44. АНАЛИЗ ЭФФЕКТИВНОСТИ МОДЕЛЕЙ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ И КЛАССИФИКАЦИИ КИБЕРАТАК

Бушенко В. А., студент гр. 272301

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Полоско Е. И. – ст. преп., каф. ЭИ

В работе рассматривается роль машинного обучения и аналитики данных в повышении эффективности кибербезопасности. Подчеркивается, что с ростом количества киберугроз и усложнением методов атак возрастает потребность в интеллектуальных инструментах для автоматического обнаружения аномалий, классификации угроз и предсказания потенциальных рисков. Машинное обучение позволяет системам выявлять скрытые закономерности в больших объемах информации, автоматически распознавать вредоносное поведение и адаптироваться к новым угрозам, что делает его важным элементом современных стратегий защиты информации.

Современный мир всё чаще сталкивается с угрозами в сфере кибербезопасности. С постоянным развитием технологий и увеличением числа подключённых устройств информация становится всё более уязвимой перед действиями хакеров и злоумышленников. В этих условиях особенно актуальным становится внедрение инновационных подходов к защите данных, способных оперативно реагировать на растущие и усложняющиеся угрозы. Учитывая масштаб цифровизации практически всех сфер жизни – от финансов и медицины до образования и государственного управления – обеспечение информационной безопасности становится критически важным элементом глобальной технологической инфраструктуры.

Одним из ключевых инструментов в современной кибербезопасности является машинное обучение. Эта технология позволяет системам самостоятельно извлекать знания из поступающих данных и принимать решения без явного программирования. Благодаря способности анализировать большие объёмы информации и выявлять скрытые взаимосвязи, алгоритмы машинного обучения становятся эффективным средством выявления аномалий, вредоносного поведения и потенциальных угроз. Они находят применение как в защите конечных пользователей, так и в обеспечении безопасности корпоративных сетей, государственных баз данных и облачных инфраструктур [1].

Не менее значимым направлением является аналитика данных, обеспечивающая возможность углублённого анализа информации из различных источников. В контексте информационной безопасности этот подход позволяет обнаруживать новые уязвимости, предсказывать будущие атаки и формировать эффективные меры противодействия. Взаимодействие машинного обучения и аналитики данных формирует основу адаптивных систем защиты, способных выявлять сложные сценарии атак и быстро реагировать на нетипичное поведение. Особенно важно то, что такие системы могут учитывать поведенческие особенности пользователей, настраивать защиту под контекст, а также эффективно работать в условиях ограниченной информации.

Машинное обучение как подраздел искусственного интеллекта активно используется для автоматизации процессов обработки информации. С помощью интеллектуальных алгоритмов можно обнаруживать закономерности и тренды, которые остаются незаметными при традиционном анализе. Это особенно важно при работе с большими объёмами данных, характерными для современных информационных систем. Применение этих алгоритмов в рамках задач кластеризации, классификации и регрессии позволяет повысить точность детектирования угроз и снизить количество ложных срабатываний [2].

На практике подобные технологии применяются, например, для анализа клиентского поведения с целью выявления мошенничества. Системы могут обнаруживать нетипичные действия, отклоняющиеся от привычных моделей, и оперативно сигнализировать о возможных нарушениях. В финансовом секторе это существенно снижает риски и повышает уровень доверия со стороны пользователей. Кроме того, подобные технологии могут применяться в e-commerce для защиты от фрод-транзакций, в страховании – для выявления недобросовестных заявок, и даже в здравоохранении – для отслеживания аномалий в доступе к медицинским данным.

Также модели обучаются для анализа поведения в компьютерных сетях. Сравнивая текущие действия пользователей с заранее заданными эталонами «нормального» поведения, такие системы выявляют подозрительную активность: резкое увеличение трафика, доступ к ресурсам в нехарактерное время, нетипичные запросы и т.д. Это позволяет своевременно выявить признаки атак – от заражения вредоносным ПО до несанкционированного доступа или фишинговых атак [3].

Ещё один важный аспект – использование методов классификации. На основе заранее размеченных наборов данных, включающих как вредоносные, так и безопасные элементы, система учится распознавать потенциально опасные объекты. Это могут быть исполняемые файлы, сетевые пакеты, письма или журналы событий. Анализируя структуру, поведенческие характеристики и способы обхода защиты, модель формирует обобщённые признаки угроз, способные идентифицировать новые атаки, даже ранее неизвестные. Такой подход превосходит традиционные сигнатурные методы и позволяет обеспечить устойчивость к широкому спектру атак [4].

Исторические данные о киберинцидентах также служат основой для построения прогностических моделей, позволяющих не только распознавать угрозы, но и предотвращать их возникновение. Это снижает нагрузку на специалистов, уменьшает время реакции и повышает общую эффективность систем защиты. Кроме того, машинное обучение позволяет гибко масштабировать защитные меры – от локальных решений до глобальных распределённых систем мониторинга и реагирования.

Дальнейшее развитие кибербезопасности невозможно без внедрения новейших концепций. Одним из перспективных направлений становится интеграция машинного обучения с системами искусственного интеллекта. Такая синергия обеспечивает создание продвинутых адаптивных решений, способных действовать в условиях неопределённости и предугадывать появление новых форм атак. Эти системы способны не только обнаруживать угрозы, но и выбирать оптимальную стратегию реагирования в зависимости от контекста, уровня риска и исторического поведения злоумышленника. В перспективе они смогут самостоятельно оптимизировать алгоритмы обнаружения, управлять сложными инцидентами и учиться в режиме реального времени.

В рамках этого направления важную роль играют самообучающиеся системы. В отличие от классических моделей, где настройка осуществляется вручную, здесь алгоритмы способны самостоятельно адаптироваться к меняющимся условиям. Это достигается с помощью методов непрерывного обучения и обучения с подкреплением, когда модель постепенно накапливает опыт, анализируя каждый новый инцидент. Такие решения становятся особенно актуальными в условиях стремительного роста числа атак и их разнообразия. Самообучающиеся системы способны обновлять свои модели без необходимости постоянного участия специалистов, что существенно снижает стоимость и сложность эксплуатации систем информационной безопасности.

Автоматизация принятия решений в ответ на инциденты является еще одним возможным трендом. Современные интеллектуальные платформы позволяют реализовывать мгновенные меры противодействия без вмешательства человека. При обнаружении аномальной активности система может изолировать устройство, ограничить доступ, запустить сканирование или уведомить ответственного администратора. Всё это осуществляется в рамках концепции SOAR (Security Orchestration, Automation and Response), в которой особое внимание уделяется автоматизации не только технических аспектов, но и координации действий между различными компонентами безопасности [5].

В условиях возрастающей сложности атак и увеличения объёма обрабатываемой информации автоматизация становится не просто удобным инструментом, а необходимостью. Интеллектуальные алгоритмы позволяют учитывать множество факторов – от поведения пользователя и временных меток до состояния сети и предыдущих инцидентов – и принимать более точные и своевременные решения.

Таким образом, развитие технологий аналитики данных и машинного обучения играет ключевую роль в обеспечении информационной безопасности. Интеграция этих подходов с искусственным

интеллектом, создание самообучающихся моделей и автоматизация реагирования формируют новую парадигму защиты информации, соответствующую вызовам цифровой эпохи. Без этого невозможно построение надёжных систем, способных эффективно функционировать в условиях постоянно изменяющихся киберугроз. Внедрение интеллектуальных технологий в кибербезопасность не только повышает точность и скорость обнаружения угроз, но и способствует снижению зависимости от человеческого фактора, что особенно важно при работе с большими объёмами данных и в условиях высокой степени неопределённости. Прогнозные модели, основанные на исторических инцидентах и поведенческом анализе, позволяют организациям принимать предупреждающие меры, обеспечивая более раннее и эффективное реагирование на угрозы для защиты информационных систем. В будущем всё более важной будет комплексная интеграция технологических, правовых и организационных решений, направленных на формирование устойчивой и адаптивной архитектуры информационной безопасности.

Список использованных источников:

1. Инновации в кибербезопасности [Электронный ресурс] – Режим доступа https://lean-center.ru/innovaczii-v-kiberbezopasnosti-s-ispolzovaniem-mashinnogo-obucheniya-i-analitiki-dannyh/ – Дата доступа: 08.04.2025

2. Что такое машинное обучение [Электронный ресурс] – Режим доступа https://practicum.yandex.ru/blog/chto-takoe-mashinnoe-obuchenie/ – Дата доступа: 08.04.2025

3. Обнаружение аномалий в машинном обучении [Электронный ресурс] – Режим доступа https://ru.macgence.com/blog/anomaly-detection-in-machine-learning/ – Дата доступа: 09.04.2025

4. Классификация данных [Электронный ресурс] – Режим доступа https://trainingdata.ru/metodic/tpost/c3rvrtk4u1-klassifikatsiya-dannih – Дата доступа: 10.04.2025

5. Роль ИИ и машинного обучения в кибербезопасности в 2025 году [Электронный ресурс] – Режим доступа https://lazarusalliance.com/ru/the-role-of-ai-and-machine-learning-in-cybersecurity-in-2025/ – Дата доступа: 11.04.2025