МЕХАНИЗМЫ АДАПТАЦИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ К ВЫЗОВАМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Ассистент преподаватель А.В.Рашидов –Каршинский Международный Университет

Аннотация

В статье рассматривается влияние технологий искусственного интеллекта на экономическую безопасность предприятий. Проанализированы ключевые направления воздействия ИИ — автоматизация процессов, обеспечение кибербезопасности, снижение затрат, а также выявлены риски: утечка данных, технологическая зависимость и трансформация рынка труда. Отмечена двойственная природа ИИ как источника инновационного роста и потенциальных угроз. На основе анализа предложены механизмы обеспечения устойчивости бизнеса в условиях цифровой трансформации, включая стратегическое планирование, регламентацию, подготовку персонала и технические меры защиты.

Ключевые слова: искусственный интеллект, экономическая безопасность, цифровая трансформация, киберугрозы, автоматизация, управление рисками, рынок труда, устойчивость бизнеса.

The Impact of Artificial Intelligence on the Economic Security of Enterprises

Assistant teacher A.V.Rashidov – Karshi International University

The article examines the impact of artificial intelligence (AI) technologies on the economic security of enterprises. The author analyzes key areas of AI influence — process automation, cybersecurity, and cost reduction — as well as associated risks such as data breaches, technological dependence, and labor market transformation. The dual nature of AI as both a driver of innovation and a source of emerging threats is emphasized. Based on the analysis, the paper proposes mechanisms for ensuring enterprise resilience in the context of digital

transformation, including strategic planning, regulatory frameworks, workforce development, and technical protection measures.

Keywords: artificial intelligence, economic security, digital transformation, cybersecurity threats, automation, risk management, labor market, business resilience.

В условиях стремительного внедрения технологий искусственного интеллекта стратегическое планирование цифровой трансформации становится ключевым элементом обеспечения экономической безопасности предприятия. Без четко сформулированной стратегии цифровизации, интеграция ИИ может привести не только к неэффективным инвестициям, но и к росту уязвимостей в информационно-технологической среде организации.

Цифровая трансформация, ориентированная на использование ИИ, должна начинаться с оценки текущего состояния предприятия в трех измерениях:

- технологическая готовность (ИТ-инфраструктура, уровень автоматизации);
- организационная зрелость (наличие цифровых компетенций, процессов управления проектами);
- рисковый профиль (угрозы кибербезопасности, юридические риски, зависимость от внешних поставщиков технологий).

На основе такой оценки формируется стратегический план цифрового развития, который включает:

- определение приоритетных направлений внедрения ИИ (например, автоматизация бухгалтерии, интеллектуальная логистика, предиктивное обслуживание оборудования);
- поэтапную дорожную карту (roadmap) цифровых инициатив;
- бюджетирование цифровых проектов и определение источников финансирования;
- назначение ответственных лиц и формирование проектных команд;

- систему показателей эффективности (KPI) цифровой трансформации.

Особое внимание в стратегическом планировании должно уделяться интеграции ИИ в систему управления рисками. Это означает включение в стратегию:

- механизмов оценки потенциальных угроз, связанных с применением ИИ (например, утечка данных, этические риски);
- разработки сценариев реагирования на критические сбои (incident response);
- адаптации корпоративной политики безопасности под новые технологии.

Эффективное стратегическое планирование позволяет не только повысить отдачу от внедрения ИИ, но и встроить его использование в общую систему обеспечения устойчивости бизнеса. Оно снижает вероятность необоснованных решений, минимизирует издержки и способствует формированию цифровой культуры на всех уровнях управления.

Технологические меры играют ключевую роль в системе обеспечения экономической безопасности предприятий, использующих решения на основе искусственного интеллекта. Рост объёмов обрабатываемых данных, широкое распространение облачных вычислений и интеграция ИИ-алгоритмов в критически важные бизнес-процессы требуют соответствующих инструментов защиты, способных предотвратить технологические и киберугрозы.

Среди основных направлений технологической защиты в условиях цифровой трансформации можно выделить следующие:

1. Защита данных и информационных потоков

Применение шифрования при передаче и хранении данных (в том числе end-to-end encryption);

Использование систем предотвращения потерь данных (DLP), отслеживающих перемещение чувствительной информации;

Внедрение межсетевых экранов нового поколения (NGFW) и систем обнаружения вторжений (IDS/IPS), обученных на основе ИИ.

2. Контроль и аудит ИИ-моделей

Регулярная валидация и верификация ИИ-алгоритмов, с целью выявления ошибок, смещений (bias) и потенциально опасных решений;

Внедрение прозрачных и интерпретируемых моделей (explainable AI), особенно при принятии решений, затрагивающих экономические или правовые интересы;

Хранение журналов событий и автоматическое логирование решений, принимаемых ИИ, для обеспечения их воспроизводимости и анализа в случае инцидентов.

3. Обеспечение устойчивости цифровой инфраструктуры

Использование резервных и отказоустойчивых ИТ-архитектур (например, кластеризация, контейнеризация, мультиоблачные среды);

Применение технологий предиктивного мониторинга и диагностики оборудования с помощью ИИ;

Построение сегментированной сети с разграничением доступа, минимизацией привилегий и контролем взаимодействия между подсистемами.

4. Информационная изоляция ИИ-решений

Для особенно чувствительных задач рекомендуется локализация ИИ-моделей на внутренней инфраструктуре предприятия, без подключения к внешним API и платформам, что исключает утечку данных и нежелательные зависимости.

5. Тестирование на устойчивость к атакам

Проведение adversarial testing (тестирование на устойчивость к враждебным воздействиям);

Использование инструментов симуляции атак (red teaming, penetration testing), адаптированных под ИИ-среды;

Разработка защитных механизмов от отравления данных (data poisoning) и подмены входных параметров.

В условиях активной цифровизации и внедрения технологий искусственного интеллекта ключевым фактором обеспечения экономической безопасности предприятия становится развитие человеческого капитала. Технологии ИИ не заменяют человека полностью, но радикально изменяют структуру трудовых ресурсов, характер выполняемых задач и требования к профессиональным компетенциям. В этой связи формирование кадровой стратегии, ориентированной на развитие цифровых навыков, становится неотъемлемой частью устойчивой трансформации бизнеса.

1. Формирование цифровых компетенций персонала

Переход к работе с ИИ-системами требует от сотрудников навыков анализа данных, взаимодействия с цифровыми платформами, понимания принципов функционирования ИИ-алгоритмов. В рамках повышения квалификации и корпоративного обучения необходимо:

- реализовать программы цифровой грамотности для всех категорий персонала;
- развивать гибридные компетенции (digital + управленческие/производственные);
- проводить тренинги по кибербезопасности и защите информации.

2. Создание новых ролей и специализаций

В процессе цифровой трансформации появляются новые профессиональные направления: специалисты по этике ИИ, аналитики данных, тренеры моделей машинного обучения, операторы цифровых платформ. Подготовка и адаптация таких специалистов позволяет предприятию самостоятельно управлять ИИ-средой, не полагаясь на сторонних провайдеров, что повышает уровень технологической независимости.

3. Снижение кадровых рисков

Нехватка квалифицированных кадров и несоответствие персонала новым требованиям представляют собой один из главных барьеров на пути цифровизации. Без опережающего развития человеческого капитала возможно возникновение:

- внутреннего сопротивления инновациям;
- неэффективного использования ИИ-систем;
- роста ошибок из-за недостаточной подготовки пользователей.

Преодоление этих рисков требует от предприятий инвестиций в программы переквалификации и адаптации персонала, включая обучение «на рабочем месте», менторство и внедрение цифровых ассистентов (например, чат-ботов).

4. Формирование цифровой культуры

Развитие человеческого капитала включает не только обучение, но и формирование новой корпоративной культуры, основанной на ценностях открытости к инновациям, ответственности за цифровые решения, уважении к этическим принципам использования ИИ. Такая культура способствует снижению сопротивления персонала, повышает вовлечённость и усиливает устойчивость к внешним шокам.

В условиях активной цифровизации и внедрения технологий искусственного интеллекта обеспечение экономической безопасности предприятий требует комплексного, системного подхода. Проведённый анализ позволил выделить три взаимосвязанных и взаимодополняющих фактора, от которых напрямую зависит устойчивость и эффективность цифровой трансформации бизнеса.

Во-первых, стратегическое планирование выступает основой управляемого и контролируемого перехода к использованию ИИ. Только при наличии чёткой стратегии, включающей оценку рисков, определение приоритетов и ресурсное обеспечение, возможно снижение неопределённости и достижение устойчивых экономических результатов.

Во-вторых, технологические меры играют решающую роль в защите цифровой инфраструктуры, данных и ИИ-сервисов от внешних и внутренних угроз. Без надёжной технической базы — средств защиты, мониторинга, аудита и устойчивости — любые достижения в цифровой сфере остаются уязвимыми и краткосрочными.

В-третьих, развитие человеческого капитала является связующим звеном, обеспечивающим не только техническую реализацию ИИ-решений, но и адаптацию сотрудников к новым условиям. Квалифицированный и мотивированный персонал способен не только эффективно использовать интеллектуальные технологии, но и предотвращать ошибки, связанные с человеческим фактором.

Таким образом, только при сбалансированном и синхронизированном развитии всех трёх компонентов — стратегии, технологий и человеческого ресурса — возможно формирование устойчивой модели экономической безопасности предприятия в условиях цифровой трансформации. Игнорирование любого из этих факторов может нивелировать эффект от внедрения ИИ и даже создать новые риски. Комплексный подход становится ключевым условием безопасного и эффективного функционирования бизнеса в цифровую эпоху.

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 рынок труда: вызовы и перспективы // Вестник Российской академии наук. — 2021. — Т. 91, № 8. С. 789–796.