Тикки Д.А. и др. Применение искусственного интеллекта в информационной безопасности // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 1(39) с. 62–67

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.67

# ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Тикки Д.А., Никольский В.Е., Авакян Е.В., Самошкин Н.С., [1]Мокряк А.В.**
*ФГБОУ ВО "РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ" Санкт-Петербург, Россия (192007, город Санкт-Петербург, Воронежская ул., д. 79)*
*[1]ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ УНИВЕРСИТЕТ ГОСУДАРСТВЕННОЙ ПРОТИВОПОЖАРНОЙ СЛУЖБЫ МИНИСТЕРСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ДЕЛАМ ГРАЖДАНСКОЙ ОБОРОНЫ, ЧРЕЗВЫЧАЙНЫМ СИТУАЦИЯМ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ СТИХИЙНЫХ БЕДСТВИЙ ИМЕНИ ГЕРОЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ГЕНЕРАЛА АРМИИ Е.Н.ЗИНИЧЕВА", Санкт-Петербург, Россия (196105, г.Санкт-Петербург, Московский проспект, д.149), e-mail: mokryakanna@mail.ru*

**Искусственный интеллект (ИИ) играет важную роль в обеспечении информационной безопасности. Технологии ИИ могут быть применены для обнаружения аномального поведения в сети, анализа больших объемов данных для выявления угроз и автоматизации процессов реагирования на кибератаки. Применение машинного обучения и алгоритмов ИИ позволяет создавать более эффективные системы защиты информации. Цель данной статьи заключается в рассмотрении применения искусственного интеллекта в сфере информационной безопасности. Рассмотрены основные задачи, решаемые ИИ, а также проанализированы преимущества и недостатки его использования.**

Ключевые слова: Искусственный интеллект, информационная безопасность, угрозы, кибератаки.

# APPLICATION OF ARTIFICIAL INTELLIGENCE IN INFORMATION SECURITY

**Tikki D.A., Nikolsky V.E., Avakyan E.V., Samoshkin N.S., [1]Mokryak A.V.**
*RUSSIAN STATE HYDROMETEOROLOGICAL UNIVERSITY, St. Petersburg, Russia (192007, St. Petersburg, Voronezhskaya str., 79)*
*[1]ST. PETERSBURG UNIVERSITY OF THE STATE FIRE SERVICE OF THE MINISTRY OF THE RUSSIAN FEDERATION FOR CIVIL DEFENSE, EMERGENCIES AND ELIMINATION OF CONSEQUENCES OF NATURAL DISASTERS NAMED AFTER THE HERO OF THE RUSSIAN FEDERATION, GENERAL OF THE ARMY E.N. ZINICHEV, St. Petersburg, Russia (196105, St. Petersburg, Moskovsky prospekt,149), e-mail: [1]mokryakanna@mail.ru*

**Artificial intelligence (AI) plays an important role in information security. AI technologies can be used to detect anomalous behavior on the network, analyze large volumes of data to identify threats, and automate response processes to cyber attacks. The use of machine learning and AI algorithms makes it possible to create more effective information security systems. The purpose of this article is to consider the application of artificial intelligence in the field of information security. The main problems solved by AI are considered, and the advantages and disadvantages of its use are analyzed.**

Keywords: Artificial intelligence, information security, threats, cyber attacks.

**Введение**

В современном цифровом мире, где технологии продолжают эволюционировать, обеспечение информационной безопасности становится одним из наиболее острых и важных вопросов. В этом контексте искусственный интеллект (ИИ) не только играет ключевую роль, но и представляет собой непревзойденный инструмент для защиты цифровых систем от угроз.

Применение искусственного интеллекта в области информационной безопасности открывает новые горизонты в предотвращении кибератак, обнаружении уязвимостей и реагировании на угрозы в реальном времени. Стремительное развитие технологий приводит к постоянно возрастающей сложности угроз, и ИИ становится неотъемлемой частью эффективной стратегии защиты информации [1].

В данной статье мы рассмотрим ключевые аспекты применения искусственного интеллекта в обеспечении информационной безопасности. От его роли в обнаружении и анализе потенциальных угроз до автоматизации процессов реагирования на кибератаки, ИИ превращается в мощный инструмент, позволяющий эффективно бороться с современными цифровыми угрозами. Рассмотрим преимущества, вызовы и перспективы использования искусственного интеллекта в сфере информационной безопасности, а также его влияние на создание более защищенной цифровой среды.

**Методика исследования**

В современном мире цифровизации и передовых технологий, обеспечение безопасности информации становится приоритетом для организаций и частных лиц. Искусственный интеллект играет важную роль в эффективной защите данных и сетей от постоянно возрастающих киберугроз [2].

*Обнаружение и предотвращение кибератак*

ИИ, основанный на алгоритмах машинного обучения, является мощным инструментом для обнаружения необычных или вредоносных паттернов в сетевом трафике. Автоматизированные системы анализируют огромные объемы данных, выявляют аномалии и моментально реагируют на потенциальные угрозы, сокращая время реакции и уменьшая возможные последствия атак.

1. Анализ и прогнозирование угроз.

Искусственный интеллект позволяет создавать прогностические модели на основе данных о предыдущих атаках и уязвимостях. Это обеспечивает возможность предсказания потенциальных угроз и принятия мер для их предотвращения до возникновения проблем, что повышает эффективность стратегий безопасности.

2. Улучшение систем безопасности через обучение.

Системы ИИ, использующие обучение с подкреплением, могут постоянно улучшать свои навыки и адаптироваться к новым сценариям атак. Благодаря этому они эффективнее справляются с постоянно меняющимися угрозами и уязвимостями, предоставляя более надежную защиту.

3. Автоматизация процессов обеспечения безопасности.

ИИ позволяет создавать автономные системы безопасности, способные реагировать на угрозы без человеческого вмешательства. Это включает в себя автоматизацию процессов реагирования на инциденты безопасности, сокращая время реакции и уменьшая потенциальные потери данных.

4. Этические и правовые аспекты.

Помимо технических аспектов, важно уделить внимание этическим и правовым вопросам использования ИИ в обеспечении информационной безопасности. Обеспечение прозрачности, соблюдение правовых норм и этических стандартов играют ключевую роль в устойчивом и эффективном применении технологий ИИ.

5. Будущие тенденции и перспективы.

С развитием технологий машинного обучения и глубокого обучения использование ИИ в информационной безопасности будет только углубляться. Новые возможности в области предотвращения и реагирования на кибератаки представляют собой перспективу создания более интеллектуальных и эффективных систем защиты данных [3–5].

Применение искусственного интеллекта в информационной безопасности становится все более значимым, и его влияние будет продолжать расти в будущем.

Рассмотрим недостатки и преимущества использования искусственного интеллекта в сфере информационной безопасности.

Преимущества:

1. Скорость и точность.

- Быстрая реакция. ИИ способен обрабатывать и анализировать большие объемы данных в реальном времени, что позволяет быстро реагировать на угрозы.
- Точность. Автоматизированные системы способны выявлять аномалии и угрозы с высокой точностью, минимизируя ошибки человеческого фактора.

2. Автоматизация и оптимизация.

- Уменьшение человеческого вмешательства. Использование ИИ позволяет автоматизировать рутинные задачи, освобождая ресурсы для более стратегических задач.
- Оптимизация процессов безопасности. Автономные системы с ИИ способны принимать решения и реагировать на угрозы без задержек, улучшая эффективность обеспечения безопасности [6].

3. Обучение на опыте.

- Постоянное улучшение. ИИ системы могут улучшаться с каждым новым обнаруженным инцидентом, учась на своих ошибках и адаптируясь к новым угрозам.

Недостатки:

1. Необходимость больших объемов данных.

- Зависимость от данных. Для эффективного функционирования искусственного интеллекта необходимы большие объемы данных для обучения, которые может быть трудно получить при ограниченном доступе к информации или недостатке данных.

2. Этические и юридические вопросы.

- Прозрачность и ответственность. Использование ИИ в сфере безопасности встречает вызовы в области этики и ответственности, включая вопросы конфиденциальности данных и человеческого вмешательства [7].

3. Потенциальные уязвимости и ошибки.

- Уязвимость перед атаками. Такие системы могут стать объектом атак или использоваться для злонамеренных целей, что требует дополнительных мер безопасности [8, 9].
- Ошибки в принятии решений. В случае неправильной настройки или обучения ИИ, системы могут делать неправильные выводы или рекомендации, повышая риск возникновения ошибок.

Использование искусственного интеллекта в информационной безопасности приносит значительные преимущества, но также ставит перед нами вызовы, требующие балансировки между техническими возможностями, этическими аспектами и обеспечением надежной защиты от возможных угроз [10].

**Выводы**

Искусственный интеллект становится неотъемлемым компонентом системы информационной безопасности, предлагая инновационные инструменты для выявления, защиты и реагирования на киберугрозы. Возможности, которые открывает использование искусственного интеллекта, значительно повышают эффективность систем безопасности, сокращают время реагирования на угрозы и минимизируют потенциальный ущерб от кибератак.

Использование искусственного интеллекта в сфере информационной безопасности открывает ряд перспективных направлений для развития в будущем. Развитие технологий машинного обучения, в частности глубокого обучения и нейронных сетей, позволит разрабатывать более точные и эффективные системы обнаружения угроз и защиты информации. Стремительное развитие технологий обучения и самообучения позволит системам стать более автономными и адаптируемыми. Это обеспечит использование более интеллектуальных методов борьбы с киберугрозами, позволяя системам более точно прогнозировать и предотвращать атаки до их возникновения. Вместе с тем развитие этических и правовых норм использования искусственного интеллекта для обеспечения информационной безопасности будет способствовать разработке прозрачных и ответственных подходов к защите информации, поддерживающих высокий уровень конфиденциальности и соблюдение нормативных требований. Эти перспективы закладывают основу для создания более надежной и безопасной цифровой среды, в которой использование передовых технологий и соблюдение этических стандартов позволит эффективно обеспечивать информационную безопасность.

Развитие искусственного интеллекта продолжается, открывая новые возможности для обеспечения безопасности в цифровом мире. Применение искусственного интеллекта в сфере информационной безопасности позволяет предвидеть и адекватно реагировать на киберугрозы, создавая более безопасную цифровую среду для всех пользователей.

**Список литературы**

1. Искусственный интеллект в информационной безопасности. Электронный ресурс – Режим доступа: https://www.securityvision.ru/blog/iskusstvennyy-intellekt-v-informatsionnoy-bezopasnosti/ (Дата обращения: 07.12.2023)

2. Булгакова А.В., Сафонова Т.В., Кутикова В.С. Классификация нейронных сетей / Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 11-18.
3. Как повлияет AI на информационную безопасность. Электронный ресурс – Режим доступа: https://is.astral.ru/news/blog/kak-povliyaet-ai-na-ib/ (Дата обращения: 08.12.2023)
4. Тикки Д.А., Никольский В.Е., Сафонова Т.В., Самошкин Н.С., Авакян Е.В. Использование облачных технологий для оптимизации бизнес-процессов / Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 76-79.
5. Искусственный интеллект в безопасности. Электронный ресурс – Режим доступа: https://cloudnetworks.ru/analitika/iskusstvennyj-intellekt-v-bezopasnosti/ (Дата обращения: 09.12.2023)
6. Булгакова А.В., Сафонова Т.В., Диденко А.Ю. Этапы разработки и внедрения нейронной сети в проект / Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 1 (45). С. 87-92.
7. Искусственный интеллект как инструмент ИБ. Электронный ресурс – Режим доступа: https://www.iksmedia.ru/articles/5691654-Iskusstvennyj-intellekt-kak-instrum.html (Дата обращения: 09.12.2023)
8. Булгакова А.В., Сафонова Т.В., Кирспуу К.А. Применение облачных решений на предприятии / Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 2 (46). С. 71-76.
9. Применение искусственного интеллекта в обеспечении безопасности данных. Электронный ресурс – Режим доступа: https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-v-obespechenii-bezopasnosti-dannyh (Дата обращения: 10.12.2023)
10. Булгакова А.В., Сафонова Т.В. Область применения гипераватоматизации в условиях цифровой трансформации производства / Информационные технологии и системы: управление, экономика, транспорт, право. 2023. № 2 (46). С. 77-82.

**References**

1. Artificial intelligence in information security. Electronic resource – Access mode: https://www.securityvision.ru/blog/iskusstvennyy-intellekt-v-informatsionnoy-bezopasnosti / (Date of request: 07.12.2023)
2. Bulgakova A.V., Safonova T.V., Kutikova V.S. Classification of neural networks / Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 11-18.
3. How AI will affect information security. Electronic resource – Access mode: https://is.astral.ru/news/blog/kak-povliyaet-ai-na-ib / (Date of request: 08.12.2023)
4. Tikki D.A., Nikolsky V.E., Safonova T.V., Samoshkin N.S., Avakian E.V. Using cloud technologies to optimize business processes / Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 76-79.
5. Artificial intelligence in security. Electronic resource – Access mode: https://cloudnetworks.ru/analitika/iskusstvennyj-intellekt-v-bezopasnosti / (Date of request: 09.12.2023)

6. Bulgakova A.V., Safonova T.V., Didenko A.Yu. Stages of development and implementation of a neural network in a project / Information technologies and systems: management, economics, transport, law. 2023. No. 1 (45). pp. 87-92.
7. Artificial intelligence as an information security tool. Electronic resource – Access mode: https://www.iksmedia.ru/articles/5691654-Iskusstvennyj-intellekt-kak-instrum.html (Date of application: 09.12.2023)
8. Bulgakova A.V., Safonova T.V., Kirspuu K.A. Application of cloud solutions in the enterprise / Information technologies and systems: management, economics, transport, law. 2023. No. 2 (46). pp. 71-76.
9. The use of artificial intelligence in ensuring data security. Electronic resource – Access mode: https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-v-obespechenii-bezopasnosti-dannyh (Date of application: 10.12.2023)
10. Bulgakova A.V., Safonova T.V. The scope of hyperautomatization in the conditions of digital transformation of production / Information technologies and systems: management, economics, transport, law. 2023. No. 2 (46). pp. 77-82.