УДК 004.8

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБЕСПЕЧЕНИИ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Д.А. Коренев, студент гр. БПЭ22-01, III курс
Научный руководитель: Кукарцев А.В., к.э.н., доцент
Сибирский государственный университет науки и технологий имени академика Михаила Фёдоровича Решетнёва
г. Красноярск

Современные условия стремительно развивающихся технологий требуют нового подхода к обеспечению национальной безопасности. В данном контексте искусственный интеллект (ИИ) приобретает особое значение как ключевой инструмент повышения эффективности и надежности систем защиты. Способность ИИ к анализу больших объемов данных, прогнозированию событий и принятию решений в реальном времени открывает значительные перспективы для защиты национальных интересов и противодействия возникающим угрозам.

Одной из важнейших сфер применения ИИ является борьба с киберугрозами [1]. Системы на основе ИИ демонстрируют высокую эффективность в защите информационных инфраструктур путем оперативного обнаружения, предотвращения и реагирования на кибератаки. Использование алгоритмов машинного обучения позволяет таким системам выявлять аномалии в поведении пользователей и сетей, что существенно повышает уровень защищенности цифровых активов. Примером успешного внедрения таких технологий служат системы обнаружения вторжений *(*IDS*),* которые осуществляют мониторинг сетевого трафика и автоматически реагируют на подозрительные активности, обеспечивая своевременное предупреждение служб безопасности [2]. Искусственный интеллект также находит широкое применение в исследовании вредоносного программного обеспечения. Применение ИИ для анализа образцов вредоносных программ позволяет быстро выявлять новые угрозы и разрабатывать эффективные защитные меры. Другим примером эффективного использования ИИ является обнаружение фишинговых атак, где системы на основе ИИ анализируют контент электронных писем и поведенческие характеристики отправителей, снижая риск успешных кибератак.

Искусственный интеллект значительно увеличивает эффективность процессов выявления угроз и принятия соответствующих мер [3]. Обрабатывая данные из множества источников с высокой скоростью и точностью, такие системы обеспечивают раннюю оценку уровня риска, расстановку приоритетов среди потенциальных угроз и предложение оптимальных вариантов реагирования. Прогностическая аналитика, основанная на анализе

исторических данных и выявлении повторяющихся паттернов, позволяет предсказывать возникновение угроз задолго до их реализации, что способствует снижению общего уровня уязвимости систем [4]. Автоматизированное реагирование, обеспечиваемое системами ИИ, представляет собой важный компонент современной кибербезопасности. В случае обнаружения угроз такие системы способны самостоятельно предпринимать необходимые меры, включая изоляцию поражённых участков сети и предотвращение дальнейшего распространения атак, что значительно повышает оперативность и эффективность защитных механизмов.

Применение ИИ в деятельности спецслужб также демонстрирует свою значимость. Благодаря автоматизации процессов обработки информации, получаемой из различных источников, таких как социальные сети, спутниковые снимки и перехваченные сообщения, ИИ позволяет ускорить и улучшить точность выявления потенциальных угроз и новых тенденций в сфере безопасности. Методы обработки естественного языка (NLP) используются для извлечения значимых данных из текстовой информации, а геопространственный анализ ИИ-систем позволяет эффективно отслеживать изменения в целевых зонах и выявлять потенциальные угрозы, предоставляя спецслужбам необходимые инструменты для оперативного реагирования [5].

Несмотря на значительный потенциал ИИ в обеспечении национальной безопасности, его применение связано с рядом этических проблем. Одна из основных сложностей связана с вопросами конфиденциальности и права на частную жизнь. Масштабное наблюдение и анализ данных граждан с использованием ИИ вызывают опасения касательно возможного злоупотребления властью [6]. Для поддержания баланса между безопасностью и правами человека необходимы чётко сформулированные правовые нормы, регулирующие сбор и использование персональных данных. Также возникают вопросы ответственности за решения, принятые ИИ. Создание механизмов контроля и аудита, обеспечивающих проверку и коррекцию работы ИИ, представляется важной задачей для минимизации рисков негативных последствий [7]. Ещё одной проблемой является предвзятость алгоритмов. ИИ обучается на существующих данных, которые могут содержать исторически обусловленные предрассудки или искажения. Это может приводить к дискриминационным решениям, особенно в областях, связанных с идентификацией личности или оценкой рисков. Следовательно, крайне важно разрабатывать алгоритмы, свободные от предвзятостей, и проводить регулярное тестирование на предмет объективности.

Будущее развитие ИИ характеризуется рядом перспектив и вызовов. Ожидается, что увеличение вычислительных мощностей и улучшение методов машинного обучения приведут к созданию более сложных и точных моделей, способных решать широкий спектр задач [8]. Однако параллельно возрастает и угроза со стороны злоумышленников, использующих ИИ для разработки более изощрённых атак. В этой связи необходима постоянная модернизация защитных систем и разработка стратегий киберустойчивости, включающих

активное обучение персонала и проведение регулярных тестов на проникновение.

Интеграция ИИ с квантовыми вычислениями представляет собой ещё одну важную тенденцию. Квантовые вычисления обладают колоссальным потенциалом для революции в области искусственного интеллекта, предлагая невиданные ранее уровни вычислительной мощности [9]. Эта технология способна кардинально расширить возможности ИИ, позволив ему справляться с обработкой сложных данных и решением задач, которые сегодня остаются вне досягаемости классических компьютеров. Квантовый ИИ обещает преобразовать подходы к анализу гигантских объемов информации и моделированию комплексных сценариев [10]. Однако его развитие требует значительных капиталовложений и тесного взаимодействия между государственными институтами и коммерческим сектором. Международное сотрудничество также становится жизненно важным, поскольку конкуренция национальных интересов диктует необходимость выработки единых стандартов и правил регулирования ИИ в области безопасности.

В заключение хочется сказать, что искусственный интеллект становится важным инструментом для повышения национальной безопасности, улучшая защиту от киберугроз и повышая эффективность аналитических процессов. Вместе с тем, его внедрение требует решения этических и правовых вопросов, таких как защита конфиденциальности и контроль за алгоритмами.

Список литературы:

1. Борьба с киберугрозами [Электронный ресурс] URL: https://www.marketresearchintellect.com/ru/blog/ai-technologies-empowering-the-future-of-security-and-national-protection/ (дата обращения: 20.02.2025).

2. Methods of developing a competitive strategy of the agricultural enterprise / V. S. Tynchenko, N. V. Fedorova, V. V. Kukartsev [et al.] // IOP Conference Series: Earth and Environmental Science, Krasnoyarsk, 20–22 июня 2019 года / Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. Vol. 315. – Krasnoyarsk: Institute of Physics and IOP Publishing Limited, 2019. – P. 22105. – DOI 10.1088/1755-1315/315/2/022105. – EDN TOXUBN.

3. Automation of the enterprise financial condition evaluation / A. A. Rukosueva, V. V. Kukartsev, D. V. Eremeev [et al.] // Journal of Physics: Conference Series : International Scientific Conference "Conference on Applied Physics, Information Technologies and Engineering - APITECH-2019", Krasnoyarsk, 25–27 сентября 2019 года / Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations; Polytechnical Institute of Siberian Federal University. Vol. 1399. – Krasnoyarsk: Institute of Physics and IOP

Publishing Limited, 2019. – P. 33102. – DOI 10.1088/1742-6596/1399/3/033102. – EDN ADYYTP.

4. Антамошкин, О. А. Модели и методы формирования надежных структур информационных систем обработки информации / О. А. Антамошкин, В. В. Кукарцев // Информационные технологии и математическое моделирование в экономике, технике, экологии, образовании, педагогике и торговле. – 2014. – № 7. – С. 51-94. – EDN TNAFCP.

5. Mathematical Models for the Design of GRID Systems to Solve Resource-Intensive Problems / V. V. Tynchenko, V. S. Tynchenko, V. A. Nelyub [et al.] // Mathematics. – 2024. – Vol. 12, No. 2. – P. 276. – DOI 10.3390/math12020276. – EDN HPEASV.

6. Development of Adaptive Educational Course in the SibFU E-Learning System / V. V. Kukartsev, E. A. Chzhan, V. S. Tynchenko [et al.] // Journal of Siberian Federal University. Humanities and Social Sciences. – 2018. – Vol. 11, No. 5. – P. 740-752. – DOI 10.17516/1997-1370-0267. – EDN XRFXZZ.

7. Martyushev, N. V. Effect of protective release coatings on the basis of superdispersersed zirconium oxide powder on the formation of gas defects in bronze casting / N. V. Martyushev, N. A. Risto // IOP Conference Series: Materials Science and Engineering : 20, Modern Techniques and Technologies, Tomsk, 14–18 апреля 2014 года. Vol. 66. – Tomsk: Institute of Physics Publishing, 2014. – P. 012013. – DOI 10.1088/1757-899X/66/1/012013. – EDN UFBFBR.

8. The use of titanium alloys for details of downhole hammers / A. I. Popelyukh, A. A. Repin, S. E. Alekseev [et al.] // IOP Conference Series: Materials Science and Engineering, Tomsk, 01–04 декабря 2015 года. Vol. 124. – Tomsk: Institute of Physics Publishing, 2016. – P. 012116. – DOI 10.1088/1757-899X/124/1/012116. – EDN WVWVUN.

9. Martyushev, N. International Conference on Information Technologies in Business and Industry 2016 / N. Martyushev, V. Avramchuk, V. Faerman // Journal of Physics: Conference Series, Tomsk, 21–26 сентября 2016 года. – Bristol: IOPscience, 2017. – P. 011001. – DOI 10.1088/1742-6596/803/1/011001. – EDN XNKBKK.

10. Свидетельство о государственной регистрации программы для ЭВМ № 2020618484 Российская Федерация. Artificial intelligence in the identification of typewritten text : № 2020617284 : заявл. 08.07.2020 : опубл. 29.07.2020 / К. Р. Аветисян, К. Ю. Жигалов, А. Р. Салгириев, Н. В. Мартюшев ; заявитель Федеральное государственное бюджетное учреждение науки Комплексный научно-исследовательский институт им. Х.И. Ибрагимова Российской академии наук. – EDN OLAYTK.