных подходов. При этом самым главным требованием, предъявляемым к таким решениям –обеспечение адаптивной и масштабируемой аналитической обработки событий, которые в последующем обеспечат безопасность данных в реальном или близком к реальному масштабе времени.

Литература

1. Большаков А.С., Хусаинов Р.В., Осин А.В. Обнаружение аномалий трафика с использованием нейронной сети для обеспечения защиты информации. I-methods. 2021, т. 13, №4. [Электронный источник] URL: https://707.su/0V4L [Дата обращения 21.04.2026].

2. МакФарланд Алекс, Инструменты кибербезопасности на основе искусственного интеллекта. [Электронный источник]. URL: https://www.unite.ai/ru/инструменты-кибербезопасности-ИИ [Дата обращения 09.04.2026].

3. Alwhbi I. A., Zou C. C., Alharbi R. N. Анализ и классификация зашифрованного сетевого трафика с использованием машинного обучения [Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning] // Sensors (Basel). 2024. Vol. 24, No. 11. Art. 3509. 17 p. DOI: 10.3390/s24113509. [Электронный источник] URL: https://www.mdpi.com/1424-8220/24/11/3509 [Дата обращения 15.04.2026].

4. Labonne M. Обнаружение сетевых аномалий с использованием методов машинного обучения. [Anomaly-

based network intrusion detection using machine learning]. Cryptography and Security [cs.CR]. Institut Polytechnique de Paris, 2020. English. [Электронный источник] URL:https://theses.hal.science/tel-02988296/document [Дата обращения 20.04.2026].

5. Vadgaonkar Priti H. Обнаружение сетевых аномалий и анализ поведения пользователей с использованием методов машинного обучения. [Network Anomaly Detection and User Behavior Analysis using Machine Learning]. International Journal of Computer Applications (0975 – 8887) Volume 175– No. 13, August 2020. [Электронный источник] URL:https://707.su/CTSQ [Дата обращения 20.04.2026].

6. Wang S., Jiang R., Wang Z., Zhou Y. Обнаружение аномалий и анализ логов в компьютерных сетях на основе глубокого обучения [Deep Learning-based Anomaly Detection and Log Analysis for Computer Networks]// Journal of Information and Computing (JIC), 2024, 2(2), 34-63. [Электронный источник] URL:https://arxiv.org/pdf/2407.05639 [Дата обращения 28.03.2026].

Anomaly Detection Methods in Computer Networks

Klochkova E.N., Pimenova O.V.

V.Ya. Kikot Moscow University of the Ministry of Internal Affairs of Russia

This article examines the main methods of anomaly detection in computer networks, provides a comparative analysis, describes the conditions for their application, and proposes a comprehensive approach to developing an integrated network anomaly detection model that combines the capabilities of machine learning algorithms and the advantages of deep neural network architecture.

Keywords: anomaly detection methods, network anomalies, network traffic anomaly detection, machine learning

References

1. Bolshakov A.S., Khusainov R.V., Osin A.V. Traffic Anomaly Detection Using a Neural Network to Ensure Information Security. I-methods. 2021, Vol. 13, No. 4. [Electronic source] URL: https://707.su/0V4L [Accessed 21.04.2026].
2. McFarland Alex, Cybersecurity Tools Based on Artificial Intelligence. [Electronic source]. URL: https://www.unite.ai/ru/инструменты-киберзащитности-ИИ [Accessed 09.04.2026].
3. Alwhbi I. A., Zou C. C., Alharbi R. N. Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning // Sensors (Basel). 2024. Vol. 24, No. 11. Art. 3509. 17 p. DOI: 10.3390/s24113509. [Electronic source] URL: https://www.mdpi.com/1424-8220/24/11/3509 [Accessed 15.04.2026].
4. Labonne M. Anomaly-based network intrusion detection using machine learning. Cryptography and Security [cs.CR]. Institut Polytechnique de Paris, 2020. English. [Electronic source] URL: https://theses.hal.science/tel-02988296/document [Accessed 20.04.2026].
5. Vadgaonkar Priti H. Network Anomaly Detection and User Behavior Analysis using Machine Learning. International Journal of Computer Applications (0975–8887) Volume 175– No. 13, August 2020. [Electronic source] URL: https://707.su/CTSQ [Accessed 20.04.2026].
6. Wang S., Jiang R., Wang Z., Zhou Y. Deep Learning-based Anomaly Detection and Log Analysis for Computer Networks // Journal of Information and Computing (JIC), 2024, 2(2), 34–63. [Electronic source] URL: https://arxiv.org/pdf/2407.05639 [Accessed 03/28/2026].