DOI 10.37882/2223-2966.2024.7.08

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В КОНТЕКСТЕ СОВРЕМЕННЫХ ВЫЗОВОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

THE USE OF ARTIFICIAL INTELLIGENCE IN THE CONTEXT OF MODERN INFORMATION SECURITY CHALLENGES

D. Bondar

Summary. The widespread development and integration of information technologies is a key trend in 2024. Through these solutions, activities in various household and professional spheres of life of a modern person are optimized and automated. However, along with the advantages, the integration of information technologies carries a number of threats and challenges related to information security. At the same time, classical methods of protection lose their effectiveness in front of continuously developing technologies of intruders. Based on this, there is a need to create innovative technological solutions that can effectively prevent illegal actions. The presented article is devoted to a comprehensive analysis of the issue related to the use of intelligent technologies in information security issues. Because of the article, work been done to systematize the most relevant issues of using smart technologies in the context of information security problems. The materials may be of value to modern representatives in the field of information security, revealing and identifying the most significant areas of development on the issue of information security.

Keywords: artificial intelligence, machine learning, information security, data protection, information.

Бондарь Денис Евгеньевич
Ведущий инженер DevOps,
Публичное акционерное общество «МТС-Банк»
expacee@gmail.com

Аннотация. Повсеместное развитие и интеграция информационных технологий является ключевым трендом в 2024 году. Посредством данных решений оптимизируется и автоматизируется деятельность в различных бытовых и профессиональных сферах жизнедеятельности современного человека. Однако вместе с преимуществами интеграция информационных технологий несет ряд угроз и вызовов, связанных с информационной безопасностью. При этом классические методы защиты теряют свою эффективность перед непрерывно развивающимися технологиями злоумышленников. Исходя из этого, складывается необходимость создания инновационных технологических решений, способных эффективному препятствованию неправомерным действиям. Представленная статья посвящена комплексному анализу вопроса, связанного с использованием интеллектуальных технологий в вопросах защиты информации. В результате статьи выполнена работа по систематизации наиболее актуальных вопросов использования умных технологий в контексте проблем информационной безопасности. Материалы могут иметь ценность для современных представителей в сфере информационной безопасности, раскрывая и обозначая наиболее значимые направления развития по вопросу обеспечения информационной безопасности.

Ключевые слова: искусственный интеллект, машинное обучение, информационная безопасность, защита данных, информация.

Введение

В современном мире значительная роль и актуальность принадлежит использованию различных информационных систем (далее — ИС), информационных технологий (далее — ИТ), а также иных цифровых и автоматизированных решений [1]. Именно посредством данных технологических инноваций решаются одни из самых сложных и требующих особого внимания задачи. Основным преимуществом их использования является возможность значительного повышения качества и эффективности выполняемых процессов, что достигается посредством автоматизации рутинных и сложно-вычислительных задач. На начало 2024 практически каждое предприятие проводит активную политику по цифровой трансформации, внедряя на своем производстве передовые информационные технологии. Можно с уверенностью заявить, что интеграция ИТ-решений является неотъемлемой частью функционирования современных предприятий и организаций.

Так, наблюдается перевод бумажных документов в электронную форму, использование различных баз данных, информационных систем, автоматизированных технологий, роботизированных комплексов и иных решений [2]. Основной особенностью использования данных технологий является цифровизация и уменьшение физических носителей информации. В век цифровых технологий значительную актуальность приобретает именно электронный формат данных, что, в сою очередь, значительно повышает риски информационной безопасности (далее — ИБ) предприятий [3]. Так, одной из ключевых проблем на текущий момент времени является обеспечение комплексной системы ИБ, позволяющей предотвратить доступ к информации ограниченного доступа и иных противозаконных действий.

Примерами угроз информационной безопасности, наиболее распространенных на текущий момент времени, является хищение информации, проникновение на объект ограниченного доступа, кража оборудования

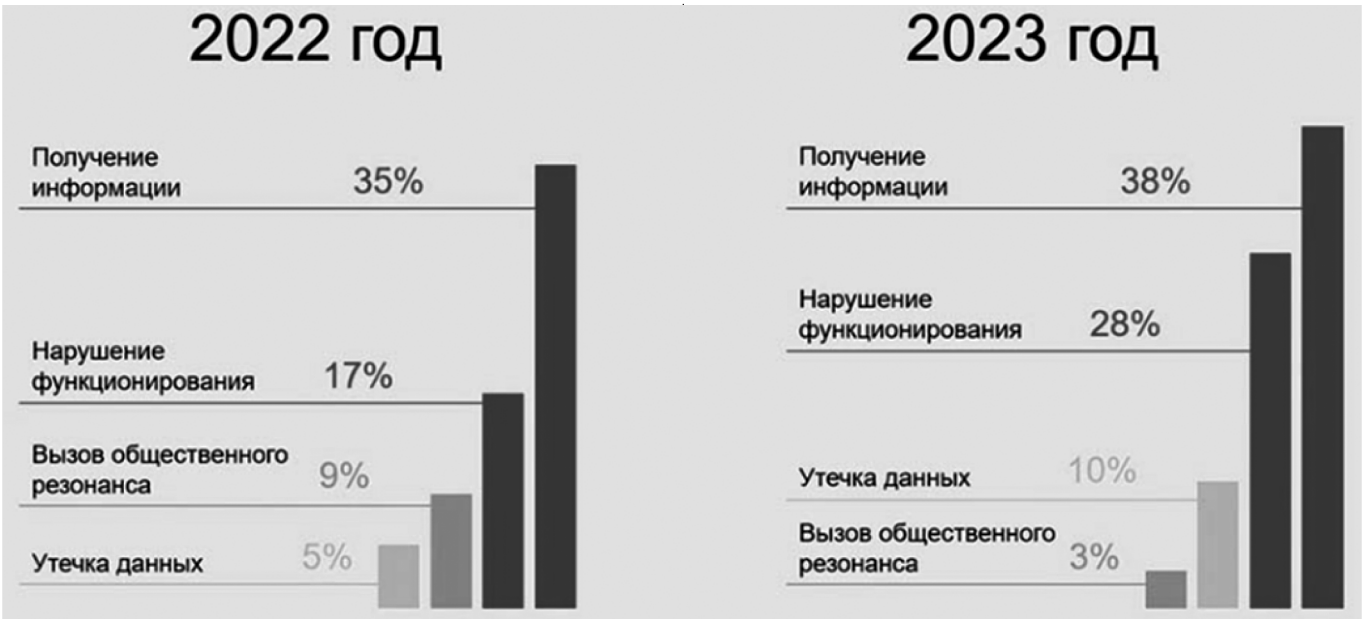

Рис. 1. Распределение целей при реализации угроз ИБ

и иное. Среди основных целей атак по анализу последних лет следует выделить получение информации, нарушение функционирования информационных систем и промышленного оборудования и утечку данных [4]. На рис. 1 представлено распределение наиболее актуальных угроз информационной безопасности за период 2022–2023 годов.

Обеспечение комплексной системы ИБ сталкивается с рядом трудностей, связанных с необходимость анализа большого объема данных в режиме реального времени. Следует отметить, что классические средства на момент 2024 года не соответствуют требованиям, предъявляемым к современным системам ИБ. В связи с этим актуализируется необходимость совершенствования подходов к обеспечению ИБ, в частности, на основе технологий искусственного интеллекта (далее — ИИ). В рамках представленной статьи более подробно рассматриваются значимые вопросы, связанные с обеспечением ИБ на основе интеграции интеллектуальных решений.

Результаты и обсуждение

В 2024 актуализируется развитие и повсеместная интеграция технологий искусственного интеллекта, которые оптимизируют и рационализируют деятельность человека как в бытовых, так и профессиональных сферах. Актуальность подтверждается результатами открытых статистических исследований, которые свидетельствуют о совокупном приросте мирового рынка ИИ-решений на 45 % в период до 2023 года (рис. 2). Особая актуальность применения данных решений относится к вопросу информационной безопасности, который требует возможности обработки большого количества данных в режиме реального времени.

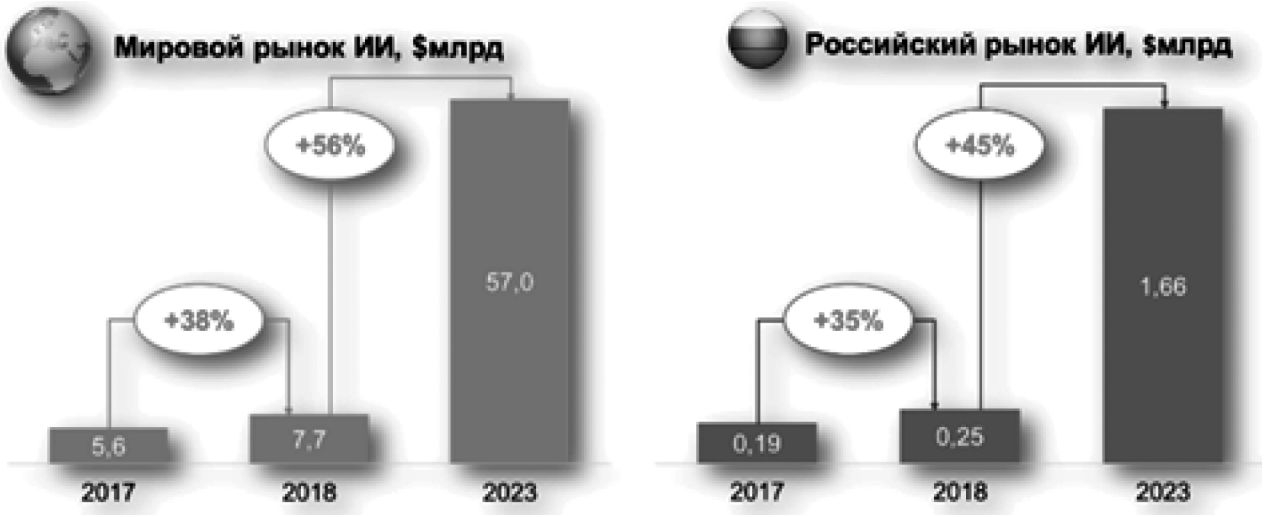

Рис. 2. Динамика роста рынка ИИ 2017–2023 гг.

Технологии искусственного интеллекта представляют собой комплекс методов и алгоритмов, которые позволяют компьютерам симулировать интеллектуальные функции человека [5]. При этом наиболее актуальной сферой, в которой в период 2024 года наблюдается активное развитие интеллектуальных инструментов является информационная безопасность. С ростом объема данных и сложности киберугроз возникает потребность в эффективных инструментах для обнаружения, предотвращения и реагирования на потенциальные угрозы. Технологии ИИ предоставляют возможности для создания автоматизированных систем мониторинга и защиты, способных адаптироваться к постоянно меняющейся среде угроз.

Одним из ключевых преимуществ использования ИИ в ИБ является способность анализировать большие объемы данных в реальном времени, а также выявлять аномалии или подозрительное поведение, которое может свидетельствовать о наличии угрозы [6]. Модели машинного обучения и алгоритмы глубокого обучения позволяют создавать системы, способные обнаруживать новые, ранее неизвестные угрозы, а также адаптироваться к изменяющимся методам атак. Более того, технологии ИИ могут повысить эффективность работы аналитиков информационной безопасности, предоставляя инструменты для автоматизации детектирования угроз, принятия оперативных мер противодействия и ряда других задач [7]. Это позволяет сократить время, необходимое для обнаружения и реагирования на угрозы, что в свою очередь уменьшает риск нанесения ущерба бизнесу и организациям. В табл. 1 представлены результаты анализа наиболее распространенных технологий ИИ на текущий момент времени, используемые при решении отдельных задач ИБ. Важно отметить, что при использовании комплекса из данных технологий предприятие сможет обеспечить высокий уровень информационной безопасности, сводя к минимуму потенциальные риски и угрозы ИБ. В связи с этим, в 2024 году также наблюдается рост рынка ИИ-решений, используемых в системах и информационной безопасности.

Как видно из табл. 1, технологии ИИ играют ключевую роль в решении этих задач, обеспечивая более точное и быстрое обнаружение угроз, автоматизацию процессов безопасности и улучшение общей защиты ИС.

Необходимо отметить, что использование искусственного интеллекта в вызовах ИБ на момент 2024 года играет ключевую роль в обеспечении защиты от разнообразных угроз. Одним из основных вызовов является увеличение объема и сложности данных, что требует более эффективных методов обнаружения и анализа угроз. ИИ позволяет автоматизировать этот процесс и обрабатывать большие массивы данных быстрее и точнее, чем традиционные методы [8]. Примеры использования ИИ в сфере информационной безопасности включают анализ сетевого трафика с использованием алгоритмов машинного обучения для выявления аномалий, которые могут указывать на атаки или несанкционированный доступ. Другой вызов — это необходимость более точной и быстрой реакции на инциденты [9]. Использование искусственного интеллекта позволяет создавать системы автоматизированного реагирования, способные оперативно анализировать и классифицировать инциденты без участия человека, что существенно сокращает время реакции и минимизирует ущерб от атак. В табл. 2 представлены результаты анализа наиболее значимых преимуществ использования ИИ в контексте рассматриваемого вопроса.

Таблица 1.

Применение ИИ в задачах ИБ

№	Задача	Инструменты ИИ
1	Обнаружение угроз и аномалий	Использование алгоритмов машинного обучения для анализа сетевого трафика и выявления аномального поведения, указывающего на возможные атаки. Применение методов обучения без учителя для выявления необычных паттернов в данных, которые могут свидетельствовать о наличии угрозы без необходимости предварительной разметки данных
2	Автоматизированное реагирование на инциденты	Создание систем автоматизированного реагирования с помощью алгоритмов машинного обучения, которые могут быстро анализировать и классифицировать инциденты без участия человека. Разработка ботов и роботов для выполнения задач по смягчению последствий инцидентов, например, для автоматической блокировки доступа или восстановления систем
3	Идентификация и аутентификация	Применение биометрических методов, таких как распознавание лиц или голоса, с использованием алгоритмов глубокого обучения для идентификации пользователей. Использование алгоритмов ИИ для анализа поведения пользователей и выявления подозрительных действий, связанных с несанкционированным доступом
4	Мониторинг и анализ уязвимостей	Применение алгоритмов машинного обучения для анализа и классификации уязвимостей в программном обеспечении или сетевых устройствах. Разработка систем, способных автоматически обнаруживать и анализировать новые уязвимости на основе данных о предыдущих атаках и обновлениях ПО

Таблица 2.

Преимущества ИИ в обеспечении ИБ

№	Преимущество	Значение
1	Автоматизация	ИИ позволяет автоматизировать процессы обнаружения угроз и оперативного принятия соответствующих мер по противодействию
2	Обнаружение аномалий	Интеллектуальные алгоритмы предоставляют возможность анализа большого объема данных в режиме реального времени и выделяя собственные шаблоны для ускорения времени на реакцию
3	Эффективный анализ данных	Использование ИИ позволяет проводить более глубокий и точный анализ больших массивов данных, что помогает выявлять скрытые угрозы и тренды, не обнаружимые традиционными методами
4	Быстрая реакция на инциденты ИБ	ИИ позволяет создавать системы моментального реагирования на инциденты, что сокращает время реакции на угрозы и минимизирует ущерб от атак
5	Эффективная защита от атак	Использование ИИ позволяет более эффективно обнаруживать и предотвращать атаки, включая новые и продвинутые виды угроз, что повышает общий уровень безопасности информационных систем

Как видно, использование ИИ в системах ИБ предоставляет современным предприятиям ряд технических и экономических преимуществ. Использование ИИ-решений позволяет предприятиям быстрее и эффективнее обнаруживать и реагировать на инциденты ИБ, сводя к минимуму риск ущерба и потерь данных [10]. Благодаря использованию ИИ, системы информационной безопасности становятся более адаптивными. Алгоритмы машинного обучения и нейронные сети позволяют создавать системы, способные самостоятельно обучаться на основе новых данных и опыта, что повышает их эффективность и точность обнаружения угроз.

Экономические преимущества использования ИИ в системах ИБ также имеют высокое значение. Внедрение ИИ позволяет сократить человеческие ресурсы, необходимые для мониторинга и обнаружения угроз, что снижает операционные расходы предприятия. Кроме того, быстрая реакция на угрозы и предотвращение инцидентов позволяют исключить потенциальные потери от реализации атак. Ввиду этого следует утверждать, что использование современных ИИ-решений в системах информационной безопасности на момент 2024 года обеспечивает предприятия надежной защитой от угроз, а также повышает их операционную и экономическую эффективность.

Заключение

В рамках представленной статьи были более подробно освещены текущие тенденции относительно использования интеллектуальных средств в задачах по обеспечению ИБ. В рамках работы показано, что ИИ в системах ИБ представляет значимый шаг в развитии современных предприятий и организаций. Проведенный анализ также выявил, что использование ИИ в ИБ обеспечивает ряд значительных преимуществ при реагировании на угрозы, а также позволяет повысить экономическую эффективность предприятий на основе автоматизации рутинных действий. Использование ИИ-решений в системе ИБ становится все более востребованным на момент 2024 года среди предприятий, стремящихся обеспечить надежную защиту своих данных и репутации. Продолжающееся развитие технологий ИИ позволит создавать еще более эффективные и инновационные системы ИБ, способные противостоять все более сложным угрозам. Материалы работы могут быть полезны для актуализации необходимости интеграции интеллектуальных решений в системе ИБ предприятия, а также непосредственно при выборе средств и технологий в задачах по обеспечению информационной безопасности.

ЛИТЕРАТУРА

1. Самолкаева А.М., Шведова С.М. Искусственный интеллект в сфере информационной безопасности: преимущества, ограничения и перспективы // Вестник науки. 2024. №3 (72). С. 534–539.
2. Хакимов А.А. Роль искусственного интеллекта в кибербезопасности // Universum: технические науки. 2023. №11-1 (116). С. 58–59.
3. Hourani H., Hammad A., Lafi M. The Impact of Artificial Intelligence on Software Testing // IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT). 2019. pp. 565–570.
4. Афанасьева Д.В. Применение искусственного интеллекта в обеспечении безопасности данных // Известия ТулГУ. Технические науки. 2020. №2. С. 151–154.
5. Ангапов В.Д., Бобров А.В., Тимонин В.А., Вишняков А.С. Использование технологий машинного обучения в защите информационных систем // Наука, техника и образование. 2023. №4 (92). С. 20–26.
6. Козлова Н.Ш., Довгаль В.А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. 2023. №3 (326). С. 65–72.
7. Бевзенко С.А. Применение искусственного интеллекта и машинного обучения в разработке программного обеспечения // Инновации и инвестиции. 2023. №8. С. 187–191.
8. Singhal P., Kundu S., Gupta H., Jain H. Application of Artificial Intelligence in Software Testing // 10th International Conference on System Modeling & Advancement in Research Trends (SMART), MORADABAD. 2021. pp. 489–492.
9. Иламанов Б.Б. Интеграция искусственного интеллекта в разработке программного обеспечения // Вестник науки. 2023. №12 (69). С. 1207–1211.
10. Xiaomei S., Lijin W., Kuangyu J., Xinyu H., Longli T. Research on Trustworthiness Analysis Technology of Artificial Intelligence Software // IEEE International Conference on Control, Electronics and Computer Technology (ICCECT). 2023. pp. 802–806.