



Дата поступления рукописи в редакцию: 27.09.2025 г.
Дата принятия рукописи в печать: 10.10.2025 г.

DOI: 10.24412/2076-1503-2025-9-586-589

ЛИСАЧЕНКО Олег Васильевич,
кандидат исторических наук,
доцент кафедры «Гуманитарные науки» институт
химических технологий и инжиниринга ФГБОУ ВО
«Уфимский государственный нефтяной университет»
в г.Стерлитамаке,
e-mail: mail@law-books.ru

ИСПОЛЬЗОВАНИЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СИСТЕМАХ КИБЕРБЕЗОПАСНОСТИ

Аннотация. Информационная безопасность становится одной из ключевых задач современной цифровой инфраструктуры. Традиционные методы защиты не всегда способны своевременно обнаруживать новые, неизвестные ранее угрозы. В связи с этим всё большее распространение получают технологии машинного обучения, которые позволяют выявлять аномальное поведение в системах на основе анализа больших объёмов данных. В статье рассматриваются теоретические и практические аспекты использования машинного обучения для обнаружения аномалий в киберпространстве, обсуждаются преимущества, ограничения и перспективы развития таких подходов.

Ключевые слова: машинное обучение, кибербезопасность, обнаружение аномалий, сетевой трафик, синтетические данные, информационная безопасность, модели без учителя.

LISACHENKO Oleg Vasilievich,
Candidate of Historical Sciences,
Associate Professor of the Department of Humanities,
Institute of Chemical Technologies and Engineering,
Federal State Budgetary Educational Institution of Higher Education
Ufa State Petroleum University in Sterlitamak

USING MACHINE LEARNING ALGORITHMS TO DETECT ANOMALIES IN CYBERSECURITY SYSTEMS

Annotation. Information security is becoming one of the key tasks of modern digital infrastructure. Traditional security methods are not always able to detect new, previously unknown threats in a timely manner. In this regard, machine learning technologies are becoming more widespread, which make it possible to identify abnormal behavior in systems based on the analysis of large amounts of data. The article examines the theoretical and practical aspects of using machine learning to detect anomalies in cyberspace, discusses the advantages, limitations and prospects for the development of such approaches.

Key words: machine learning, cybersecurity, anomaly detection, network traffic, synthetic data, information security, unsupervised models.

Введение

Обеспечение информационной безопасности в условиях стремительного роста объёмов цифровых данных и расширения границ сетевого взаимодействия требует новых решений, способных обнаруживать угрозы в реальном времени и с высокой степенью точности. Одним из таких

решений становится применение алгоритмов машинного обучения (МО), позволяющих не просто фиксировать заранее известные типы атак, но и выявлять ранее неизвестные, отклоняющиеся от нормального поведения системы инциденты.

Аномалии, как правило, отражают нетипичную или подозрительную активность, например,

неожиданное обращение к конфиденциальной информации, резкое увеличение исходящего трафика или выполнение системных команд, ранее не характерных для пользователя. Алгоритмы МО способны выявлять такие действия без необходимости ручной настройки или предварительного задания сигнатур, что делает их особенно актуальными в современных гибридных и облачных инфраструктурах.

Теоретические основы машинного обучения в кибербезопасности

Машинное обучение — это совокупность методов, позволяющих алгоритмам автоматически обучаться на исторических данных с целью распознавания закономерностей и предсказания будущих событий. В контексте кибербезопасности основная задача таких алгоритмов заключается в построении моделей нормального поведения системы или пользователей и выявлении отклонений от этой модели.

Выделяют два ключевых подхода: обучение с учителем и обучение без учителя. В первом случае используется заранее размеченная выборка, в которой известны примеры как нормальной, так и вредоносной активности. Во втором случае алгоритм самостоятельно формирует представление о норме и фиксирует выход за её пределы. Методы без учителя наиболее эффективны при обнаружении новых, нестандартных угроз, о которых заранее нет сведений [1].

Современные методы машинного обучения, такие как случайный лес, градиентный бустинг, автоэнкодеры, а также различные архитектуры нейронных сетей (включая рекуррентные и сверточные), находят широкое применение в задачах анализа логов, мониторинга сетевого трафика и оценки поведения приложений. Особый интерес представляет использование ансамблевых методов и гибридных подходов, сочетающих обучение с и без учителя, что позволяет существенно снизить уровень ложных срабатываний [2].

Практическое применение и эффективность

На практике алгоритмы машинного обучения используются для анализа сетевых потоков, событий безопасности, поведения пользователей и приложений. Одним из важных направлений является обнаружение аномалий в сетевом трафике. В таких задачах модели обучаются на нормальных шаблонах взаимодействия между пользователями и сетевыми ресурсами, и при появлении отклонений (например, попытки доступа к нетипичным портам, необычные протоколы, нетипичное географическое расположение клиента) фиксируют потенциальную угрозу.

В ряде работ было продемонстрировано, что применение МО позволяет существенно повысить точность систем обнаружения атак, особенно при использовании синтетических данных для обучения моделей. Такой подход даёт возможность избежать ограничений, связанных с конфиденциальностью реальных логов, и при этом обеспечить репрезентативность тренировочной выборки [2].

Для повышения точности выявления аномалий часто используются методы ансамблевого обучения, объединяющие результаты нескольких моделей. Также важную роль играет качество предобработки данных: очистка, нормализация и агрегация существенно влияют на результат работы алгоритмов [3]. В условиях высоких нагрузок в корпоративных и облачных системах особую актуальность приобретают подходы, позволяющие масштабировать модели и проводить их адаптацию в режиме реального времени.

Проблемы и ограничения

Несмотря на высокую эффективность, применение машинного обучения в системах кибербезопасности сопряжено с рядом сложностей. Одной из них является проблема «чёрного ящика» — невозможность интерпретировать поведение модели, особенно в случае использования глубоких нейросетей. Это затрудняет принятие решений на стороне оператора и снижает доверие к таким системам.

Кроме того, сами алгоритмы могут становиться объектом атак. Например, при использовании техники отравления данных (data poisoning) злоумышленник может преднамеренно встраивать ложные данные в обучающую выборку, тем самым нарушая корректность работы модели. Также возможны атаки типа evasion — изменение поведения вредоносного объекта таким образом, чтобы он остался незамеченным для модели [4].

Важным ограничением остаётся зависимость от полноты и актуальности обучающего набора. Изменения в поведении пользователей, обновления программного обеспечения, появление новых протоколов требуют регулярной переобучаемости модели. В этой связи возрастает интерес к методам онлайн-обучения и федеративного обучения, позволяющим учитывать текущие данные без необходимости централизованного сбора всей информации.

Перспективы развития

Наиболее перспективным направлением развития являются адаптивные системы обнаружения угроз, способные встраиваться в архитектуру организации и непрерывно обучаться. Особую значимость приобретает применение синте-

тических данных — генерация реалистичных логов для обучения моделей в условиях, когда реальный доступ к данным ограничен или невозможен по соображениям безопасности [2].

Кроме того, стоит отметить рост интереса к разработке интерпретируемых моделей. Такие решения позволяют не только фиксировать факт аномалии, но и объяснять причину срабатывания, что существенно упрощает работу специалистов по безопасности. В долгосрочной перспективе можно ожидать широкого распространения систем, сочетающих экспертные правила и методы машинного обучения, а также интеграции с решениями на базе искусственного интеллекта более высокого уровня.

Интеграция машинного обучения с системами реагирования на инциденты

Эффективность применения алгоритмов машинного обучения в сфере кибербезопасности во многом зависит от того, насколько быстро и точно система может не только обнаружить аномалию, но и организовать автоматизированное или полуавтоматическое реагирование на потенциальную угрозу. Современные подходы к построению комплексных решений безопасности предполагают тесную интеграцию моделей машинного обучения с системами управления событиями безопасности и информацией (SIEM), платформами реагирования на инциденты (SOAR) и системами автоматизации безопасности.

Одним из ключевых преимуществ такой интеграции является возможность минимизации времени реакции на инцидент. Например, при обнаружении подозрительной активности модель может не просто зафиксировать событие, но и передать его в систему SOAR для автоматического запуска сценария расследования: блокировки IP-адреса, изоляции устройства в сети, анализа связанных событий и оповещения специалистов службы безопасности.

Кроме того, интеграция позволяет реализовать замкнутый цикл «обнаружение — анализ — реагирование — обучение», в котором данные о реагировании используются для дообучения модели. Это способствует повышению её точности и адаптивности к новым типам атак. Например, если система успешно заблокировала DDoS-атаку, информация об этом случае может быть добавлена в обучающую выборку, что улучшит распознавание аналогичных атак в будущем.

Важно отметить, что эффективная интеграция требует стандартизации форматов данных и протоколов взаимодействия между компонентами системы безопасности. Для этих целей всё чаще применяются открытые стандарты, такие как STIX/TAXII для обмена угрозами, OpenC2 для команд и управления, а также MISP для обмена метаданными о киберугрозах.

Таким образом, внедрение машинного обучения в состав комплексных решений кибербезопасности открывает возможности для создания более интеллектуальных, быстрых и масштабируемых систем защиты, способных противостоять современным киберугрозам.

Применение машинного обучения в защите облачных инфраструктур

С переходом организаций на облачные технологии значительно усложняется архитектура информационных систем и расширяются поверхности атак. Облачные среды характеризуются высокой динамичностью, гибкой масштабируемостью и децентрализованным управлением, что делает традиционные методы обеспечения безопасности недостаточно эффективными. В этой связи всё большее значение приобретают решения, основанные на алгоритмах машинного обучения, способные адаптироваться к изменяющимся условиям и оперативно выявлять подозрительную активность.

Особую сложность представляет защита микросервисных архитектур, контейнеризованных приложений и serverless-решений, где классические средства мониторинга не всегда применимы. Модели машинного обучения позволяют анализировать поведение сервисов, отслеживать сетевые взаимодействия между контейнерами и обнаруживать аномалии, которые могут указывать на компрометацию системы. Например, неожиданное обращение одного микросервиса к базе данных другого, или внезапное увеличение числа API-запросов может быть признаком внутренней атаки или утечки учетных данных.

Важным направлением является использование методов машинного обучения для анализа логов и метрик, собираемых из различных облачных платформ (например, AWS CloudTrail, Azure Monitor, Google Cloud Logging). Системы обнаружения аномалий на основе МО способны выделять шаблоны поведения пользователей, сервисных аккаунтов и приложений, и сигнализировать о любых существенных отклонениях.

Кроме того, в облачных средах становится особенно важной концепция Zero Trust Architecture (архитектура с нулевым доверием), в которой каждый запрос проверяется независимо. Интеграция моделей машинного обучения в такие архитектуры позволяет реализовать динамическую политику доступа, основанную на контексте запроса: местоположении, времени, типе устройства, поведении пользователя и других факторах.

Таким образом, применение алгоритмов машинного обучения в защите облачных инфраструктур открывает новые возможности для обеспечения безопасности в условиях высокой динамики и сложности современных ИТ-систем.

Обучение на потоковых данных и его роль в обнаружении аномалий

Современные системы кибербезопасности сталкиваются с необходимостью обработки огромных объёмов данных в режиме реального времени. Традиционные подходы, основанные на статических наборах данных и периодическом переобучении моделей, зачастую не успевают адаптироваться к быстро меняющейся среде. В этой связи всё большее внимание уделяется методам обучения на потоковых данных (stream learning), позволяющим обновлять модель по мере поступления новых примеров без необходимости полного переобучения.

Потоковые алгоритмы машинного обучения отличаются высокой скоростью обработки и низким потреблением ресурсов, что делает их особенно актуальными для таких задач, как анализ сетевого трафика, мониторинг активности пользователей или выявление необычного поведения в реальном времени. Примером могут служить фреймворки, такие как River (для Python), специально разработанные для онлайн-обучения.

Ключевыми преимуществами использования stream learning в кибербезопасности являются:

- Непрерывная адаптация модели к изменению паттернов поведения пользователей и систем;
- Снижение задержек при обнаружении новых типов атак;
- Возможность работы с ограниченными вычислительными ресурсами, что особенно важно в edge-вычислениях и IoT-устройствах;
- Обеспечение актуальности модели в условиях концептуальных сдвигов (concept drift), когда закономерности в данных со временем меняются.

Однако внедрение потокового обучения связано и с рядом вызовов: необходимость устойчивости к шуму, защита от вредоносного влияния на модель, сложность оценки качества в условиях отсутствия немедленной обратной связи (delayed labels) и другие.

Заключение

Применение алгоритмов машинного обучения в кибербезопасности открывает широкие возможности для повышения эффективности защиты информационных систем. Особенно перспектив-

ными являются подходы, ориентированные на обнаружение аномалий, поскольку они позволяют выявлять новые типы угроз, минуя ограничения сигнатурных методов. Вместе с тем важным остаётся комплексный подход, включающий обеспечение качества данных, адаптивность моделей, устойчивость к атакам и развитие интерпретируемости. Всё это делает машинное обучение не просто инструментом, а важным компонентом современной системы защиты цифровых активов.

Список литературы:

- [1] Лапина М. А., Мовзалевская В. В., Токмакова М. Е., Бабенко М. Г., Саджид М. (2024). Применение технологий машинного обучения для обнаружения веб-атак. Вестник ВОКИБ, 2024(4), 92–103.
- [2] Гурьянов А. И. (2024). Синтетические данные в задаче обнаружения аномалий в сфере информационной безопасности. Труды конференции «Абрау-2024», 6.
- [3] Никуличев В. А. (2020). Обнаружение аномалий в работе docker-контейнера с использованием методов машинного обучения. ВКР магистра, СПбПУ.
- [4] Михайлов А. Н. (2023). Обнаружение аномалий в сетевом трафике с использованием методов машинного обучения. Наука и образование.
- [5] Ким Г., Ли С., Ким С. (2021). Применение методов машинного обучения для выявления аномалий в сетевом трафике. Киберленинка.

References:

- [1] Lapina M.A., Movzalevskaya V.V., Tokmakova M.E., Babenko M.G., Sajid M. (2024). Application of machine learning technologies to detect web attacks. VOKIB Bulletin, 2024 (4), 92-103.
- [2] A. Guryanov (2024). Synthetic data in the task of detecting anomalies in the field of information security. Proceedings of the conference "Abrau-2024," 6.
- [3] Nikulichev V. A. (2020). Detecting anomalies in the docker container using machine learning methods. WRC Master, SPbPU.
- [4] Mikhailov A. N. (2023). Detection of anomalies in network traffic using machine learning techniques. Science and education.
- [5] Kim G, Lee S, Kim S (2021). Application of machine learning methods to identify anomalies in network traffic. Cyberleninka.

