ВЛИЯНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА НА ЭКОНОМИЧЕСКУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЙ

А.В.Рашидов *–*

Каршинский Международный Университет

E-mail: azizvohidovich@gmail.com

Аннотация: *В статье рассматривается влияние технологий искусственного интеллекта (ИИ) на экономическую безопасность предприятий. Автор анализирует как позитивные эффекты цифровизации, включая автоматизацию процессов и повышение эффективности управления, так и потенциальные угрозы, связанные с киберрисками, технологической зависимостью и социальной нестабильностью. На основе проведенного анализа предложены меры по обеспечению устойчивости бизнеса при внедрении ИИ-технологий.*

Ключевые слова: *искусственный интеллект, экономическая безопасность, цифровизация, риски, автоматизация, предприятие.*

THE IMPACT OF ARTIFICIAL INTELLIGENCE ON THE ECONOMIC SECURITY OF ENTERPRISES

This article examines the impact of artificial intelligence (AI) technologies on the economic security of modern enterprises. The paper highlights both the positive effects of AI implementation — including process automation, cost reduction, and improved cybersecurity — and the emerging risks associated with data breaches, technological dependence, and labor market disruptions. The dual role of AI as a tool for both increasing operational efficiency and generating new threats is emphasized. Based on the conducted analysis, the author proposes a set of measures to ensure enterprise resilience and economic security in the context of digital transformation.

Keywords: *Artificial Intelligence, Economic Security, Digital Transformation, Cybersecurity, Data Protection, Automation, Risk Management, Enterprise Resilience, Labor Market, Technological Dependence.*

Современная цифровизация экономики сопровождается стремительным развитием технологий искусственного интеллекта (ИИ), которые всё чаще внедряются в производственные и управленческие процессы предприятий. Наряду с очевидными преимуществами, связанными с повышением эффективности, ИИ-технологии формируют и новые вызовы, особенно в сфере экономической безопасности бизнеса. Учитывая, что экономическая безопасность представляет собой устойчивое состояние защищённости организации от внешних и внутренних угроз, важно определить, в какой степени внедрение ИИ способствует её укреплению либо ослаблению.

Целью данной статьи является исследование влияния искусственного интеллекта на экономическую безопасность предприятий, выявление рисков и угроз, а также формирование рекомендаций по их минимизации.

1. Позитивное влияние ИИ на экономическую безопасность

Одним из ключевых направлений воздействия искусственного интеллекта на экономическую безопасность предприятий является автоматизация бизнес-процессов, которая напрямую способствует снижению операционных издержек. Современные ИИ-системы позволяют частично или полностью заменить человеческий труд в рутинных, повторяющихся операциях, таких как обработка заказов, документооборот, бухгалтерский учет, клиентская поддержка и управление запасами.

Внедрение автоматизированных интеллектуальных алгоритмов приводит к следующим экономическим эффектам:

Сокращение затрат на оплату труда. За счёт сокращения численности персонала, занятого на вспомогательных и стандартных операциях, снижается фонд заработной платы.

Уменьшение времени выполнения операций. Автоматизация позволяет существенно сократить временные издержки на выполнение внутренних процессов, что повышает общую производительность предприятия.

Снижение количества ошибок. Исключение человеческого фактора в рутинных задачах уменьшает вероятность ошибок, связанных с невнимательностью или недостаточной квалификацией персонала.

Оптимизация ресурсопользования. Системы на базе ИИ способны динамически адаптироваться к изменяющимся условиям, обеспечивая более рациональное распределение материальных, трудовых и временных ресурсов.

Примером может служить использование ИИ в логистике, где алгоритмы на основе машинного обучения позволяют в режиме реального времени оптимизировать маршруты доставки, сокращая затраты на топливо и повышая точность исполнения заказов. В производственной сфере интеллектуальные системы управления технологическими процессами позволяют минимизировать потери сырья, оптимизировать графики выпуска продукции и сократить простои оборудования.

В условиях цифровизации и интеграции искусственного интеллекта в корпоративную инфраструктуру резко возрастает актуальность вопросов кибербезопасности. Надёжная защита информационных систем является важнейшим компонентом экономической безопасности предприятия, поскольку утечка данных, хищение интеллектуальной собственности или парализация ИТ-систем могут привести к значительным финансовым потерям и подрыву деловой репутации.

Искусственный интеллект способен не только порождать новые угрозы, но и выступать в качестве эффективного инструмента обеспечения кибербезопасности. В частности, ИИ-технологии находят применение в следующих направлениях:

Интеллектуальный мониторинг активности. Системы на базе машинного обучения способны анализировать поведенческие паттерны пользователей и в реальном времени выявлять аномалии, характерные для несанкционированного доступа, фишинга или внутренних злоупотреблений.

Прогнозирование и предотвращение атак. Предиктивная аналитика, основанная на данных о прошлых инцидентах, позволяет формировать проактивные стратегии защиты, включая автоматическое обновление политик доступа, блокировку вредоносной активности и изоляцию скомпрометированных участков сети.

Управление уязвимостями. ИИ может использоваться для автоматического поиска уязвимостей в программном обеспечении и инфраструктуре, сокращая временной лаг между выявлением проблемы и её устранением.

Классификация и фильтрация угроз. Современные антивирусные и антифрод-системы, построенные на ИИ, демонстрируют высокую точность в идентификации сложных многоэтапных атак, включая нулевые угрозы (zero-day exploits), которые не распознаются традиционными методами.

Развитие искусственного интеллекта и его активное внедрение в корпоративную ИТ-инфраструктуру сопровождается не только возможностями повышения эффективности, но и существенным ростом киберугроз. Одной из наиболее чувствительных областей, подверженных влиянию цифровых рисков, является информационная безопасность, в частности — защита от несанкционированного доступа и утечек конфиденциальных данных.

В современных условиях предприятия обрабатывают и хранят огромные объемы данных: персональные сведения клиентов и сотрудников, коммерческую тайну, финансовую отчетность, производственные алгоритмы. Любая компрометация этих данных может привести к:

прямым финансовым потерям (штрафы, компенсации, простои бизнеса);

репутационным издержкам;

потере конкурентных преимуществ;

юридическим последствиям, особенно в условиях действия законов о защите персональных данных (например, GDPR, ФЗ-152 и др.).

С развитием ИИ появляются новые формы киберугроз:

Атаки на обучающие данные (data poisoning). Злоумышленники могут внедрять искаженные данные в обучающую выборку, тем самым влияя на поведение модели ИИ и вызывая системные сбои.

Атаки на модель (model inversion, adversarial attacks). Воздействие на входные данные с целью заставить ИИ принять ошибочные решения или получить доступ к исходным данным модели.

Использование ИИ самими злоумышленниками. Генерация фишинговых писем, подбор паролей, автоматизация атак происходит с помощью тех же технологий ИИ, что используются и в легальных целях.

Особую опасность представляют **утечки данных через облачные сервисы** и **интеграции с внешними ИИ-платформами**, когда чувствительная информация передается на сторонние серверы. При недостаточном контроле или отсутствии шифрования данные могут быть перехвачены, что особенно критично для компаний, работающих в сфере финансов, телекоммуникаций, здравоохранения и государственного управления.

Согласно исследованию компании IBM (2023), средняя стоимость одной утечки данных для организации составляет более 4,5 млн долларов США, а

самыми дорогостоящими являются инциденты, связанные с использованием искусственного интеллекта в критических бизнес-процессах.

Внедрение технологий искусственного интеллекта в экономику оказывает не только технологическое и управленческое, но и значительное социальное влияние. Наиболее острая проблема связана с трансформацией рынка труда и возникновением социально-экономического неравенства. Автоматизация, стимулируемая ИИ, приводит к структурным изменениям в системе занятости, что имеет далеко идущие последствия для экономической стабильности предприятий и общества в целом.

Снижение спроса на низкоквалифицированный труд

Наиболее уязвимой категорией работников в условиях цифровизации становятся специалисты, выполняющие стандартные, повторяющиеся функции — кассиры, операторы call-центров, водители, сотрудники службы поддержки и др. ИИ-системы, способные выполнять эти функции быстрее и дешевле, вытесняют человека из этих сегментов. Это способствует росту безработицы в уязвимых группах населения и требует от государства и бизнеса принятия компенсаторных мер.

Рост требований к квалификации

Одновременно наблюдается увеличение спроса на высококвалифицированных специалистов в области анализа данных, разработки алгоритмов, кибербезопасности, управления цифровыми системами. Это порождает **структурное расслоение** на рынке труда и усиливает профессиональное и образовательное неравенство. Предприятиям становится сложнее находить кадры, соответствующие новым требованиям, что может тормозить процессы цифровой трансформации.

Социальная напряжённость

Массовое внедрение ИИ без должной социальной адаптации способно вызвать рост социальной напряжённости, снижение доверия к

технологическим преобразованиям, протестные настроения. Особенно это актуально в регионах с высоким уровнем зависимости от моноотраслей и невысокой цифровой культурой.

Увеличение расходов на обучение и адаптацию

Для устойчивого внедрения ИИ в производственные процессы предприятиям приходится нести дополнительные затраты на обучение персонала, переподготовку, внедрение программ социальной адаптации и развитие корпоративной культуры. Это становится необходимым условием сохранения лояльности работников и предотвращения кадрового дефицита.

Таким образом, социально-экономические последствия внедрения ИИ выходят за рамки технологической трансформации и затрагивают ключевые аспекты устойчивости экономики. Пренебрежение этими аспектами может нивелировать положительный эффект от цифровизации и создать новые риски для экономической безопасности предприятий. Поэтому требуется интеграция социальной политики и кадровой стратегии в контекст цифровых преобразований.

Анализ влияния технологий искусственного интеллекта на экономическую безопасность предприятий показывает, что ИИ обладает двойственной природой: с одной стороны, он существенно расширяет возможности бизнеса по оптимизации процессов, снижению затрат и повышению конкурентоспособности, с другой — порождает новые вызовы, связанные с киберрисками, утечкой данных, социальной нестабильностью и технологической зависимостью.

Внедрение ИИ способствует автоматизации и цифровизации ключевых бизнес-функций, повышает качество аналитики, ускоряет принятие решений и обеспечивает дополнительный уровень защиты информационных систем. Вместе с тем, формируются и новые уязвимости, особенно в контексте взаимодействия с внешними платформами, дефицита квалифицированных

кадров и недостаточной регламентации использования алгоритмов в корпоративной среде.

Для минимизации негативных последствий и укрепления экономической безопасности в условиях цифровой трансформации необходимо формировать комплексный подход, включающий:

разработку стратегий цифровой устойчивости;

организацию внутреннего контроля за ИИ-моделями;

инвестиции в обучение персонала;

выбор защищённых и прозрачных ИИ-решений;

интеграцию этических и правовых норм в процесс внедрения технологий.

Таким образом, экономическая безопасность предприятий в эпоху искусственного интеллекта требует баланса между инновациями и контролем, гибкости в управлении и стратегической готовности к новым формам цифровых угроз. Только при условии системного и осознанного подхода ИИ может стать не угрозой, а гарантом устойчивого и безопасного развития бизнеса в долгосрочной перспективе.

Список литературы

1. Ковалева Т.В. Экономическая безопасность предприятия: системный подход. — М.: Инфра-М, 2022. — 288 с.

2. Назаров Д.Ю. Цифровизация бизнеса и управление рисками. — СПб.: Питер, 2021. — 304 с.

3. Губанова Е.А. Информационная безопасность в условиях цифровизации экономики // Экономика и предпринимательство. — 2023. — № 2 (147). — С. 97–102.

4. Афанасьев М.П., Селиванов А.В. Искусственный интеллект и управление организацией: возможности и угрозы // Менеджмент в России и за рубежом. — 2022. — № 6. — С. 14–20.

5. Филиппов А.Ю. Цифровая трансформация и структурные изменения рынка труда // Вестник РАН. — 2021. — Т. 91, № 8. — С. 789–796.

6. Петрова Н.А. Риски и уязвимости ИИ-систем в корпоративной среде // Информационная безопасность. — 2022. — № 4. — С. 33–39.

7. OECD. Artificial Intelligence in Society. — Paris: OECD Publishing, 2019. — 144 p. DOI: 10.1787/eedfee77-en.