www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2024.2.5

УДК 004.85:004.056
ББК 32.972.53

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ В ПРОГНОЗИРОВАНИИ И ПРЕДОТВРАЩЕНИИ КИБЕРАТАК

Александр Валерьевич Лощилин

Магистрант, кафедра информационной безопасности,
Волгоградский государственный университет
a_loshilina@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Владислав Георгиевич Яриков

Кандидат педагогических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
yarikov.vladislav@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Арина Валерьевна Никишова

Кандидат технических наук, доцент кафедры информационной безопасности,
Волгоградский государственный университет
nikishova.arina@volsu.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Аннотация. Эта статья рассматривает роль машинного обучения (ML) в прогнозировании и предотвращении кибератак, подробно описывая использование методов обучения с учителем, без учителя и с подкреплением. Обсуждаются преимущества и вызовы интеграции ML в кибербезопасность, включая точность, проблемы конфиденциальности и технические препятствия. Также предлагаются решения для преодоления этих вызовов, такие как постоянное усовершенствование моделей и разработка этических рекомендаций, подчеркивая потенциал ML для усиления стратегий киберзащиты.

Ключевые слова: машинное обучение, кибербезопасность, прогнозирование кибератак, предотвращение кибератак, вызовы машинного обучения, конфиденциальность данных.

В эпоху цифровизации, когда бизнес, государственные учреждения и личная жизнь все больше зависят от Интернета и цифровых технологий, вопросы кибербезопасности становятся особенно актуальными. Кибератаки могут привести к утечке конфиденциальной информации, финансовым потерям и даже к нарушению работы критически важной инфраструктуры. В этом контексте защита информационных систем и данных становится приоритетной задачей.

Машинное обучение, как одно из самых перспективных направлений в области искусственного интеллекта, предлагает новые возможности для обеспечения кибербезопасности. Использование алгоритмов машинного обучения позволяет не только обнаруживать и анализировать киберугрозы в реальном времени, но и прогнозировать потенциальные атаки до их осуществления. Это становится возможным благодаря способности систем машинного обучения анализировать огромные объемы данных, выявлять закономерности и аномалии, которые могут указывать на подготовку или начало кибератаки.

На рисунке представлена мировая статистика кибератак по секторам в 2023 году. На этом графике показано как процентное увеличение кибератак, так и средняя стоимость этих атак в миллионах долларов для различных секторов [6–8].

График кибератак показывает, что секторы образования и финансов наиболее подвержены росту атак, вероятно, из-за большого объема важной информации. Финансовый и энергетический сектора несут высокие затраты от последствий атак, что подчеркивает критическую необходимость их защиты. Различия между секторами требуют индивидуализированных стратегий кибербезопасности.

В таблице 1 представлен обзор различных типов кибератак и связанных с ними последствий.

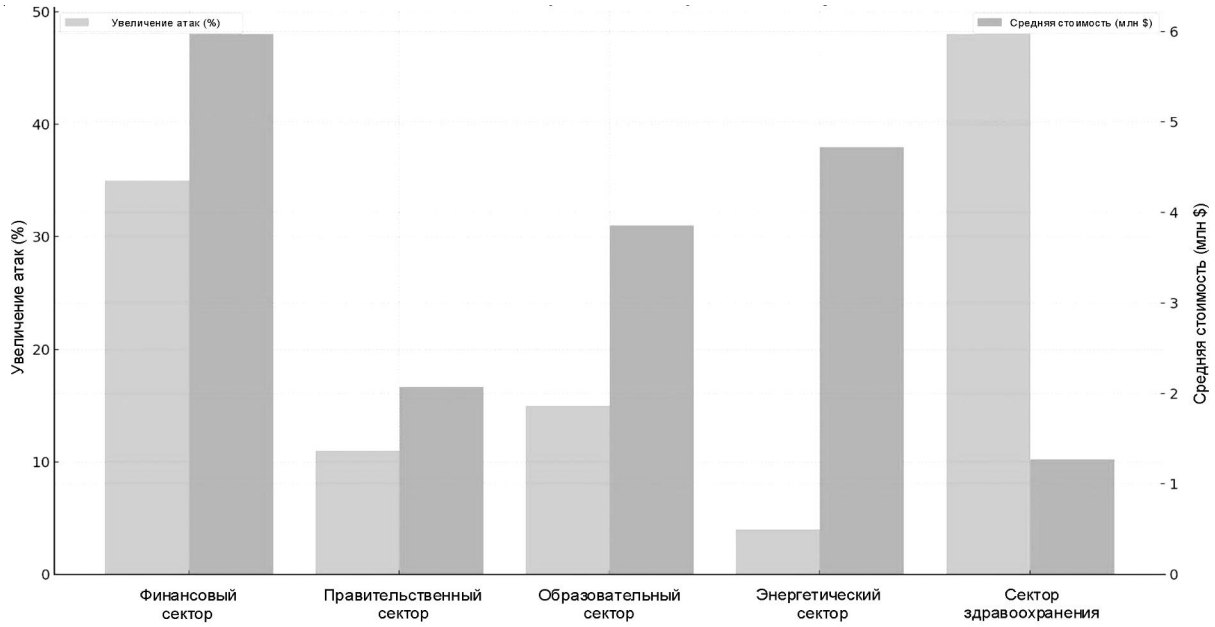
Эта таблица подчеркивает разнообразие киберугроз и потенциальные риски, с которыми сталкиваются индивидуальные пользователи и организации. Понимание типов атак и их последствий является ключевым для разработки эффективных мер безопасности и стратегий защиты [5].

Машинное обучение играет решающую роль в современной кибербезопасности, предлагая новые методы для обнаружения и противодействия киберугрозам. Основные подходы включают:

1. Обучение с учителем. Применяется, когда доступен размеченный набор данных. Это позволяет моделям научиться распознавать угрозы на основе предыдущих примеров, что делает его эффективным в обнаружении известных видов атак.

2. Обучение без учителя. Используется в ситуациях, когда разметка данных отсутствует. Этот подход идеален для выявления неизвестных или новых угроз, так как он анализирует данные в поисках аномалий или отклонений от нормы.

3. Обучение с подкреплением. Вовлекает систему в процесс постоянного само-



Статистика кибератак по секторам за 2023 год

совершенствования через систему вознаграждений и наказаний. Это подходит для адаптации к меняющейся тактике атак и улучшения стратегий обнаружения в реальном времени [1].

Преимущества и ограничения использования машинного обучения в обнаружении угроз рассмотрены в таблице 2.

Машинное обучение предлагает значительные возможности для улучшения кибербезопасности, хотя и требует тщательного применения и постоянной адаптации к меняющемуся ландшафту угроз [2].

Таблица 3 демонстрирует, как различные методы машинного обучения могут быть применены для прогнозирования и предотвращения кибератак. Обучение с учителем фокусируется на идентификации и классификации известных угроз, что делает его мощным инструментом для прогнозирования кибератак на

Таблица 1

Основные виды кибератак

Вид кибератаки	Последствия
Фишинг	Кража конфиденциальной информации, финансовые потери, кража личности
Ransomware	Шифрование данных, нарушение работы, финансовые потери из-за выплат выкупа
DDoS-атаки	Недоступность услуг, нарушение операций, финансовые убытки
Вредоносное ПО	Несанкционированный доступ, кража данных, повреждение системы
Угрозы со стороны инсайдеров	Утечки данных, финансовые потери, ущерб репутации
Продвинутые постоянные угрозы (APT)	Долгосрочное нарушение данных, шпионаж, значительный финансовый и репутационный ущерб
SQL-инъекции	Кража данных, несанкционированный доступ, потеря целостности данных
Zero-Day Exploits	Эксплуатация до обнаружения, значительное нарушение данных, компрометация системы

Таблица 2

Преимущества и ограничения ML

Преимущества	Ограничения
Повышенная точность и скорость обнаружения угроз благодаря автоматизации и способности анализировать большие объемы данных	**Зависимость от качества и объема данных.** Недостаточное или некачественное обучающее множество может снизить эффективность моделей машинного обучения
Способность к обнаружению новых и сложных угроз, что трудно достижимо традиционными методами кибербезопасности	**Проблемы с фальсификацией и ложноположительными срабатываниями**, которые могут привести к ненужным тревогам и отвлечению ресурсов
Адаптивность и масштабируемость систем обнаружения, что критически важно в условиях постоянно развивающихся киберугроз	**Необходимость в постоянном обновлении моделей** для адаптации к новым угрозам и изменениям в данных

Таблица 3

Методы использования ML

Метод машинного обучения	Для прогнозирования кибератак	Для предотвращения кибератак
Обучение с учителем	Идентификация известных паттернов атак, классификация вредоносного трафика	Автоматическое блокирование известных угроз на основе предыдущих данных
Обучение без учителя	Выявление аномалий и необычных паттернов поведения, обнаружение новых угроз	Проактивное выявление и изоляция потенциальных угроз до их активации
Обучение с подкреплением	Адаптация к изменяющимся стратегиям атак, оптимизация решений в реальном времени	Динамическое управление безопасностью, настройка системы защиты в соответствии с текущей ситуацией

основе предыдущих данных [3]. Обучение без учителя выделяется своей способностью обнаруживать новые и неизвестные угрозы за счет выявления аномалий, что критически важно для прогнозирования. Обучение с подкреплением обеспечивает адаптацию к меняющимся стратегиям злоумышленников и оптимизацию защитных мер в реальном времени, что делает его ключевым для предотвращения атак.

Применение этих методов в области кибербезопасности не только увеличивает точность и скорость обнаружения угроз, но и усиливает способность системы адаптироваться и реагировать на новые и развивающиеся угрозы. Однако каждый метод имеет свои ограничения и требует комплексного подхода, включая сочетание различных стратегий и технологий для обеспечения максимальной защиты от кибератак.

Можно выделить следующие вызовы, связанные с использованием машинного обучения в кибербезопасности [4]:

1. Точность и ложные срабатывания: одним из основных вызовов является баланс между высокой точностью обнаружения угроз и минимизацией ложных срабатываний. Модели машинного обучения, особенно при обучении без учителя, могут генерировать ложные тревоги, что ведет к неоправданным затратам времени и ресурсов.

2. Адаптация к новым угрозам: быстро меняющийся ландшафт угроз требует от систем на основе машинного обучения способности к быстрой адаптации. Однако разработка и обновление моделей, способных справляться с новыми и эволюционирующими угрозами, представляет собой значительную проблему.

3. Зависимость от данных: эффективность машинного обучения напрямую зависит от качества и количества доступных данных для обучения. Недостаток или искажение в обучающих данных может привести к снижению эффективности моделей.

4. Вопросы приватности и этики:

– сбор и обработка данных: методы машинного обучения часто требуют обширных наборов данных, включая личную информацию пользователей. Это вызывает опасения по поводу приватности и защиты данных, а также этические вопросы относительно использования и распространения такой информации;

– **автономное принятие решений:** системы, способные к автономному принятию решений о блокировке доступа или действиях в ответ на угрозы, могут столкнуться с этическими дилеммами, особенно если такие решения влекут за собой юридические или финансовые последствия для пользователей.

5. Технические и операционные ограничения:

– ресурсы и инфраструктура: развертывание и поддержка мощных систем машинного обучения требуют значительных вычислительных ресурсов и специализированной инфраструктуры, что может быть недоступно для всех организаций;

– сложность интеграции: интеграция сложных моделей машинного обучения в существующие системы кибербезопасности может представлять технический вызов, требующий специальных знаний и навыков.

Для преодоления проблем и вызовов, связанных с использованием машинного обучения в кибербезопасности, можно предложить следующие решения:

1. Улучшение точности и снижение ложных срабатываний:

– разработка более сложных алгоритмов фильтрации и анализа данных для уменьшения ложных срабатываний;

– использование комбинации методов машинного обучения для улучшения обнаружения и точности классификации;

– регулярное обновление и переобучение моделей с использованием актуальных наборов данных для адаптации к новым угрозам.

2. Адаптация к новым угрозам:

– создание и поддержка широкомасштабных репозиториев данных об угрозах для обучения и тестирования моделей;

– применение техник обучения с подкреплением для разработки адаптивных систем, способных самостоятельно совершенствоваться в процессе эксплуатации.

3. Управление данными и приватность:

– разработка и внедрение строгих протоколов обработки и хранения данных с учетом требований к приватности и защите персональных данных;

– применение методов анонимизации и псевдонимизации данных для минимизации рисков для приватности пользователей.

4. Этические рассмотрения:

– разработка этических принципов и стандартов для использования машинного обучения в кибербезопасности, включая прозрачность и объяснимость решений системы;

– введение человеческого надзора для решений, принятых автономными системами, особенно в критически важных ситуациях.

5. Технические и операционные ограничения:

– инвестиции в облачные вычисления и услуги для обеспечения необходимой вычислительной мощности и инфраструктуры без значительных затрат на собственные ресурсы;

– проведение специализированных тренингов и курсов для улучшения квалификации специалистов в области кибербезопасности и машинного обучения.

При применении этих решений важно поддерживать баланс между инновациями и обеспечением безопасности и приватности, а также сотрудничать с регулирующими органами и другими заинтересованными сторонами для разработки и внедрения общепринятых стандартов и практик в области кибербезопасности и машинного обучения.

В статье рассмотрены ключевые аспекты использования машинного обучения в кибербезопасности, охватывая методы обучения, их применение для прогнозирования и предотвращения кибератак, а также сопутствующие проблемы и вызовы. Очевидно, что машинное обучение предоставляет мощные инструменты для улучшения защиты от киберугроз через автоматизированное обнаружение и реагирование на атаки. Однако внедрение этих технологий сопряжено с вызовами, включая необходимость обеспечения точности моделей, адаптации к новым угрозам, защиты данных и приватности, а также преодоления технических и операционных ограничений.

Преодолеть эти проблемы помогут комплексный подход к обучению моделей, сбалансированное использование различных методов машинного обучения, разработка этических принципов и стандартов, а также инвестиции в развитие инфраструктуры и квалификации специалистов. Таким образом, хотя машинное обучение представляет собой обещающее направление в кибербезопасности, его успешное применение требует внимательного учета как технических возможностей, так и потенциальных рисков.

СПИСОК ЛИТЕРАТУРЫ

1. Машинное обучение в кибербезопасности. – Электрон. текстовые дан. – Режим доступа: https://habr.com/ru/articles/534674/

2. Петров, А. А. Искусственный интеллект и машинное обучение в кибербезопасности: технологии и применение / А. А. Петров. – М. : Техносфера, 2019. – 256 с.

3. Романов, Д. В. Применение методов машинного обучения для обнаружения угроз в информационных системах / Д. В. Романов, А. С. Карпов // Компьютерные инструменты в образовании. – 2020. – Т. 13, № 4. – С. 153–165.

4. Чернов, А. А. Анализ и предотвращение угроз в компьютерных сетях с использованием алгоритмов машинного обучения / А. А. Чернов, В. В. Горбунов // Компьютерные исследования и моделирование. – 2021. – Т. 13, № 1. – С. 63–72.

5. Щербаков, А. Е. Исследование применения искусственного интеллекта и машинного обучения в области кибербезопасности: техники обнаружения аномалий и предотвращения угроз / А. Е. Щербаков // Вестник науки. – 2023. – Т. 1, № 7 (64). – С. 151–156.

6. Cyber Attack Statistics to Know. – Electronic text data. – Mode of access: https://www.cobalt.io/blog/cybersecurity-statistics-2024

7. Top Cybersecurity Statistics for 2024. – Electronic text data. – Mode of access: https://www.cobalt.io/blog/cybersecurity-statistics-2024

8. 2024 Must-Know Cyber Attack Statistics and Trends. – Electronic text data. – Mode of access: https://www.embroker.com/blog/cyber-attack-statistics/

REFERENCES

1. *Mashinnoe obuchenie v kiberbezopasnosti* [Machine Learning in Cybersecurity]. URL: https://habr.com/ru/articles/534674/

2. Petrov A.A. *Iskusstvennyj intellekt i mashinnoe obuchenie v kiberbezopasnosti: tehnologii i primenenie* [Artificial Intelligence and Machine Learning in Cybersecurity: Technology and Application]. Moscow, Technosphera Publ., 2019. 256 p.

3. Romanov D.V., Karpov A.S. Primenenie metodov mashinnogo obuchenija dlja obnaruzhenija ugroz v informacionnyh sistemah [Application of Machine Learning Methods for Threat Detection in Information Systems]. *Kompyjuternye instrumenty v obrazovanii* [Computer Tools in Education], 2020, vol. 13, no. 4, pp. 153-165.

4. Chernov A.A., Gorbunov V.V. Analiz i predotvrashhenie ugroz v kompyjuternyh setjah s ispolzovaniem algoritmov mashinnogo obuchenija [Analysis and Prevention of Threats in Computer Networks Using Machine Learning Algorithms]. *Kompyjuternye issledovanija i modelirovanie* [Computer Research and Modeling], 2021, vol. 13, no. 1, pp. 63-72.

5. Scherbakov A.E. Issledovanie primenenija iskusstvennogo intellekta i mashinnogo obuchenija v oblasti kiberbezopasnosti: tehniki obnaruzhenija anomalij i predotvrashhenija ugroz [Research on the Application of Artificial Intelligence and Machine Learning in the Field of Cybersecurity: Anomaly Detection and Threat Prevention Techniques]. *Vestnik nauki* [Bulletin of Science], 2023, vol. 1, no. 7 (64), pp. 151-156.

6. *Cyber Attack Statistics to Know*. URL: https://www.cobalt.io/blog/cybersecurity-statistics-2024

7. *Top Cybersecurity Statistics for 2024*. URL: https://www.cobalt.io/blog/cybersecurity-statistics-2024

8. *2024 Must-Know Cyber Attack Statistics and Trends*. URL: https://www.embroker.com/blog/cyber-attack-statistics/

MACHINE LEARNING METHODS IN PREDICTING AND PREVENTING CYBER ATTACKS

Alexander V. Loschilin

Master's Student, Department of Information Security,
Volgograd State University
a_loshilina@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Vladislav G. Yarikov

Candidate of Sciences (Pedagogy), Associate Professor,
Department of Information Security,
Volgograd State University
yarikov.vladislav@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Arina V. Nikishova

Candidate of Sciences (Engineering), Associate Professor,
Department of Information Security,
Volgograd State University
nikishova.arina@volsu.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Abstract. This article examines the role of machine learning (ML) in predicting and preventing cyberattacks, detailing the use of supervised, unsupervised, and reinforcement learning techniques. The article discusses the benefits and challenges of integrating ML into cybersecurity, including accuracy, privacy concerns, and technical difficulties. Solutions to overcome these challenges, such as continuous model refinement and ethical compliance, are also proposed, highlighting the potential of ML to enhance cyber defense strategies. Key aspects of the use of machine learning in cybersecurity are reviewed: machine learning techniques, their application to predicting and preventing cyberattacks, and related issues and challenges. It is clear that machine learning provides powerful tools to improve defense against

cyber threats by automatically detecting and responding to attacks. However, there are challenges to implementing these technologies, including the need to ensure model accuracy, adapt to new threats, protect data and privacy, and overcome technical and operational limitations. An integrated approach to training models, balancing the use of different machine learning techniques, developing ethical principles and standards, and investing in infrastructure and skills will help overcome these challenges. Thus, while machine learning represents a promising trend in cybersecurity, its successful application requires careful consideration of both technical capabilities and potential risks.

Key words: machine learning, cybersecurity, predicting cyberattacks, preventing cyberattacks, machine learning challenges, data privacy.