УДК 004.056; 004.8

ИСКУССТВЕННЫЙ ИНТЕЛЕКТ В КИБЕРБЕЗОПАСНОСТИ

Р.А. Кокарев, С.А. Мигалевич

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматривается роль искусственного интеллекта (ИИ) в кибербезопасности, его применения для защиты данных и цифровых инфраструктур. Особое внимание уделено использованию ИИ в обнаружении угроз, автоматизации анализа угроз и фильтрации вредоносного контента. Рассматриваются как преимущества, так и вызовы, связанные с его применением, включая угрозы для алгоритмов машинного обучения и проблемы интерпретируемости решений. Ожидается, что в будущем ИИ будет играть ещё более важную роль в защите от киберугроз благодаря интеграции с новыми технологиями, такими как блокчейн и квантовые вычисления. В статье также освещены перспективы развития методов интерпретируемого машинного обучения, что повысит доверие к решениям ИИ. Заключение подчеркивает, что развитие ИИ поможет создать более безопасную и адаптивную цифровую среду, способную эффективно противостоять изменяющимся киберугрозам.

Ключевые слова: техническая защита информации; кибербезопасность; программные методы защиты; антивирусные системы; искусственный интеллект в безопасности; интернет вещей; блокчейн в защите данных; обнаружение аномалий; поведенческий анализ; интерпретируемое машинное обучение.

ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

R.A. Kokarev, S.A. Migalevich
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article discusses the role of artificial intelligence (AI) in cybersecurity. its applications for data protection and digital infrastructures. Special attention is given to the use of AI in threat detection, automated threat analysis. and malware filtering. Both the advantages and challenges associated with its application are considered. including threats to machine learning algorithms and issues related to the interpretability of decisions. It is expected that in the future, AI will play an even more important role in protecting against cyber threats due to its integration with new technologies such as blockchain and quantum computing. The article also highlights the prospects for the development of interpretable machine learning methods, which will increase trust in AI-driven decisions. The conclusion emphasizes that the development of AI will help create a safer and more adaptive digital environment capable of effectively countering evolving cyber threats.
Keywords: technical information protection; cybersecurity; software protection methods; antivirus systems; artificial intelligence in security; Internet of Things; blockchain in data protection; anomaly detection; behavioral analysis; interpretable machine learning.

Введение

Современные технологии развиваются стремительными темпами, что приводит к росту сложности угроз в сфере кибербезопасности. Кибератаки становятся все более изощренными, а традиционные методы защиты уже не всегда способны эффективно им противостоять. В таких условиях искусственный интеллект (ИИ) играет ключевую роль в обеспечении защиты данных и цифровых инфраструктур. Его способность анализировать огромные объемы информации, выявлять угрозы на ранних стадиях и автоматически реагировать на инциденты делает его незаменимым инструментом в современных системах безопасности [1].

Применение ИИ в кибербезопасности

ИИ используется в различных аспектах защиты информации, помогая как в обнаружении угроз, так и в предотвращении атак. Одним из важных направлений является выявление аномалий в сетевом трафике и системных процессах. Машинное обучение позволяет анализировать большие массивы данных, обнаруживая подозрительные активности, которые могут свидетельствовать о взломе или вредоносной деятельности. Алгоритмы глубинного обучения способны находить ранее неизвестные угрозы, выявляя скрытые закономерности, которые традиционные методы не способны обнаружить [2].

Автоматизированные системы на основе ИИ также активно применяются для предотвращения атак и оперативного реагирования на инциденты. Поведенческий анализ пользователей помогает выявлять попытки несанкционированного доступа, сравнивая текущие действия с привычными моделями поведения. В случае выявления отклонений система может автоматически блокировать потенциально скомпрометированные учетные записи или ограничивать доступ к критически важным ресурсам[1].

Другим важным направлением является автоматизация анализа угроз. Современные интеллектуальные системы способны обрабатывать огромные объемы информации, выявлять новые уязвимости и формировать отчеты для специалистов по кибербезопасности. Это значительно ускоряет процесс расследования инцидентов, позволяя экспертам сосредоточиться на стратегическом планировании и предотвращении сложных атак.

ИИ также активно используется для фильтрации вредоносного контента. Антивирусные программы, основанные на машинном обучении, способны определять новые виды вредоносного программного обеспечения без необходимости предварительного анализа сигнатур. Это позволяет эффективнее защищать пользователей от фишинговых атак, вредоносных вложений в электронных письмах и программ-вымогателей.

Преимущества и вызовы

ИИ обладает рядом преимуществ в области кибербезопасности. Он способен анализировать большие объемы данных в реальном времени, выявляя сложные и скрытые угрозы. Автоматические системы на основе ИИ могут не только обнаруживать атаки, но и самостоятельно реагировать на них, минимизируя возможный ущерб. Кроме того, алгоритмы машинного обучения обладают способностью к адаптации, что позволяет им улучшать свою эффективность по мере накопления новых данных.

Однако существуют и определенные вызовы, связанные с использованием ИИ в кибербезопасности. Одним из главных рисков является возможность атак на сами алгоритмы машинного обучения[3]. Злоумышленники могут использовать методы обмана ИИ, вводя его в заблуждение ложными данными, что приводит к ошибочным выводам. Кроме того, системы искусственного интеллекта требуют значительных вычислительных ресурсов и качественных данных для обучения, что может стать препятствием для их массового внедрения.

Также важно учитывать вопросы прозрачности и интерпретируемости решений, принимаемых ИИ[3]. Многие современные алгоритмы работают как «черные ящики», что затрудняет анализ их логики и принятие корректных решений в критических ситуациях. Поэтому одним из ключевых направлений развития ИИ в кибербезопасности становится создание моделей, которые будут не только эффективными, но и понятными для специалистов.

Перспективы развития

В ближайшие годы ожидается не только дальнейшее совершенствование существующих технологий ИИ в кибербезопасности, но и появление новых подходов, которые существенно повысят эффективность защиты от киберугроз[1]. Ведутся активные исследования в области защиты алгоритмов машинного обучения от атак, направленных на их компрометацию или подделку, что позволит значительно повысить надежность интеллектуальных систем и укрепить их сопротивляемость внешним воздействиям. Это включает в себя разработку методов защиты от атак, таких как «зашумление данных» и «обман целевой модели», а также улучшение устойчивости к моделям атаки, использующих фальсифицированные данные.

Интеграция искусственного интеллекта с передовыми технологиями, такими как блокчейн, квантовые вычисления и Интернет вещей, открывает новые горизонты для повышения уровня защиты данных и снижения вероятности взлома. Блокчейн может стать ключевым элементом в улучшении прозрачности и контроля за действиями, а также в создании неизменяемых записей, что станет дополнительной гарантией безопасности. В свою очередь, квантовые вычисления, несмотря на свою относительно раннюю стадию развития, обещают значительно ускорить процесс обработки и анализа данных для повышения способности к быстрому выявлению угроз.

Одним из важнейших направлений будущего развития станет углубленное изучение и внедрение методов интерпретируемого машинного обучения. Такие методы позволяют глубже анализировать логику принятия решений ИИ, что значительно повышает доверие к его результатам, а также способствует лучшему пониманию работы алгоритмов. Важность этих технологий возрастает в условиях возникновения все более сложных киберугроз, когда необходимо не только обнаружить и предотвратить атаки, но и пояснить причины тех или иных действий ИИ, что позволит экспертам быстрее и точнее реагировать на новые виды угроз.

Заключение

Искусственный интеллект приобретает все более высокую значимость в обеспечении кибербезопасности, помогая оперативно выявлять и предотвращать угрозы. Однако его применение связано с рядом вызовов, включая необходимость защиты самих алгоритмов от атак, высокие вычислительные требования и сложность интерпретации решений. Несмотря на это, развитие интеллектуальных систем безопасности открывает новые возможности для эффективной защиты цифрового пространства. В дальнейшем совершенствование технологий ИИ позволит создать гораздо более безопасную цифровую среду, способную адаптироваться к постоянно меняющимся угрозам и минимизировать риски кибератак.

Список использованных источников

1. Агафонова, О.Б. (2024). Как искусственный интеллект влияет на кибербезопасность. Молодой ученый *(40), 1-3.*

2. Рахматов Д.Р. (2021). Искусственный интеллект и кибербезопасность: возможности и вызовы. Экономика и управление народным хозяйством. *Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, посвященной 65-летию филиала УГНТУ в г. Салавате и Году науки и технологий.*

3. Шананин В.А. (2022). Применение систем искусственного интеллекта в защите информации. *Инновации и инвестиции (11), 201-205.*

References

1. Agafonova, O. B. (2024). How Artificial Intelligence Impacts Cybersecurity. Young Scientist (40). 1-*3.*

2. Rakhmatov, D. R. (2021). Artificial Intelligence and Cybersecurity: Opportunities and Challenges. Economics and Management of the National Economy. Proceedings of the All-Russian Scientific and Technical Conference of Students, Postgraduates, and Young Scientists Dedicated to the 65th Anniversary of the UGNTA Branch in Salavat and the Year of Science and Technology.

3. Shananin, V. A. (2022). Application of Artificial Intelligence Systems in Information Security. Innovations and Investments (11). 201-205.

Сведения об авторах

Кокарев Р.А., студент, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», rmilh1@mail.ru.
Мигалевич С.А., магистр технических наук, начальник центра информатизации и инновационных разработок, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», migalevich@bsuir.by.

Information about the authors

Kokarev R. A., student. Educational Institution "Belarusian State University of Informatics and Radioelectronics", rmilh1@mail.ru.
Migalevich S. A., Master of Technical Sciences, Head of the Center for Informatization and Innovative Developments, Educational Institution "Belarusian State University of Informatics and Radioelectronics", migalevich@bsuir.by.