

“Risks of Using Artificial Intelligence in Organizations and Governance Mechanisms”

Ruziboev Otamurod Shuxratovich

Mamun university Bachelor’s student of the Faculty of Economics, second year

e-mail: roziboyevotamurod88@gmail.com

tel: +998 93 758 88 86

Annotation: This thesis analyzes the main risks associated with the use of artificial intelligence in organizations and the mechanisms for managing them. The importance of effective control and responsible use of AI technologies to improve management efficiency is emphasized.

Keywords: artificial intelligence, risks, management mechanisms, digital transformation, organization

Аннотация: В тезисе рассматриваются основные риски использования искусственного интеллекта в организациях и механизмы их управления. Обоснована необходимость эффективного контроля и рационального применения AI-технологий для повышения управленческой эффективности

Ключевые слова: искусственный интеллект, риски, механизмы управления, цифровая трансформация, организация.

Annotatsiya: Mazkur tezisdagi tashkilotlarda sun’iy intellektdan foydalanish jarayonida yuzaga keladigan asosiy risklar va ularni boshqarish mexanizmlari tahlil qilinadi. Sun’iy intellekt texnologiyalaridan samarali va xavfsiz foydalanish orqali boshqaruv samaradorligini oshirish masalalari yoritilgan.

Kalit so‘zlar: sun’iy intellekt, risklar, boshqaruv mexanizmlari, raqamli transformatsiya, tashkilot.

Введение: В условиях стремительного развития цифровых технологий искусственный интеллект (ИИ) становится одним из ключевых факторов трансформации современных организаций. Использование AI-технологий позволяет автоматизировать управленческие процессы, оптимизировать использование ресурсов, повышать точность прогнозирования и принимать более обоснованные управленческие решения. Искусственный интеллект активно внедряется в сферы финансового управления, маркетинга, логистики, управления персоналом и стратегического планирования. Несмотря на значительные преимущества, использование искусственного интеллекта в организациях сопровождается рядом рисков, которые могут негативно повлиять на эффективность управления, устойчивость бизнеса и репутацию организаций. Недостаточное понимание данных рисков и отсутствие эффективных механизмов управления ими способны привести к финансовым потерям, ошибочным управленческим решениям и снижению доверия со стороны заинтересованных сторон. В связи с этим актуальной научной и практической задачей является анализ рисков использования искусственного интеллекта в организациях и разработка механизмов их эффективного управления. Целью данного тезиса является исследование основных видов рисков, возникающих при внедрении AI-технологий, а также обоснование необходимости комплексного и рационального подхода к управлению ими.

Роль искусственного интеллекта в современных организациях.

Искусственный интеллект представляет собой совокупность технологий и алгоритмов, способных имитировать когнитивные функции человека, включая анализ данных, обучение, прогнозирование и принятие решений. В современных организациях AI используется для обработки больших массивов данных, выявления закономерностей и автоматизации сложных

управленческих процессов. Основными направлениями применения искусственного интеллекта в организациях являются: финансовое прогнозирование и управление рисками; анализ потребительского поведения; оптимизация бизнес-процессов; поддержка управленческих решений; автоматизация процессов управления персоналом. В условиях цифровой трансформации искусственный интеллект становится стратегическим инструментом повышения конкурентоспособности организаций. Однако его широкое внедрение требует осознания возможных рисков и формирования эффективных механизмов контроля. Основные риски использования искусственного интеллекта. Риски информационной безопасности и конфиденциальности Одним из наиболее значимых рисков использования искусственного интеллекта является угроза безопасности и конфиденциальности данных. AI-системы функционируют на основе больших объемов информации, включая персональные и коммерчески чувствительные данные. Нарушение защиты таких данных может привести к утечкам информации, финансовым потерям и репутационным рискам. Особую опасность представляет использование внешних облачных AI-платформ, где контроль над данными может быть ограничен. В условиях отсутствия четких регламентов по защите информации риск кибератак и несанкционированного доступа значительно возрастает. Алгоритмические ошибки и искажения, AI-системы принимают решения на основе алгоритмов и обучающих данных. Если данные являются неполными, искаженными или некорректными, это может привести к ошибочным результатам и неправильным управленческим решениям. Алгоритмические ошибки особенно опасны в финансовом управлении и стратегическом планировании. Кроме того, наличие скрытых предвзятостей (bias) в данных может привести к дискриминационным

решениям, что негативно отражается на социальной ответственности организаций и их устойчивом развитии. Риск снижения роли человеческого фактора. Активная автоматизация управленческих процессов может привести к чрезмерной зависимости организаций от искусственного интеллекта и снижению роли человеческого фактора. В ряде случаев менеджеры могут полностью полагаться на рекомендации AI-систем, игнорируя профессиональный опыт и интуицию. Это создает риск потери управленческой гибкости, а также снижает способность организации реагировать на нестандартные ситуации, которые не могут быть корректно интерпретированы алгоритмами. Отсутствие прозрачности и объяснимости решений. Многие современные AI-модели, особенно основанные на машинном обучении и нейронных сетях, характеризуются низкой прозрачностью. Руководители организаций не всегда могут понять, каким образом система пришла к тому или иному решению. Отсутствие объяснимости решений создает риски для корпоративного управления, снижает доверие к AI-технологиям и усложняет процесс контроля их использования. Использование искусственного интеллекта поднимает ряд этических и правовых вопросов, связанных с ответственностью за принимаемые решения, соблюдением прав человека и социальной справедливостью. В условиях недостаточного правового регулирования AI-технологий организации могут столкнуться с юридическими спорами и санкциями.

Механизмы управления рисками использования искусственного интеллекта. Формирование системы корпоративного управления AI. Одним из ключевых механизмов управления рисками является создание системы корпоративного управления искусственным интеллектом. Такая система должна включать четкие регламенты использования AI-технологий,

распределение ответственности и контроль за их применением. Руководство организации должно определить стратегические цели внедрения AI и обеспечить соответствие технологий корпоративным ценностям и принципам устойчивого развития. Качество данных является критически важным фактором эффективного функционирования AI-систем. Для снижения рисков необходимо внедрение процедур проверки, очистки и актуализации данных. Использование надежных источников информации и регулярный аудит данных позволяют минимизировать вероятность алгоритмических ошибок. Постоянный мониторинг работы AI-систем и регулярный аудит алгоритмов являются важными элементами управления рисками. Это позволяет своевременно выявлять ошибки, отклонения и потенциальные угрозы, а также корректировать работу систем в соответствии с изменяющимися условиями.

Обеспечение взаимодействия человека и искусственного интеллекта: Эффективное управление рисками предполагает сохранение баланса между автоматизацией и участием человека в процессе принятия решений. Концепция «человек-в-контуре» (human-in-the-loop) позволяет сочетать аналитические возможности AI с профессиональным опытом менеджеров. Важным механизмом управления является разработка и внедрение этических норм использования искусственного интеллекта. Такие стандарты должны регулировать вопросы прозрачности, ответственности и социальной справедливости при применении AI-технологий. Значение управления AI-рисками для повышения управленческой эффективности. Рациональное управление рисками использования искусственного интеллекта способствует повышению эффективности управления и устойчивому развитию организаций. Применение комплексного подхода позволяет: повысить качество управленческих решений; снизить вероятность финансовых потерь; укрепить

доверие заинтересованных сторон; обеспечить соответствие деятельности организаций требованиям цифровой экономики. Организации, которые осознанно подходят к управлению AI-рисками, получают стратегические преимущества и повышают свою конкурентоспособность в долгосрочной перспективе.

Заключение: Искусственный интеллект является мощным инструментом цифровой трансформации и повышения управленческой эффективности. Однако его использование в организациях сопровождается значительными рисками, связанными с безопасностью данных, алгоритмическими ошибками, этическими и управленческими аспектами. В данном тезисе обоснована необходимость внедрения эффективных механизмов управления рисками использования искусственного интеллекта. Комплексный подход, включающий контроль качества данных, мониторинг AI-систем, развитие человеческого капитала и формирование этических стандартов, позволяет минимизировать негативные последствия и обеспечить устойчивое развитие организаций в условиях цифровой экономики.

REFERENCES:

1. Kaplan A., Haenlein M. *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*. — Business Horizons, 2019.
2. Russell S., Norvig P. *Artificial Intelligence: A Modern Approach*. — Pearson Education, 2021.
3. Bughin J., Seong J., Manyika J. *The future of AI: Managing risks and rewards*. — McKinsey Global Institute, 2020.
4. Dwivedi Y. et al. *Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges*. — International Journal of Information Management, 2021.
5. OECD. *Artificial Intelligence Risk Management*. — OECD Publishing, 2023.