www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2024.4.3

УДК 004.8:004.056.5
ББК 32.813

РОЛЬ И ЗНАЧЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ: ПЕРСПЕКТИВЫ И ВЫЗОВЫ

Александр Валерьевич Лощилин

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

Олеся Александровна Какорина

Кандидат физико-математических наук,
Заведующий кафедрой информационной безопасности,
Волгоградский государственный университет
davletova.olesya@volsu.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

Аннотация. В современном цифровом обществе безопасность информации становится критически важной задачей, и внедрение искусственного интеллекта (далее – ИИ) в эту сферу представляет собой необходимое решение. ИИ обладает уникальными возможностями обработки больших объемов данных и выявления угроз, что делает его мощным инструментом в борьбе с киберугрозами. Настоящее исследование анализирует роль ИИ в обеспечении безопасности информационных систем, рассматривая методы его применения, перспективы и вызовы, с которыми сталкиваются системы безопасности. В работе представлены статистические данные о применении ИИ в различных отраслях, а также сравнительный анализ методов, таких как машинное обучение, обработка естественного языка и экспертные системы. Каждый из методов имеет свои преимущества и ограничения, что подчеркивает необходимость тщательного выбора подходящих технологий для конкретных задач. Исследование также выявляет проблемы, связанные с внедрением ИИ, такие как защита данных, этические вопросы и нехватка квалифицированных специалистов. В заключение подчеркивается, что ИИ способен значительно улучшить защиту информационных систем, обеспечи-

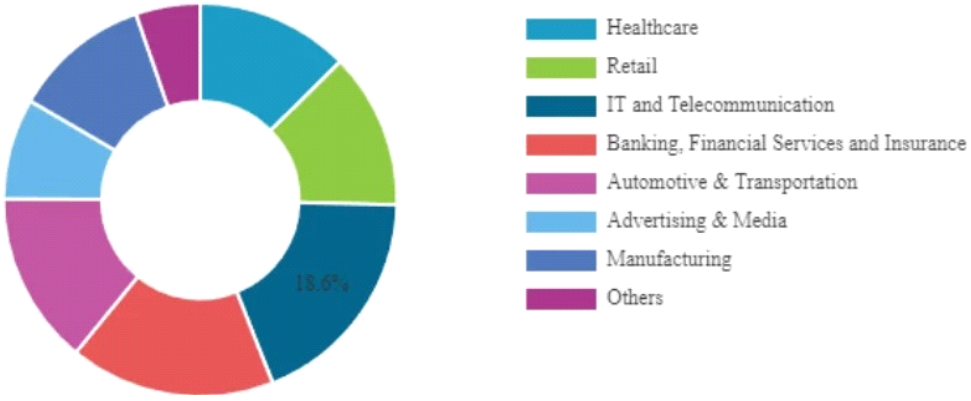
вая более оперативное выявление и предотвращение киберугроз, и указывается на необходимость дальнейших исследований в этой области для оптимизации алгоритмов и методов обнаружения угроз.

Ключевые слова: искусственный интеллект, кибербезопасность, обнаружение угроз, машинное обучение, защита информационных систем, алгоритмы ИИ.

В современном цифровом обществе безопасность информации становится все более актуальной и важной проблемой. В этом контексте внедрение ИИ в область обеспечения безопасности информационных систем становится необходимым решением. Искусственный интеллект обладает уникальными способностями в обработке больших объемов данных и выявлении угроз, что делает его мощным инструментом в борьбе с киберугрозами. Настоящее исследование направлено на анализ роли и значимости искусственного интеллекта в обеспечении безопасности информационных систем, включая основные методы применения, перспективы использования и вызовы, с которыми сталкиваются системы безопасности при его внедрении.

На рисунке представлена статистика использования ИИ в различных отраслях экономики, как видно IT-отрасли и телекоммуникациях являются лидерами [3].

ИИ широко используется в обеспечении безопасности информационных систем, предоставляя широкий набор методов и технологий для выявления и предотвращения угроз [5]. Методы и технологии ИИ представлены в таблице 1.



Использование ИИ по отраслям экономики

Таблица 1

Сравнение методов ИИ

Название метода	Описание	Примеры использования	Преимущества	Ограничения
Машинное обучение	Алгоритмы, адаптирующиеся на основе данных	Прогнозирование, рекомендательные системы	Способность обучения и адаптации, большой объём данных	Требуют много данных, возможность переобучения
Обработка естественного языка (NLP)	Технологии для понимания и обработки человеческого языка	Чат-боты, анализ тональности текстов	Улучшение интерфейсов и коммуникаций	Сложность понимания контекста
Генетические алгоритмы	Методы оптимизации на основе принципов естественного отбора	Оптимизация маршрутов	Эффективность поиска нестандартных решений	Время затратность настройки
Экспертные системы	Имитация решений эксперта в узкой области	Медицинская диагностика	Накопление и структурирование знаний	Трудность обновления и поддержки

Из таблицы 1 следует, что каждый метод нашел применение и обладает рядом преимуществ в различных областях, в то же время каждый метод сталкивается с определенными ограничениями, такими как требования к данным, вычислительные затраты и сложности в интерпретации результатов. В целом эффективное применение ИИ требует тщательного выбора подходящих методов в соответствии с конкретными задачами и ограничениями.

Методы ИИ можно использовать для анализа сетевого трафика и обнаружения аномальных или вредоносных действий в сети, а также для выявления необычных или подозрительных действий пользователей, что может свидетельствовать о компрометации учетных записей [1].

ИИ способен анализировать большие объемы данных и выявлять скрытые недостатки, что позволяет более эффективно обнаруживать угрозы, включая новые и ранее неизвестные виды атак [7]. ИИ представляет собой мощный инструмент, способный значительно улучшить защиту данных и инфраструктуры организаций от киберугроз [6].

Но в свою очередь применение искусственного интеллекта в области защиты информации сталкивается с рядом проблем. Основные проблемы и возможности их решения представлены в таблице 2 [2].

Решение этих проблем, а также разработка стратегий и методов их преодоления, является важным шагом в успешном внедрении искусственного интеллекта в область обеспечения безопасности информационных систем [4].

Для внедрения и повышения эффективности использования искусственного интеллекта в области информационной безопасности необходимо разрабатывать и оптимизировать алгоритмы машинного обучения для более точного обнаружения аномалий и угроз в информационных системах, разработать оптимальные стратегии реагирования на угрозы и адаптироваться к изменяющимся условиям среды.

В данном исследовании были рассмотрены ключевые аспекты роли и значимости ИИ в обеспечении безопасности информационных систем. Проанализированы методы применения ИИ, успешные примеры его использования, вызовы, с которыми сталкиваются системы безопасности, а также перспективы развития данной области.

Сводные выводы исследования позволяют подчеркнуть, что искусственный интеллект играет ключевую роль в повышении эффективности защиты информационных систем. Благодаря возможностям анализа больших объемов данных, обнаружения аномалий и принятия автоматизированных решений, ИИ

Таблица 2

Проблемы и возможности их решения

Проблема	Возможные решения	Примеры успешных практик	Потенциальные риски
Защита данных	Разработка комплексных систем безопасности, обучение сотрудников основам кибергигиены	Использование шифрования, многофакторной аутентификации	Утечки данных, хакерские атаки
Этические вопросы	Разработка этических принципов и стандартов, учет социальных и культурных факторов	Этические комитеты в IT-компаниях, общественные дискуссии	Дискриминация, предвзятость алгоритмов
Интеграция с существующими системами	Постепенное внедрение ИИ, использование API и микросервисной архитектуры	Интеграция ИИ в CRM-системы, модернизация IT-инфраструктуры	Технические несоответствия, затраты на переход
Нехватка квалифицированных специалистов	Программы обучения и переподготовки, привлечение иностранных специалистов	Сотрудничество с университетами, корпоративные университеты	Высокая конкуренция за таланты
Сопротивление изменениям	Коммуникационные кампании, обучение и вовлечение сотрудников в процесс цифровой трансформации	Пилотные проекты с демонстрацией успешных результатов, программа «послов цифровизации»	Снижение продуктивности, неудовлетворенность

способствует более оперативному выявлению и предотвращению киберугроз.

Значимость роли искусственного интеллекта в обеспечении безопасности информационных систем подчеркивается его способностью к адаптации к изменяющимся условиям и контекстам, а также возможностью создания инновационных методов защиты.

Исследование указывает на необходимость дальнейших исследований в этой области, включая улучшение алгоритмов и методов обнаружения угроз, разработку новых моделей управления доступом и фокус на прозрачности и объяснимости решений искусственного интеллекта.

В целом развитие и применение искусственного интеллекта в области безопасности информационных систем представляет собой перспективное направление, способствующее улучшению защиты данных и инфраструктуры организаций от киберугроз.

СПИСОК ЛИТЕРАТУРЫ

1. Деревянченко, В. П. Интеграция искусственного интеллекта в системы информационной безопасности / В. П. Деревянченко // Научный лидер. – 2024. – № 5 (155).

2. Рахматов, Д. Искусственный интеллект и кибербезопасность: возможности и вызовы / Д. Рахматов // Всероссийская научно-техническая конференция студентов, аспирантов и молодых ученых, посвященная 65-летию филиала УГНТУ в г. Салавате. – Уфа : Изд-во УГНТУ, 2021. – С. 13–15.

3. Статистика искусственного интеллекта (2024) // ИНКЛИЕНТ : офиц. сайт. – Электрон. текстовые дан. – Режим доступа: https://inclient.ru/ai-stats/. – Загл. с экрана.

4. Хакимов, А. А. Роль искусственного интеллекта в кибербезопасности / А. А. Хакимов // Universum: технические науки. – 2023. – Т. 11-1, № 116. – URL: https://cyberleninka.ru/article/n/rol-iskusstvennogo-intellekta-v-kiberbezopasnosti

5. Collins, C. Artificial Intelligence in Information Systems Research: A Systematic Literature Review and Research Agenda / C. Collins, D. Dennehy, K. Conboy, P. Mikalef // International Journal of Information Management. – 2021. – Vol. 60. – Art. 102383.

6. Kaur, R. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions / R. Kaur, D. Gabrijelčič, T. Klobučar // Information Fusion. – Art. 101804. – DOI: 10.1016/j.inffus.2023.101804

7. Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities / Z. Zhang [et al.] // Artificial Intelligence Review. – 2022. – № 2 (55). – P. 1029–1053. – DOI: 10.1007/s10462-021-09976-0

REFERENCES

1. Derevyanchenko V.P. Integracija iskusstvennogo intellekta v sistemy informacionnoj bezopasnosti [Integration of Artificial Intelligence in Information Security Systems]. *Nauchnyj lider* [Scientific Leader], 2024, vol. 5 (155).

2. Rahmatov D. Iskusstvennyj intellekt i kiberbezopasnost': vozmozhnosti i vyzovy [Artificial Intelligence and Cyber Security: Opportunities and Challenges]. *Vserossijskaya nauchno-tehnicheskaya konferenciya studentov, aspirantov i molodyh uchenyh, posvjashhennaya 65-letiju filiala UGNTU v g. Salavate* [All-Russian Scientific and Technical Conference of Students, Graduate Students and Young Scientists, Dedicated to the 65th Anniversary of the Branch of UGNTU in Salavat]. Ufa, UGNTU Publ., 2021, pp. 13-15.

3. Statistika iskusstvennogo intellekta (2024) [Artificial Intelligence Statistics (2024)]. *INKLIENT: ofitc. sait* [INKLIENT. Official Site]. URL: https://inclient.ru/ai-stats/

4. Khakimov A.A. Rol' iskusstvennogo intellekta v kiberbezopasnosti [The Role of Artificial Intelligence in Cyber Security]. *Universum: tehnicheskie nauki* [Universum: Technical Sciences], 2023, vol. 11-1, no. 116. URL: https://cyberleninka.ru/article/n/rol-iskusstvennogo-intellekta-v-kiberbezopasnosti

5. Collins C., Dennehy D., Conboy K., Mikalef P. Artificial Intelligence in Information Systems Research: A Systematic Literature Review and Research Agenda. *International Journal of Information Management*, 2021, vol. 60, pp. 102383.

6. Kaur, R., Gabrijelčič D., Klobučar T. Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions. *Information Fusion*, pp. 101804. DOI: 10.1016/j.inffus.2023.101804

7. Zhang Z., Ning H., Shi F., Farha F., Xu Y., Xu J., Zhang F., Choo K.-K.R. Artificial Intelligence in Cyber Security: Research Advances, Challenges, and Opportunities. *Artificial Intelligence Review*, 2022, vol. 2 (55), pp. 1029-1053. DOI: 10.1007/s10462-021-09976-0

THE ROLE AND SIGNIFICANCE OF ARTIFICIAL INTELLIGENCE IN ENSURING THE SECURITY OF INFORMATION SYSTEMS: PROSPECTS AND CHALLENGES

Alexander V. Loschilin

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

Olesya A. Kakorina

Candidate of Sciences (Physics and Mathematics),
Head of the Department of Information Security,
Volgograd State University
davletova.olesya@volsu.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

Abstract. In today's digital society, information security is becoming a critically important task, and the introduction of artificial intelligence (AI) in this area is a necessary solution. AI has unique capabilities for processing large amounts of data and detecting threats, which makes it a powerful tool in the fight against cyber threats. This study analyzes the role of AI in ensuring the security of information systems, considering the methods of its application, prospects and challenges faced by security systems. The paper presents statistical data on the use of AI in various industries, as well as a comparative analysis of methods such as machine learning, natural language processing and expert systems. Each of the methods has its advantages and limitations, which emphasizes the need for careful selection of appropriate technologies for specific tasks. The study also identifies problems related to the implementation of AI, such as data protection, ethical issues and a shortage of qualified specialists. In conclusion, it is emphasized that AI can significantly improve the protection of information systems, providing more rapid detection and prevention of cyber threats, and indicates the need for further research in this area to optimize algorithms and methods for detecting threats.

Key words: artificial intelligence, cybersecurity, threat detection, machine learning, information system protection, AI algorithms.