Научная статья
УДК 327
https://doi.org/10.53658/RW2025-4-4(18)-225-238

Политические науки

Политические риски в сфере искусственного интеллекта: сравнительный анализ

Антон Владимирович Василенко✉

Независимый исследователь, Москва, Россия
anton.vasilenko25@gmail.com, https://orcid.org/0009-0004-7575-8382

Аннотация. Исследование, представленное в статье, направлено на выявление системных угроз политической стабильности и цифровому суверенитету Республики Узбекистан, обусловленных фрагментарностью правового регулирования в области искусственного интеллекта (ИИ). На основании сравнительного анализа регуляторных моделей Узбекистана, Российской Федерации и Республики Казахстан были выявлены критические пробелы в системе правового регулирования ИИ в Узбекистане. В частности, отсутствуют специализированные законодательные акты, регулирующие использование ИИ, этические нормы его применения, прямые запреты на использование манипулятивных технологий, таких как deepfake, механизмы оценки рисков внедрения ИИ, четкое разграничение ответственности за причиненный вред, а также развитая национальная инфраструктура и эффективные инструменты подготовки кадров. В контексте медиаэкологической теории Маршалла Маклюэна, рассматривающей ИИ как «внешний мозг», указанные пробелы формируют порочный круг взаимосвязанных политических рисков. Когнитивная уязвимость населения, известная как «brain rot», в сочетании с нерегулируемыми синтетическими медиа (deepfake) создает условия для массовых манипуляций. Технологическая зависимость от зарубежных платформ и отток специалистов приводят к утрате цифрового суверенитета. Некритичное внедрение ИИ в государственный сектор при отсутствии механизмов ответственности подрывает институциональное доверие. В статье приведены доказательства того, что сохранение текущего регуляторного подхода превращает ИИ из инструмента развития в источник системной уязвимости. Для минимизации этих рисков необходимо незамедлительное принятие комплексного законодательства,

учитывающего передовой опыт соседних государств и отвечающего современным вызовам в области правового регулирования ИИ.

Ключевые слова: искусственный интеллект, Республика Узбекистан, регулирование ИИ, deepfake, brain rot, иллюзия компетентности, технологический суверенитет

Для цитирования: Василенко А.В. Политические риски в сфере искусственного интеллекта: сравнительный анализ // Россия и мир: научный диалог. 2025. № 4(18). С. 225-238, https://doi.org/10.53658/RW2025-4-4(18)-225-238

Original Article Political Sciences
https://doi.org/10.53658/RW2025-4-4(18)-225-238

Political Risks in Artificial Intelligence: A Comparative Analysis

Anton V. Vasilenko✉

Independent Researcher, Moscow, Russia
anton.vasilenko25@gmail.com, https://orcid.org/0009-0004-7575-8382

Abstract. The study presented in this article aims to identify systemic threats to political stability and digital sovereignty in the Republic of Uzbekistan caused by fragmented legal regulation in the field of artificial intelligence (AI). A comparative analysis of regulatory models in Uzbekistan, Russia and Kazakhstan revealed critical gaps in legal frameworks for AI, specifically, there is a lack of specialized legislation on use of AI, ethical standards, and a direct prohibition on manipulative techniques such as deepfakes, mechanisms for risk assessment, clear delineation of responsibility for harm, and the development of national infrastructure with effective training tools. In the context of Marshall McLuhan's media ecological theory, which views AI as an "external brain," these gaps create a vicious cycle of interrelated political risks. The population's cognitive vulnerability, known as "brain rot," combined with unregulated synthetic media (deepfakes), creates the conditions for mass manipulation. Technological dependence on foreign platforms and the exodus of specialists lead to the loss of digital sovereignty. The uncritical implementation of AI in the public sector without accountability mechanisms undermines institutional trust. The article provides evidence that maintaining the current regulatory approach turns AI from a tool for development into a source of systemic vulnerability. In order to minimize these risks, it is necessary to immediately adopt comprehensive legislation that takes into account best practices from neighboring countries and addresses current challenges in the legal regulation of AI.

Keywords: artificial intelligence, Republic of Uzbekistan, AI regulation, deepfake, brain rot, illusory competence, technological sovereignty

For citation: Vasilenko A.V. Political Risks in Artificial Intelligence: A Comparative Analysis. Russia & World: Scientific Dialogue. 2025; 4(18): 225-238, https://doi.org/10.53658/RW2025-4-4(18)-225-238

Введение

Стремительное проникновение технологий искусственного интеллекта (ИИ) в ключевые сферы общественной жизни, включая государственное управление, образование и медиакоммуникации, порождает комплекс новых вызовов для национальной безопасности и социально-политической стабильности государств. Особую актуальность эти вызовы приобретают для развивающихся стран, где регуляторные механизмы зачастую не успевают за скоростью технологических изменений[1]. Республика Узбекистан (РУ), активно внедряющая ИИ в рамках утвержденной Стратегии развития до 2030 г., не является исключением.

Как отмечают современные и классические исследователи, технологии, изначально воспринимаемые как инструмент прогресса, способны обнажать и усиливать системные риски, связанные с человеческой природой и институциональными ограничениями. Интернет, задуманный как глобальное хранилище знаний, трансформировался в среду распространения дезинформации и поляризации [3]. Социальные сети, эксплуатирующие биологические механизмы вознаграждения, влияют на когнитивные функции пользователей [4]. Современные системы ИИ, делегирующие когнитивные функции человека (анализ данных, генерация контента, поддержка решений), несут новые угрозы: создание сверхреалистичных дипфейков (deepfakes) для манипуляции общественным мнением[2], распространение низкокачественного контента, ведущего к «когнитивной деградации» («brain rot») [9], формирование иллюзии компетентности и зависимости от алгоритмических решений[3]. Эти риски напрямую затрагивают политическую сферу, угрожая дестабилизацией, эрозией доверия к институтам власти и потерей цифрового суверенитета.

Несмотря на осознание рисков на глобальном уровне (принципы ОЭСР[4], Регламент ЕС об ИИ[5]) и активную разработку регуляторных рамок в соседних

1 World Bank (2023). Digital Policy in Transition Economies: Institutional Lag and Innovation Challenges. P. 7. URL: https://openknowledge.worldbank.org.
2 ИМЭМО РАН. Искусственный интеллект для войны и мира: подводя итоги года // Официальный сайт ИМЭМО, 2023. URL: https://www.imemo.ru/publications/policy-briefs/text/artificial-intelligence-for-war-and-peace-summing-up-the-year.
3 Walther C.C. Intelligence Illusion: What Apple's AI Study Reveals About Reasoning // Forbes, 2025. URL: https://www.forbes.com/sites/corneliawalther/2025/06/09.
4 Recommendation of the Council on OECD Legal Instruments Artificial Intelligence // OECD. URL: https://wecglobal.org/uploads/2019/07/2019_OECD_Recommendations-AI.pdf.
5 Регламент (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 г., устанавливающий гармонизированные правила в отношении искусственного интеллекта и вносящий поправки в Регламенты (ЕС) № 300/2008, (ЕС) № 167/2013, (ЕС) № 168/2013, (ЕС) 2018/858, (ЕС) 2018/1139 и (ЕС) 2019/2144 и Директивы 2014/90/ЕС, (ЕС) 2016/797 и (ЕС) 2020/1828 (Закон об искусственном интеллекте) // EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

государствах – Российской Федерации (РФ)[6] и Республике Казахстан (РК)[7], – в Узбекистане сохраняется фрагментарность правового регулирования ИИ. Основываясь преимущественно на внесении поправок в существующие акты и декларативной Стратегии, система РУ демонстрирует значительные пробелы по ключевым аспектам: отсутствие этических принципов, запретов на опасные применения (включая deepfake в политическом контексте), механизмов управления рисками и оценки соответствия, четкого разграничения ответственности, а также развитой национальной инфраструктуры и реальных инструментов поддержки[8].

Проблема исследования заключается в отсутствии комплексного сравнительного анализа регуляторных подходов к ИИ в РУ, РФ и РК, ориентированного на выявление конкретных пробелов узбекистанского регулирования и оценку связанных с ними политических рисков в контексте современных вызовов (deepfake, brain rot, потеря технологического суверенитета, отток кадров).

Целью данного исследования является проведение сравнительного анализа правовых и стратегических подходов к регулированию ИИ в РФ, РК и РУ для определения ключевых недостатков регуляторной модели Узбекистана и оценки потенциальных политических рисков, обусловленных этими недостатками.

Материалы и методы

Концептуальной основой для анализа трансформации когнитивных процессов и коммуникаций под влиянием ИИ служат подходы к пониманию медиа канадского философа и футуролога Маршалла Маклюэна. В фундаментальном труде «Понимание медиа: внешние расширения человека» (1964) Маклюэн утверждает, что любая технология является продолжением (протезом) человеческих органов или функций (колесо – ноги, одежда – кожа, электрические медиа (ТВ, радио) – центральная нервная система), создавая эффект «глобальной деревни» [4]. Экстраполируя эту концепцию на современность, ИИ можно интерпретировать как формирование «внешнего мозга» – технологического расширения, берущего на себя функции биологической когнитивной системы: хранение и обработку информации (память), генерацию текстов и идей (мышление), прогнозирование (принятие решений). Подобное «делегирование» когнитивных функций, предупреждал Маклюэн, несет риск снижения критической рефлексии и зависимости от технологических посредников [4]. Современные исследования подтверждают и конкретизируют эти риски в контексте ИИ, выявляя ключевые феномены, в том числе имеющие политические и социальные последствия:

- Иллюзия компетентности – феномен, при котором пользователи приписывают себе знания и аналитические способности, фактически генерируемые ИИ-системой (например, при использовании генеративных моделей для написания текстов или анализа данных). Это ведет к переоценке собственной экспертизы, снижению мотивации к глубокому освоению материала и неадекватной оценке рисков [2]. В политическом контексте это проявляется как у чиновников, некритично делегирующих решения ИИ-алгоритмам в управлении или правоприменении, так и у граждан, формирующих политические суждения на основе поверхностно усвоенного ИИ-контента, что снижает качество публичной дискуссии и повышает манипулятивность[9].
- «Brain rot» как метафора когнитивной деградации – термин, получивший распространение в научной коммуникации (в т.ч. как «Слово года 2024» по версии «Оксфордского словаря»[10]), описывает комплекс негативных когнитивных эффектов от потребления низкокачественного, часто генерируемого ИИ контента (абсурдные видео, упрощенные нарративы), оптимизированного исключительно для удержания внимания. Исследования фиксируют связь такого контента с фрагментацией внимания, снижением способности к концентрации, критическому анализу и долгосрочному запоминанию сложной информации [9]. Политический риск заключается в формировании электората, восприимчивого к упрощенным популистским лозунгам, манипуляциям и неспособного к анализу комплексных политических программ, что подрывает основы демократического дискурса и стабильность [6].
- Deepfake как инструмент политической дестабилизации: технологии синтетических медиа (deepfake), позволяющие создавать сверхреалистичные подделки видео- и аудиозаписей публичных лиц, представляют собой качественно новый уровень информационной угрозы. Уже упомянутая концепция Маршалла Маклюэна, описывающая медиа как «внешние расширения», которые искажают восприятие реальности, здесь достигает апогея [4]. Эмпирические исследования и инциденты (например, фейковое видео спикера Палаты представителей США Нэнси Пелоси в 2022 г.[11]) демонстрируют высокую эффективность deepfake в подрыве доверия к политическим институтам [7], разжигании социальной розни, фальсификации

6 О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента Российской Федерации от 10.10.2019 № 490 (ред. от 15.02.2024) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/.

7 Об искусственном интеллекте: проект Закона Республики Казахстан (январь 2025 г.) // Zakon.kz. URL: https://online.zakon.kz/Document/?doc_id=34868071.

8 Об утверждении Стратегии развития искусственного интеллекта в Республике Узбекистан на период до 2030 года: Постановление Президента Республики Узбекистан № ПП-123 от 01.10.2024 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/ru/docs/7158606.

9 Walther C.C. Intelligence Illusion: What Apple's AI Study Reveals About Reasoning // Forbes, 2025. URL: https://www.forbes.com/sites/corneliawalther/2025/06/09.

10 «Brain rot» named Oxford Word of the Year 2024 // Oxford Languages, 2024. URL: https://corp.oup.com/news/brain-rot-named-oxford-word-of-the-year-2024/.

11 Fact Check: Video features deepfakes of Nancy Pelosi, Alexandria Ocasio-Cortez and Joe Biden // Reuters, 2023. URL: https://www.reuters.com/article/fact-check.

событий и манипуляции электоральным поведением [1]. Риск усугубляется скоростью распространения такого контента в социальных сетях и трудностью его оперативного опровержения.

Идеи Маклюэна находят развитие у ключевых теоретиков цифрового общества:

- Элвин Тоффлер («Третья волна», 1980) прогнозировал переход к «супериндустриальному обществу», где информация становится ключевым ресурсом власти [8]. Его концепт «футурошока» (дезориентация от ускорения изменений) объясняет уязвимость общества к ИИ-рискам: технологии развиваются быстрее, чем способность институтов к адаптации.
- Мануэль Кастельс («Информационная эпоха», 1996) показал, что сетевая структура общества усиливает асимметрию контроля над данными [3]. Для Узбекистана это означает риск потери технологического суверенитета и зависимость от зарубежных ИИ-платформ.
- Нил Постман («Развлекаемся до смерти», 1985) утверждал, что медиаформат (например, телевидение) определяет содержание политики, вытесняя рациональный дискурс развлечением [11]. ИИ-генерация brain rot-контента – логичное продолжение этой тенденции в эпоху алгоритмов.

Рассмотренные концепции ученых-футурологов и экстраполяция этих идей на современные негативные проявления в сфере ИИ позволяют сформулировать ключевые политические риски для Республики Узбекистан через призму упомянутых цифровых и медиафеноменов. В Таблице 1 выделены ключевые соответствия между теоретическими концепциями и специфическими рисками ИИ для Узбекистана.

Таблица 1. Синтез теорий применительно к ИИ-рискам
Table 1. Synthesis of theories applied to AI risks

Научный концепт	Политический риск для Узбекистана
Маклюэн: «Внешний мозг» – Иллюзия компетентности	Чиновники или граждане переоценивают свои силы, делегируя решения ИИ – Эрозия экспертизы
Тоффлер: «Футурошок» – Скорость изменений	Регуляторы РУ не успевают за ИИ-инновациями – Правовой вакуум
Кастельс: Сетевая власть – Контроль данных	Зависимость от зарубежных платформ – Потеря технологического суверенитета
Постман: Триумф развлечений – Brain rot	Алгоритмический контент разрушает критическое мышление – Уязвимость к популизму

Источник: составлено автором по материалам [3–5; 8]
Source: compiled by the author based on materials from [3–5; 8]

Синтез выявленных рисков, основанный на рассмотренных теориях, демонстрирует их взаимоусиливающий характер. Порочный круг когнитивной зависимости (Маклюэн), где ИИ, как «внешний мозг», ослабляет критическое мышление («иллюзия компетентности»), создавая аудиторию, уязвимую к генерируемому им же манипулятивному контенту (brain rot, deepfake), снижает саму способность общества распознавать угрозы. Этот риск усугубляется институциональным отставанием (Тоффлер): скорость ИИ-развития («футурошок») создает высокую вероятность правового вакуума, при котором регуляторы Республики Узбекистан не успевают адаптировать нормы к новым вызовам, оставляя риски, описанные Маклюэном и Постманом, без адекватного ответа. Дополнительным фактором является угроза технологическому суверенитету (Кастельс): зависимость от зарубежных ИИ-платформ («сетевая власть») означает, что контроль над данными и алгоритмами находится вне юрисдикции Узбекистана, что потенциально ограничивает возможности страны в противодействии манипуляциям (deepfake) и защите от когнитивной деградации (brain rot). Наконец, эрозия публичной сферы (Постман), вызванная доминированием алгоритмического развлекательного контента (brain rot) и усиленная эффектами «иллюзии компетентности» (Маклюэн), напрямую повышает уязвимость общества к упрощенным популистским нарративам, подрывая основы рационального политического диалога.

Таким образом, эффективность государственной политики Республики Узбекистан по противодействию этому комплексу взаимосвязанных рисков напрямую зависит от способности законодательства и институтов: адаптироваться к скорости изменений (преодолевая «футурошок» Тоффлера), обеспечивать технологический суверенитет (вопреки вызовам «сетевой власти» Кастельса) и защищать когнитивные способности граждан от деградации (нивелируя эффекты Маклюэна и Постмана). Далее будет проанализировано, насколько текущее законодательство Узбекистана в сфере ИИ соответствует этим вызовам в сравнении с законодательством соседних стран.

Результаты исследования

Сравнительный анализ нормативно-правовых баз РФ, РК и РУ по семи ключевым критериям регулирования ИИ, разработанным автором, выявил существенные различия в подходах и значительные пробелы в системе Узбекистана. Основные результаты структурированы в соответствии с методологическими критериями (Таблица 2).

Таблица 2. Сравнительный анализ подходов к регулированию ИИ в РФ, РК и РУ
Table 2. Comparative analysis of approaches to AI regulation in the Russian Federation, Kazakhstan and the Republic of Uzbekistan

Критерий	Республика Узбекистан (РУ)	Республика Казахстан (РК)	Российская Федерация (РФ)
К1. Структура регулирования	Отсутствие базового закона. Регулирование через поправки в Законы «Об информатизации», «Об электронном правительстве»[12] и Стратегию до 2030 г.[13]	В первом чтении принят специализированный Закон «Об искусственном интеллекте» (2025)[14] с четкой архитектурой норм	Указ Президента № 490 (2019) + Нацстратегия до 2030 г.[15] Законопроект об искусственном интеллекте на стадии разработки (2025)[16]
К2. Этические принципы	Отсутствуют. Стратегия[17] упоминает «общечеловеческие ценности» без расшифровки применительно к ИИ	Закреплены 7 принципов: человекоцентричность, прозрачность, безопасность, конфиденциальность, инклюзивность, подотчетность, устойчивость[18]	Этические нормы включены в Нацстратегию[19]: «доверенный ИИ», приоритет человека, недискриминация
К3. Запрещенные применения	Нет прямых запретов. Не регулируются deepfake, системы социального рейтинга, автономное оружие	Четкий запрет: манипуляции сознанием (вкл. deepfake без маркировки), социальный рейтинг, оценка поведения, автономное оружие[20]	Запрет на использование ИИ для угроз безопасности (Стратегия[21]). Госдума рассматривает поправки о deepfake[22]
К4. Управление рисками	Нет требований к оценке рисков ИИ-систем. Не созданы механизмы контроля	Обязательная оценка рисков на всех этапах жизненного цикла ИИ. Сертификация систем «высокого риска»[23]	Создание Центра развития ИИ (2025) для координации оценки рисков. Требования к «критическим» ИИ-системам в Стратегии[24]
К5. Инфраструктура	Отсутствует национальная платформа, песочницы, механизмы доступа к госданным для разработчиков	Запущена Национальная платформа ИИ (QazAI) с открытыми библиотеками данных, API и тестовой средой[25]	Развертывание Единой платформы данных в рамках реализации Указа Президента РФ[26]
К6. Ответственность	Не разграничена. Нет специальных норм об ответственности за вред от ИИ-решений	Четкое разделение: разработчик → оператор → пользователь. Гражданско-правовая ответственность за дискриминационные / вредоносные решения[27]	Регулируется общими нормами ГК РФ. Законопроект об искусственном интеллекте (2025)[28] вводит понятие «оператор ИИ» и его ответственность
К7. Господдержка	Декларативные положения Стратегии[29]. Нет механизмов финансирования, налоговых льгот, грантов	Фонд QazTech Ventures, налоговые каникулы для ИИ-стартапов, гранты на исследования, льготные кредиты[30]	Бюджет на исследования (2025), субсидии компаниям, акселераторы в рамках реализации Указа Президента РФ [31]

Источник: составлено автором

Source: compiled by the author

ISSN 2782-3067 (Print)

12 О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с совершенствованием законодательства в сфере обеспечения кибербезопасности: Закон Республики Узбекистан от 20.09.2024 № ЗРУ-964 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/ru/docs/7108725.

13 Об утверждении Стратегии развития искусственного интеллекта в Республике Узбекистан на период до 2030 года: Постановление Президента Республики Узбекистан № ПП-123 от 01.10.2024 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/ru/docs/7158606.

ISSN 2782-3067 (Print)

14 Об искусственном интеллекте: проект Закона Республики Казахстан (январь 2025 г.) // Zakon.kz. URL: https://online.zakon.kz/Document/?doc_id=34868071.

15 О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента Российской Федерации от 10.10.2019 № 490 (ред. от 15.02.2024) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/.

16 Авторы законопроекта об искусственном интеллекте пояснили суть инициативы // РБК, 2025. URL: https://www.rbc.ru/technology_and_media/15/04/2025/67fe02d89a79472cf8ca1af4.

17 Там же.

18 Об искусственном интеллекте: проект Закона Республики Казахстан (январь 2025 г.) // Zakon.kz. URL: https://online.zakon.kz/Document/?doc_id=34868071.

19 О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента Российской Федерации от 10.10.2019 № 490 (ред. от 15.02.2024) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/.

20 Об искусственном интеллекте: проект Закона Республики Казахстан (январь 2025 г.) // Zakon.kz. URL: https://online.zakon.kz/Document/?doc_id=34868071.

21 О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента Российской Федерации от 10.10.2019 № 490 (ред. от 15.02.2024) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/.

22 О внесении изменений в Уголовный кодекс Российской Федерации (в части установления уголовной ответственности за совершение преступлений с использованием технологий подмены личности): законопроект № 718538-8 (16.09.2024 – 14.10.2024) // Официальный сайт Государственной Думы РФ. URL: https://sozd.duma.gov.ru/bill/718538-8.

23 Об искусственном интеллекте: проект Закона Республики Казахстан (январь 2025 г.) // Zakon.kz. URL: https://online.zakon.kz/Document/?doc_id=34868071.

24 О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента Российской Федерации от 10.10.2019 № 490 (ред. от 15.02.2024) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/.

25 Об искусственном интеллекте: проект Закона Республики Казахстан (январь 2025 г.) // Zakon.kz. URL: https://online.zakon.kz/Document/?doc_id=34868071.

26 О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента Российской Федерации от 10.10.2019 № 490 (ред. от 15.02.2024) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/.

27 Об искусственном интеллекте: проект Закона Республики Казахстан (январь 2025 г.) // Zakon.kz. URL: https://online.zakon.kz/Document/?doc_id=34868071.

28 Авторы законопроекта об искусственном интеллекте пояснили суть инициативы // РБК, 2025. URL: https://www.rbc.ru/technology_and_media/15/04/2025/67fe02d89a79472cf8ca1af4.

29 Об утверждении Стратегии развития искусственного интеллекта в Республике Узбекистан на период до 2030 года: Постановление Президента Республики Узбекистан № ПП-123 от 01.10.2024 // Национальная база данных законодательства Республики Узбекистан. URL: https://lex.uz/ru/docs/7158606.

30 Об искусственном интеллекте: проект Закона Республики Казахстан (январь 2025 г.) // Zakon.kz. URL: https://online.zakon.kz/Document/?doc_id=34868071.

31 О развитии искусственного интеллекта в Российской Федерации (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года»): Указ Президента Российской Федерации от 10.10.2019 № 490 (ред. от 15.02.2024) // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_335184/.

Ключевые выводы по критериям:

- Правовая неопределенность (К1). Узбекистан – единственная из трех стран без специализированного закона или его проекта. Регулирование фрагментарно, что создает правовой вакуум для разработчиков и пользователей. РК демонстрирует наиболее продвинутую законодательную базу.
- Этические аспекты (К2). Отсутствие этических принципов ИИ в РУ контрастирует с детально проработанными нормами РК и РФ. Это повышает риски дискриминационных решений в госсекторе.
- Уязвимость к манипуляциям (К3). Неспособность РУ противодействовать deepfake (из-за отсутствия запретов и требований к маркировке) создает критический риск политических провокаций. РК устанавливает здесь «золотой стандарт».
- Слепое внедрение (К4). Отсутствие оценки рисков в РУ повышает вероятность внедрения опасных ИИ-систем в госуправлении, ведущего к техногенным авариям или утечкам данных. Механизмы РК и РФ обеспечивают контроль.
- Технологическая зависимость (К5). Отсутствие инфраструктуры в РУ усиливает зависимость от зарубежных платформ, создавая угрозу утраты технологического суверенитета в сфере ИИ. РК и РФ активно развивают национальные аналоги.
- Безнаказанность (К6). Неразграниченная ответственность в РУ делает невозможным привлечение виновных к ответу за вред от ИИ-решений (например, дискриминация при оказании госуслуг). РК предлагает четкую модель.
- Утечка кадров (К7). Декларативность поддержки в РУ при активных мерах РК и РФ создает высокий риск оттока специалистов и стартапов за рубеж.

Обсуждение

Политические риски регуляторных пробелов Узбекистана

Сравнительный анализ выявил системные недостатки регулирования ИИ в РУ. Ниже обсуждается, как эти пробелы (в контексте медиаэкологической теории Маклюэна и современных вызовов) формируют конкретные угрозы политической стабильности, суверенитету и доверию населения к государственным институтам.

Риск массовых манипуляций и дестабилизации

Отсутствие этических принципов (К2) и прямых запретов на использование deepfake в политических целях (К3) создает в РУ опасный правовой вакуум. В условиях растущего распространения brain rot-контента, снижающего критическое мышление населения, синтетические медиа (deepfake) становятся идеальным инструментом для:

- фальсификации выступлений политиков (пример: поддельное видео президента / министров с провокационными заявлениями, особенно в периоды выборных кампаний);
- разжигания межэтнической / межрегиональной розни (пример: фейковые видео «нападений» на фоне напряженности);
- подрыва легитимности выборов (пример: «доказательства» фальсификаций от ИИ-ботов).

Как показывает опыт США (кейс Пелоси[32]), даже единичный инцидент может спровоцировать волну насилия. Для РУ, где медиаэкосистема уязвима, а население активно пользуется соцсетями, отсутствие механизмов блокировки и маркировки deepfake (как в РК) является непосредственной угрозой национальной безопасности. Концепция Маклюэна о медиа как «внешних расширениях», искажающих реальность [4], здесь реализуется в наиболее опасной форме.

Утрата цифрового суверенитета и технологическое отставание

Зависимость от иностранных ИИ-платформ из-за отсутствия национальной инфраструктуры (К5) и отток ИИ-кадров / стартапов зарубеж из-за декларативной поддержки (К7) ведут к утрате суверенитета:

- технологического; данные граждан и госорганов РУ обрабатываются на зарубежных серверах, подчиняясь чужим юрисдикциям (напр., законам США / ЕС);
- интеллектуального; разработка критически важных ИИ-решений (для госуправления, безопасности) зависит от иностранных компаний или уехавших специалистов.

Вместо усиления когнитивного суверенитета РУ рискует стать потребителем чужих, потенциально враждебных «когнитивных расширений». Опыт Казахстана (нацплатформа QazAI) и России (Единая платформа данных) демонстрирует путь к технологической независимости, закрытый для РУ из-за пробелов в К5 и К7.

Эрозия институционального доверия и «правовой беспредел»

Внедрение ИИ в госсектор без оценки рисков (К4) и при неразграниченной ответственности (К6) чревато:

- дискриминационными решениями алгоритмов (напр., при назначении пособий, одобрении кредитов), что вызовет волну недовольства и судебных исков;
- техногенными сбоями (напр., коллапс системы «электронного правительства» из-за ошибки ИИ), подрывающими доверие к цифровизации;
- безнаказанностью разработчиков / операторов за вредоносные ИИ-действия.

Феномен «иллюзии компетентности» усугубляет риск: чиновники, переоценивающие свои навыки работы с ИИ, будут некритично доверять алгоритмам. В отличие от РК, где закон четко распределяет ответственность, правовой вакуум РУ превращает ИИ в «черный ящик», ошибки которого исправить невозможно. Это непосредственно угрожает социальной стабильности и репутации государственных институтов.

32 Fact Check: Video features deepfakes of Nancy Pelosi, Alexandria Ocasio-Cortez and Joe Biden // Reuters, 2023. URL: https://www.reuters.com/article/fact-check.

Взаимосвязь рисков

Выявленные регуляторные пробелы образуют систему взаимно усиливающихся рисков, где игнорирование одного компонента катализирует кризис в смежных сферах:

- нерегулируемые deepfake (К3) в условиях массовой когнитивной уязвимости (brain rot) создают идеальную среду для фальсификации политической реальности, провоцируя социальные взрывы;
- отсутствие национальной инфраструктуры (К5) на фоне оттока кадров (К7) консервирует технологическую зависимость, передавая контроль над данными и алгоритмами внешним игрокам;
- «слепое» внедрение ИИ в госсектор (К4) при правовой безнаказанности (К6) усугубляется «иллюзией компетентности» чиновников, превращая алгоритмы в инструмент институциональной дискредитации.

Эта триада рисков формирует порочный круг: технологическая зависимость ограничивает возможности противодействия deepfake, а эрозия доверия к институтам снижает способность общества распознавать манипуляции, усиливая когнитивную уязвимость.

Выводы

Проведенное исследование демонстрирует, что фрагментарное регулирование искусственного интеллекта в Республике Узбекистан формирует системные угрозы политической стабильности, технологическому суверенитету и социальному доверию. Сравнительный анализ с опытом РФ и РК выявил критические пробелы: отсутствие базового закона об ИИ, этических принципов, запретов на манипулятивные технологии (deepfake), механизмов оценки рисков и ответственности, а также национальной инфраструктуры. Эти пробелы создают благоприятную среду для реализации ключевых рисков, теоретически предсказанных в рамках медиаэкологической парадигмы Маклюэна и развитых футурологами.

Нерегулируемое распространение синтетических медиа (К3) в условиях когнитивной уязвимости населения («brain rot») превращает ИИ в инструмент политической дестабилизации. Технологическая зависимость от зарубежных платформ (К5) и отток кадров (К7) подрывают цифровой суверенитет, переводя Узбекистан в позицию потребителя враждебных «когнитивных расширений». Одновременно «слепое» внедрение ИИ в госсектор (К4) при правовой безнаказанности (К6) усугубляется «иллюзией компетентности» чиновников, приводя к эрозии институционального доверия.

Взаимосвязь этих рисков образует порочный круг: технологическое отставание ограничивает возможности противодействия deepfake, эрозия доверия снижает резистентность к манипуляциям, а когнитивная деградация усиливает восприимчивость к популизму. В контексте теории Маклюэна ИИ, как «внешний мозг», не только генерирует угрозы, но и ослабляет способность общества к их распознаванию, реализуя предупреждение Тоффлера о «футурошоке» – стремительном отставании институтов от технологий.

Таким образом, сохранение регуляторного статус-кво в РУ создает кумулятивную угрозу: технологии, призванные служить развитию, превращаются в фактор системной уязвимости. Преодоление этого сценария требует не декларативных мер, а конвертации теоретических императивов в правовые решения, как это продемонстрировали соседние государства. Будущее политической стабильности Узбекистана зависит от способности трансформировать осознание рисков в эффективную архитектуру технологического суверенитета.

Список литературы

1. Виноградова Е.А. Потенциальные угрозы несанкционированного использования политических дипфейков в период политических выборов: международный опыт [Potential Threats of Unauthorized Use of Political Deepfakes during Political Elections: International Experience] // Мировая политика. 2024. № 3. С. 44–60. https://doi.org/10.25136/2409-8671.2024.3.71519. EDN: KNTVCO. URL: https://nbpublish.com/library_read_article.php?id=71519.
2. Grgić-Hlača N. et al. Knowing About Knowing: An Illusion of Human Competence Can Hinder Appropriate Reliance on AI Systems // Proceedings of the ACM Conference on Fairness, Accountability, and Transparency. 2024. P. 1–15. https://doi.org/10.1145/3544548.3581025.
3. Castells M. The Information Age: Economy, Society, and Culture. Oxford: Blackwell, 2000. 608 p.
4. McLuhan M. Understanding Media: The Extensions of Man. New York: McGraw-Hill, 1964.
5. Postman N. Amusing Ourselves to Death: Public Discourse in the Age of Show Business. New York: Penguin Books, 1985. 184 p.
6. Rădulescu B.-G. The Threat of Algorithmic Populism: Intelligence Strategies for Safeguarding Democracy // Intelligence Info 2025. Vol. 8(1). P. 33–49. URL: https://www.intelligenceinfo.org/the-threat-of-algorithmic-populism-intelligence-strategies-for-safeguarding-democracy/.
7. The Political Economy of Attention // Annual Review of Anthropology. 2023. Vol. 52. P. 287–304. URL: https://www.annualreviews.org/content/journals/10.1146/annurev-anthro-101819-110356.
8. Toffler A. The Third Wave. New York: Bantam Books, 1980.
9. Yousef A.M.F., Alshamy A., Tlili A., Metwally A.H.S. Demystifying the New Dilemma of Brain Rot in the Digital Era: A Review // Brain Sci. 2025. № 15. P. 283. https://doi.org/10.3390/brainsci15030283.

Информация об авторе

ВАСИЛЕНКО Антон Владимирович. Независимый исследователь. https://orcid.org/0009-0004-7575-838. Адрес: Российская Федерация, г. Москва. anton.vasilenko25@gmail.com

Раскрытие информации о конфликте интересов

Автор заявляет об отсутствии конфликта интересов.

Информация о статье

Поступила в редакцию: 11 июля 2025 г. Одобрена после рецензирования: 10 октября 2025 г. Принята к публикации: 20 ноября 2025 г. Опубликована: 1 декабря 2025 г.

Автор прочитал и одобрил окончательный вариант рукописи.

Информация о рецензировании

«Россия и мир: научный диалог» благодарит анонимных рецензентов за их вклад в рецензирование этой работы.

References

1. Vinogradova E.A. Potential Threats of Unauthorized Use of Political Deepfakes during Political Elections: International Experience. Mirovaya Politika [World Politics], 2024; 3:44–60 [In Russian]. https://doi.org/10.25136/2409-8671.2024.3.71519. EDN: KNTVCO. Available from: https://nbpublish.com/library_read_article.php?id=71519.
2. Grgić-Hlača N. et al. Knowing About Knowing: An Illusion of Human Competence Can Hinder Appropriate Reliance on AI Systems. Proceedings of the ACM Conference on Fairness, Accountability, and Transparency. 2024:1–15 [In English]. https://doi.org/10.1145/3544548.3581025.
3. Castells M. The Information Age: Economy, Society, and Culture. Oxford: Blackwell, 2000. 608 p. [In English].
4. McLuhan M. Understanding Media: The Extensions of Man. New York: McGraw-Hill, 1964 [In English].
5. Postman N. Amusing Ourselves to Death: Public Discourse in the Age of Show Business. New York: Penguin Books, 1985 [In English].
6. Rădulescu B.-G. The Threat of Algorithmic Populism: Intelligence Strategies for Safeguarding Democracy. Intelligence Info 2025; 8(1):33–49 [In English]. Available from: https://www.intelligenceinfo.org/the-threat-of-algorithmic-populism-intelligence-strategies-for-safeguarding-democracy/.
7. The Political Economy of Attention. Annual Review of Anthropology. 2023; 52:287–304 [In English] Available from: https://www.annualreviews.org/content/journals/10.1146/annurev-anthro-101819-110356.
8. Toffler A. The Third Wave. New York: Bantam Books, 1980 [In English].
9. Yousef A.M.F., Alshamy A., Tlili A., Metwally A.H.S. Demystifying the New Dilemma of Brain Rot in the Digital Era: A Review. Brain Sci. 2025; 15:283 [In English]. https://doi.org/10.3390/brainsci15030283.

About the author

Anton V. VASILENKO. Independent Researcher. https://orcid.org/0009-0004-7575-838. Address: Moscow, Russian Federation. anton.vasilenko25@gmail.com

Contribution of the author

The author declares no conflicts of interests.

Article info

Received: July 11, 2025. Approved after review: October 10, 2025. Accepted for publication: November 20, 2025. Published: December 1, 2025.

The author has read and approved the final manuscript.

Peer review info

«Russia & World: Scientific Dialogue» thanks the anonymous reviewers for their contribution to the peer review of this work.