УДК 004.896

Н.А. Горбунова, А.А. Жамантаев
Карагандинский университет им. Е.А. Букетова
Караганда, Казахстан

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СФЕРЕ КОРПОРАТИВНОЙ КИБЕРБЕЗОПАСНОСТИ

***Аннотация**. В статье рассматривается тема кибербезопасности с упором на кибербезопасность в корпоративной среде. Перечисляются возможные меры противодействия угрозам, утечкам информации. Рассказывается об искусственном интеллекте и его применении в сфере кибербезопасности. Приводятся некоторые решения в сфере кибербезопасности на основе искусственного интеллекта.*

N.A. Gorbunova, A.A. Zhamantayev
Karaganda Buketov University
Karaganda, Kazakhstan

ARTIFICIAL INTELLIGENCE IN CORPORATE CYBERSECURITY

***Abstract**. The article examines the topic of cybersecurity with a focus on cybersecurity in the corporate environment. Possible measures to counter threats and information leaks are listed. It talks about artificial intelligence and its application in the field of cybersecurity. Some solutions in the field of cybersecurity based on artificial intelligence are presented.*

Современные организации сталкиваются с разнообразными и сложными угрозами в киберпространстве. Киберпреступники активно осуществляют атаки, направленные на кражу данных, вымогательство, внедрение в системы и кибершпионаж. Этот разнообразный спектр угроз требует разработки комплексных стратегий по кибербезопасности.

Информация становится ключевым ресурсом, и защита конфиденциальных данных, бизнес-планов и другой чувствительной информации становится первостепенной задачей. Потеря или утечка данных может повлечь за собой серьезные финансовые и репутационные последствия.

Организации активно внедряют технологические решения для обеспечения кибербезопасности. Современные антивирусные программы, брандмауэры, системы обнаружения вторжений и шифрование данных становятся стандартом. Использование

технологий искусственного интеллекта и машинного обучения дополняет эти меры, позволяя выявлять аномалии в сетевом трафике.

Человеческий фактор остается одним из слабых мест в системах безопасности. Обучение сотрудников основам кибербезопасности, включая распознавание фишинга, использование надежных паролей и осведомленность о социальной инженерии, становится неотъемлемой частью стратегии.

Однако кибербезопасность — это не только вопрос технологий и обучения. Важно внедрение стратегий управления рисками, регулярные аудиты безопасности, мониторинг сетевой активности и готовность к быстрому реагированию на инциденты. Системы резервного копирования данных и планы восстановления после инцидентов становятся неотъемлемой частью общей стратегии безопасности.

С учетом постоянно меняющейся киберугрозы, организации должны быть готовы к новым угрозам. Это включает в себя угрозы в области интернета вещей (IoT), использование искусственного интеллекта для кибератак и развитие квантовых вычислений, которые могут подорвать существующие методы шифрования.

Кроме того, сотрудничество в сфере кибербезопасности становится все более важным. Организации должны активно сотрудничать с другими компаниями, правительственными органами и кибербезопасностными сообществами для обмена информацией о новых угрозах и разработки совместных стратегий защиты.

В условиях быстрого развития киберугрозы организации должны подходить к кибербезопасности комплексно, объединяя технологии, обучение персонала и готовность к сотрудничеству в глобальном масштабе. Только так можно обеспечить эффективную защиту от современных киберугроз.

Искусственный интеллект (ИИ) представляет собой область информатики, занимающуюся созданием систем, способных выполнять задачи, обычно требующие человеческого интеллекта. Эти системы стремятся имитировать различные аспекты человеческого мышления, такие как обучение, распознавание образов, планирование и принятие решений. В основе многих технологий искусственного интеллекта лежит использование алгоритмов машинного обучения, глубокого обучения и нейронных сетей.

Цель искусственного интеллекта включает в себя создание систем, способных решать задачи более эффективно, чем традиционные программы, и обеспечивать автоматизацию ряда задач, которые ранее требовали человеческого вмешательства. Эта область

имеет широкое применение, включая медицину, финансы, образование, транспорт, производство и многие другие сферы жизни.

В последние десятилетия искусственный интеллект стал непреодолимой силой, трансформирующей многие области человеческой деятельности. Одной из наиболее актуальных и важных сфер, где его влияние проявляется наиболее сильно, является кибербезопасность. В мире, где цифровые технологии становятся неотъемлемой частью нашей повседневной жизни, возрастает необходимость в эффективных средствах защиты от киберугроз.

Искусственный интеллект в кибербезопасности представляет собой мощный инструмент, способный анализировать огромные объемы данных, выявлять аномалии, обнаруживать угрозы и реагировать на них в режиме реального времени.

Искусственный интеллект в кибербезопасности является ключевым элементом защиты в современном цифровом мире, где кибератаки становятся более сложными и изощренными. Методы обнаружения вторжений, основанные на технологиях искусственного интеллекта, позволяют выявлять аномальные активности и потенциальные угрозы, даже если они не соответствуют заранее определенным шаблонам. Это существенно повышает эффективность систем безопасности, обеспечивая более раннее и точное выявление инцидентов.

Прогнозирование угроз также становится более точным благодаря алгоритмам машинного обучения, способным анализировать большие объемы данных и выявлять скрытые закономерности. Это позволяет создавать предупреждения о потенциальных киберугрозах и принимать меры до их активации, что является важным элементом в сфере предотвращения кибератак.

Однако, с ростом возможностей искусственного интеллекта в кибербезопасности, также возникают новые вызовы. Злоумышленники могут пытаться обходить системы, обученные на основе искусственного интеллекта, используя ухищрения и атаки, направленные на обман алгоритмов. Поэтому важно постоянно совершенствовать методы обнаружения и адаптировать системы к новым видам угроз.

К примеру, Darktrace, компания, основанная в Великобритании, предоставляет решение, направленное на защиту корпоративных сетей от кибератак. Это решение основывается на методах машинного обучения, анализируя все устройства в сети и их поведение на предмет безопасности. Этот продукт может обнаруживать потенциальные угрозы безопасности в реальном времени и использует технологии

автономного реагирования для принятия мер против кибератак. Darktrace визуализирует информацию в удобном виде. Существуют и другие решения от других компаний, такие как Vectra AI, CrowdStrike и другие, которые работают по схожему принципу.

В заключение, использование искусственного интеллекта в кибербезопасности представляет собой важную часть стратегии обеспечения цифровой безопасности. Это не только улучшает способность выявления и предотвращения киберугроз, но также дает возможность строить более гибкие и адаптивные системы, способные эффективно реагировать на постоянно меняющийся характер кибератак. Развитие и интеграция искусственного интеллекта в сферу кибербезопасности становится ключевым фактором в обеспечении безопасности в цифровой эпохе.

Список использованных источников

1. Базы знаний интеллектуальных систем / Т.А. Гаврилова, В.Ф. Хорошевский –СПб.: Питер, 2000. –384 с.

2. Основы информационной безопасности. Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. -М.: Горячая линия – Телеком, 2006. 544 с.

УДК 004.896

N.A. Gorbunova, A.G. Podlesny
Karaganda Buketov University
Karaganda, Kazakhstan

THE ROLE OF AI AND DEEP LEARNING IN DIGITIZING HEALTHCARE

Abstract. *The article discusses the benefits of artificial intelligence and deep learning in healthcare. Artificial intelligence (AI) and deep learning (DL) are changing healthcare in unprecedented ways, marking a pivotal shift in medical science. Their integration opens up new opportunities for innovation in the field of digitalization of healthcare.*

Н.А. Горбунова, А.Г. Подлесный
Карагандинский университет им. Е.А. Букетова
Караганда, Казахстан