Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

# Legal Aspects of Regulating Deepfake Usage in the Face of Contemporary Challenges and Threats

**Yugay LYUDMILA**[1]

Academy of the Republic of Uzbekistan

**ARTICLE INFO**

***Article history:***
Received June 2025
Received in revised form
15 July 2025
Accepted 15 July 2025
Available online
25 August 2025

***Keywords:***
artificial intelligence,
machine learning,
cybercrime,
political manipulation,
pornographic deepfakes,
legal responsibility.

**ABSTRACT**

This paper examines the relevance of research and study of the use of Deepfake technology in the era of digitalization. Statistical indicators of the Republic of Uzbekistan on the dynamics of crimes in the digital sphere are analyzed. The experience of the USA, China, Great Britain, Australia, South Korea and other countries in regulating the use of deepfakes is examined. Based on the study of the opinions of scientists, advanced foreign experience, legislation and law enforcement practice, recommendations for improving this area are formulated.


DOI: https://doi.org/10.47689/2181-1415-vol6- iss4-pp8-16


# Zamonaviy tahdidlar va chaqiriqlar sharoitida Dipfeyk texnologiyasidan foydalanishni huquqiy tartibga solishning ayrim masalalari

***Kalit so‘zlar:***
sun’iy intellekt,
mashina yordamida o‘qitish,
kiberjinoyatchilik,
siyosiy manipulyatsiyalar,
pornografik dipfeyklar,
yuridik javobgarlik.

**ANNOTATSIYA**

Ushbu ishda raqamlashtirish davrida Dipfeyk texnologiyasidan foydalanishni tadqiq etish va o‘rganishning dolzarbligi ochib beriladi. O‘zbekiston Respublikasining raqamli sohadagi jinoyatlar dinamikasi bo‘yicha statistik ko‘rsatkichlari tahlil qilinadi. AQSH, Xitoy, Buyuk Britaniya, Avstraliya, Janubiy Koreya va boshqa davlatlarning dipfeyklardan foydalanishni tartibga solish bo‘yicha tajribasi o‘rganiladi. Olimlarning fikrlari, ilg‘or xorijiy tajriba, qonunchilik va huquqni qo‘llash amaliyotini o‘rganish asosida ushbu sohani takomillashtirish bo‘yicha tavsiyalar ishlab chiqilgan.

[1] Doctor of law (DSc), Associate Professor, Law Enforcement Academy of the Republic of Uzbekistan.
E-mail: yugai.lyudmila@mail.ru

# Некоторые вопросы правового регулирования использования дипфейков в условиях современных вызовов и угроз

***Ключевые слова:***
искусственный интеллект, машинное обучение, киберпреступность, политические манипуляции, порнографические дипфейки, юридическая ответственность.

**АННОТАЦИЯ**

В работе раскрывается актуальность исследования и изучения использования технологии Дипфейк в условиях эпохи цифровизации. Анализируются статистические показатели Республики Узбекистан по динамике преступлений в цифровой сфере. Проводится анализ опыта США, Китая, Великобритании, Австралии, Южной Кореи и других стран по регулированию использования дипфейков. Исходя из изучения мнения ученых, передового зарубежного опыта, законодательства и правоприменительной практики сформулированы рекомендации по совершенствованию данной сферы.

## ВВЕДЕНИЕ

Статья 31 обновлённой Конституции Республики Узбекистан впервые закрепляет право каждого на защиту своих персональных данных. Статья 33 возлагает на государство обязанность создавать условия для обеспечения доступа к всемирной информационной сети Интернет [1], что значительно расширяет и укрепляет цифровые права граждан.

Согласно данным Global Digital 2025, в начале 2025 года в мире насчитывается **5,56 млрд.** интернет-пользователей, что соответствует уровню проникновения в **67,9%.** За 2024 год количество пользователей увеличилось на 136 миллионов (+2,5%) [2].

Вместе с тем, в соответствии с ежегодным отчетом о цифровом пространстве страны аналитической платформы Datareportal Digital 2025: Uzbekistan количество интернет-пользователей в Узбекистане достигло **32,7 млн.** человек, что составляет **89 %** от всего населения республики. При этом, по сравнению с прошлым годом рост составил **626 тысяч** человек [3].

Цифровизация всех сфер жизни населения, с одной стороны, предоставляет такие преимущества, как получение банковских, государственных, медицинских и других услуг в удалённом режиме, экономию времени, расширение доступа к сервисам и минимизацию коррупционных рисков. С другой стороны, возрастает утечка персональных данных, содержащихся в информационных базах; эти данные могут подвергаться модификации, увеличиваются риски совершения киберпреступлений и возникают другие угрозы.

В Республике Узбекистан за 2024 год было зафиксировано более **12 млн.** попыток совершения кибератак, в то время как в 2023 году этот показатель составил порядка **11 млн**.

Согласно данным МВД, за последние пять лет в Узбекистане зафиксирован рост киберпреступности – с **863 случаев** в 2019 году до почти **59 тысяч** в 2024-м. Только за последний год число таких преступлений увеличилось в **9 раз**, а их доля в общей структуре преступности выросла **с 6,2% до 44,4%** [4].

На сегодняшний день в Республике Узбекистан участились случаи распространения дипфейков. Происхождение термина «дипфейк» (deepfake) берет начало от двух английских слов: deep learning – «глубокое обучение» и fake – «фальшивый». В большинстве случаев в основе метода лежат генеративно-состязательные нейросети. Дипфейк представляет сгенерированную аудио- или видеозапись реальных людей, которые имеют практически неотличимый от оригинала черты лица, голос, манеры, акцент и т.д.

С учетом распространения во многих государствах мира, сопутствующих рисков и угроз, на сегодняшний день вопрос дипфейков является предметом исследования таких ученых, как Christopher Doss, Jared Mondschein, Dule Shu, Tal Wolfson, Denise Kopecky, Valerie A. Fitton-Kane, Lance Bush, Conrad Tucker [5], Bahar Uddin Mahmud, Afsana Sharmin [6, P.13-23], М.Б. Добробаба [7, С.112-119], И.Н. Архипцев, А.Н. Александров, А.В. Максименко, К.И. Озеров [8, С.69-74], М.А. Фалалеев, Н.А. Ситдикова, Е.Е. Нечай [9, С. 101-106], М.А. Желудков, А.П. Алексеева [10 С.159-169] и других ученых.

**ОСНОВНАЯ ЧАСТЬ**

Специалисты отмечают наиболее известные примеры противоправного использования технологии дипфейков:

– создание порнографических видео (98% дипфейков носит порнографический характер, на десяти самых известных специализированных платформах количество просмотров порнографических дипфейков составляет свыше 303 млн, 99% порнографических дипфейков создаются с участием женских персонажей) [11];

– создание аудио- и видеозаписей в целях совершения мошенничества или вымогательства [12, С. 106-113];

– политические манипуляции.

Ущерб от преступлений с использованием дипфейков более существенный по сравнению с традиционными видами преступлений. Последствия от них могут быть экономическими, политическими, репутационными, моральными и т.д.

При этом если первые дипфейки в Узбекистане в большинстве случаев преследовали **мошеннические цели**, то последние с участием известных медийных лиц, спортсменов, политиков, бизнесменов и других несут в ряде случаев попытки **политических манипуляций** [13], что несомненно может повлиять на состояние общественного порядка, могут нанести ущерб законным правам и интересам граждан, а также поставить под угрозу национальную безопасность и социальную стабильность.

Одним из важнейших направлений государства по противодействию использованию дипфейков в злонамеренных целях является совершенствование соответствующей правовой базы.

**ЗАРУБЕЖНЫЙ ОПЫТ**

**В США TAKE IT DOWN Act** (закон от 19 мая 2025 г.) требует от онлайн платформ и веб-сайтов незамедлительного удаления порнографических дипфейков, размещенных без согласия лица. Нарушители обязаны возместить ущерб и подлежат уголовному наказанию, включая тюремное заключение и/или штраф. Угрозы опубликования интимных визуальных изображений субъекта также запрещены законом и подлежат уголовному наказанию.

Платформы должны установить процедуры, посредством которого субъекты интимных визуальных изображений могут уведомить платформу об их существовании и запросить удаление данного контента, который был опубликован без согласия субъекта. Онлайн платформы должны удалить такие изображения в течение **48 часов** с момента уведомления. Согласно законопроекту, охваченные платформы определяются как публичные веб-сайты, онлайн-сервисы или приложения [14].

Еще в 2018 г. в Калифорнии был приняты законы **AB 602** (Assembly Bill No. 602) и **AB 730** (Assembly Bill No. 730), закрепляющие запрет на создание и распространение дипфейков, использующих изображения людей в порнографическом контексте без их согласия, а также с целью причинения вреда, обмана или манипуляции, особенно в контексте порнографии и политических выборов [15]. В законе Калифорнии не используется слово deepfake, но ответственность предусматривается за «подделки, созданные с помощью ИИ, а также видеоролики, вводящие в заблуждение, чтобы выставить кого-то в негативном свете».

**Справочно:** 22 января 2024 года Генеральная прокуратура штата Нью-Гэмпшир начала расследование по факту рассылки автоматических голосовых сообщений (так называемых «робозвонков»), полученных тысячами жителей штата С. Крамером. Голос президента США Д. Байдена в записанных сообщениях был клонирован с использованием нейросетевого алгоритма. Статья RSA 659:40, III (уголовное нарушение, связанное с подавлением избирательной активности) определяет, что «Никто не должен заниматься подавлением избирательной активности, сознательно пытаясь предотвратить или удержать другого человека от голосования или регистрации для голосования на основании мошеннической, обманчивой, вводящей в заблуждение или ложной информации». Было зарегистрировано 13 административных правонарушений по статье RSA 666:7-a (имитация кандидата). По решению Федеральной комиссии по связи США телекоммуникационная компания Lingo Telecom, оборудование которой использовалось для совершения роботизированных звонков, выплатила штраф. Выдвинуто обвинение в отношении С. Крамера, оценив размер штрафа в 6 миллионов долларов [16].

В **Сингапуре** в 2019 принят закон, направленный на защиту от дипфейков **POFMA (Protection from Online Falsehoods and Manipulation Act)** [17]

Данный Закон о защите от онлайн-лжи и манипуляций (POFMA) запрещает распространение онлайн-ложных утверждений о фактах или вводящей в заблуждение информации.

**Китай** стал одним из первых внедрил специальные меры по регулированию распространения дипфейк-контента. Предусмотрена обязательная маркировка, что позволяет распознавать подделки и снижает вероятность распространения дезинформации.

С 1 января 2020 г. введена **уголовная ответственность** за распространение дипфейков **без соответствующей маркировки**. Исполнение данного требования контролируется Администрацией киберпространства Китая.

В ноябре 2022 г. были приняты **Положения об управлении глубоким синтезом информационных сервисов в Интернете** [18], в положениях законов **«О кибербезопасности», «О безопасности данных», «О защите личной**

**информации», «Об управлении информационными службами Интернета»** и нормативно-правовых актов КНР закреплены запреты на использование дипфейков в целях угрозы национальной безопасности и интересам, для нанесения ущерба имиджу нации, посягательства на общественные интересы, нарушения экономического и социального порядка или посягательства на законные права и интересы других лиц.

**Положение об управлении глубоким синтезом информационных сервисов в Интернете содержат следующие положения:**

– компании должны получить согласие людей, прежде чем создавать дипфейки, и они должны подтвердить подлинность настоящих личностей пользователей;

– поставщики услуг должны создать и усовершенствовать механизмы опровержения слухов;

– созданные дипфейки не могут быть использованы для осуществления деятельности, запрещенной законами и административными нормами;

– поставщики услуг глубокого синтеза должны добавлять подпись или водяной знак, чтобы показать, что работа является синтетической, чтобы избежать путаницы или неправильной идентификации среди общественности [19].

В **Европейском Союзе** рассматриваются правила, связанные с искусственным интеллектом, которые могут охватывать дипфейки. В частности, проект **Artificial Intelligence Act 2024** (Регламент о ИИ) [20] включает понятие дипфейков, положения о высоких рисках, связанных с манипуляцией данными. Регламент допускает использование дипфейков, но определяет минимальные требования по соблюдению открытости и гласности. Создатели дипфейков обязаны маркировать свой контент. За нарушение регламента предусмотрены штрафы для органов, учреждений и агентств, а также поставщиков моделей ИИ.

**Digital Services Act (DSA)** (2024) определяют обязанность маркировки синтетического/манипулированного контента, например, водяным знаком или метаданными. DSA предоставляет право гражданам уведомлять платформу о незаконных дипфейках, и требует от платформ удалять или ограничивать доступ при подтверждении факта. Регуляторы получили инструменты принуждения, включая штрафы до 6 % глобального оборота, если платформы не противодействуют дипфейкам и другой дезинформации

В **Австралии** приняты законы, касающиеся дипфейков, с целью кибербуллинга, распространения порнографии без согласия, а также борьбы с дезинформацией [21]. **Criminal Code Amendment (Deepfake Sexual Material) Act 2024** устанавливает уголовную ответственность за распространение порнографических дипфейков посредством онлайн-сервисов. В качестве отягчающего вину обстоятельства выступает создание дипфейка и его распространение.

Во **Франции** предусмотрено уголовное наказание в виде тюремного заключения сроком на 1 год и штрафа в размере 15000 евро за публикацию любым способом фото- и видеоматериала, смонтированного со словами или изображением гражданина без его согласия, за исключением случаев, если представляется очевидным, что это монтаж, или об этом прямо упоминается.

В 2018 г. был принят **Закон о борьбе с манипулированием информацией**, который усиливает контроль над публикациями в социальных сетях и за работой иностранных СМИ, и в частности, позволяет зарегистрированному кандидату,

партии, или объединению граждан, потребовать в судебном порядке удалить из соцсетей или из СМИ информацию, которую они считают ложной. Суд должен рассмотреть в течение 48 часов жалобу и «приостановить распространение ложной информации».

В **Великобритании** принят в 2023 г. **Online Safety Act** (Закон о безопасности в Интернете), который охватывает защиту детей, кибербуллинг и домогательства, конфиденциальность и безопасность данных, а также другие области безопасности в Интернете. Один из разделов Закона о безопасности в Интернете запрещает обмен интимными изображениями с использованием дипфейков без согласия (Министерство юстиции, 2022 г.).

**Data (Use and Access) Act 2025** включает комплекс поправок – от доступа к данным до защиты через борьбу с дипфейками. В соответствии с данным нормативно-правовым документом за создание сексуально откровенных дипфейков без согласия, с целью получения удовольствия или причинения вреда предусматривается наказание в виде неограниченного штрафа.

В **Южной Корее** в соответствии с **Special Act on the Punishment of Sexual Crimes 2024** создание и распространение сексуальных дипфейков без согласия карается до 7 лет лишения свободы, вне зависимости от намерения распространять. При этом, покупка, хранение или просмотр таких дипфейков также признано преступлением, которое предусматривает наказание в виде заключения сроком до 3 лет или штрафа в размере до 30 миллионов корейских вон.

В **2023 году в Public Official Election Act** (Закон об избрании госслужащих) были добавлены изменения, запрещающие публикацию манипулятивных медиа, включая дипфейки, за 90 дней до выборов. Нарушения этого закона могут повлечь за собой наказание в виде тюремного заключения сроком до семи лет и штрафов в размере 50 миллионов вон. При этом, кампании обязаны раскрывать использование AI-контента.

В Государственной думе **Российской Федерации** рассматривается **Законопроект № 718538-8** предусматривающий использование дипфейков (изображение, голос, биометрические данные) как отягчающее обстоятельство при ряде преступлений: клевета (ст. 128.1), мошенничество (159), кража (158), вымогательство (163) и прочие.

Второй пакет мер по борьбе с кибермошенничеством предусматривает прямую уголовную ответственность за дипфейк-деяния: за мошеннические действия с использованием ИИ может быть назначен штраф в размере от 100 тыс. до 500 тыс. руб. Допускается и лишение свободы на срок до шести лет со штрафом до 80 тыс. руб. Если были украдены деньги с банковского счета с помощью нейросетей, то наказанием может стать тюремный срок от трех до восьми лет, а также штраф до 100 тыс. руб. Вымогательство с помощью ИИ влечет за собой взыскание от 100 тыс. до 500 тыс. руб. или лишение свободы до пяти лет. Злостное воздействие на информационные системы, компьютерную информацию или сети связи с использованием ИИ – штраф до 500 тыс. руб., лишение свободы до четырех лет.

Само по себе создание дипфейков не является противозаконным. В российской судебной практике имеются прецеденты признания дипфейков объектами авторского права [22]. Однако необходимо принимать во внимание что изображение лица охраняется в соответствии с нормами гражданского права. При создании и распространении дипфейков при распространении дипфейков с участием реальной личности необходимо также учитывать данные аспекты.

В **Казахстане** распространение заведомо ложной информации регулируется Законом «Об онлайн-платформах и онлайн-рекламе» 2023 г. Под ложной информацией понимается все, что искажает факты и вводит в заблуждение, создавая ложное представление о событиях, людях и явлениях.

Ответственность за фейки может быть как административной (по статье 456-2 КоАП), так и уголовной (статья 274 УК РК). Последняя предусматривает штраф 3 тыс. МРП, исправительные работы, общественные работы до 800 часов или лишение свободы на срок до 3 лет.

В **мае 2025 г**. Мажилис был одобрен в первом чтении законопроект **«Об искусственном интеллекте»**, который предусматривает меры ответственности за создание дипфейков. Согласно законопроекту использование ИИ является отягчающим обстоятельством. За создание и распространение дипфейков в Казахстане планируется введение административной ответственности (штрафах от 15 до 100 МРП).

Справочно: в июне т.г. в Казахстане были широко распространены носящие политический характер дипфейки с участием акима Костанайской области Кумара Аксакалова, акима Северо-Казахстанской области Гауеза Нурмухамбетова, акима СКО Гауеза Нурмухамбетова, депутата Сената Парламента РК от Восточно-Казахстанской области Ольги Булавкиной и т.д. [23]

В **Кыргызстане** в июне 2024 г. на официальном сайте Жогорку Кенеша опубликован проект закона, предусматривающего внесение изменений в действующие нормативные акты республики по противодействию угрозам, связанным с «дипфейками».

Законодательная инициатива направлена на защиту прав граждан и государственных интересов от рисков манипулирования общественным мнением, целенаправленной дискредитации и дезинформации.

**НАЦИОНАЛЬНАЯ ПРАКТИКА**

В **Республике Узбекистан** неоднократно поднимался вопрос о введении ответственности за использование искусственного интеллекта при совершении преступления.

В первом чтении прошел обсуждение в Законодательной палате Олий Мажлиса **проект Закона Республики Узбекистан «Об упорядочении отношений, возникающих в связи с использованием искусственного интеллекта»,** который определяет обязанность маркировки дипфейков и ответственности за незаконную обработку и распространение дипфейков [24].

Кроме того, прошел стадию общественного обсуждения **проект Закона Республики Узбекистан «О защите прав пользователей онлайн-платформ и веб-сайтов»**, который обязывает интернет-платформы оперативно удалять противоправный контент – фейковые новости, рекламу наркотиков или оскорбительные материалы. Законопроект усиливает конфиденциальность персональных данных. Платформы обязаны не предоставлять информацию о пользователях третьим лицам без их согласия.

**ЗАКЛЮЧЕНИЕ**

С учетом передового зарубежного опыта, законодательства и правоприменительной практики считаем целесообразным:

1. Предусмотреть за создание и распространение дипфейков без маркировки административную ответственность;

2. Совершение преступления (мошенничества, вымогательства, преступлений политической направленности и т.д.) с использованием дипфейков определить в качестве отягчающего вину обстоятельства;

3. Предусмотреть отдельную уголовную ответственность за создание и распространение порнографического дипфейка и обязать платформы незамедлительно их удалять (в течении 48 часов с момента обращения).

4. Предусмотреть ответственность цифровых платформ за размещение дипфейков без маркировки, чтобы пользователи могли идентифицировать такой контент. Обязать их использовать детекторы дипфейков перед размещением видео- и аудиоматериалов на своих ресурсах;

5. Необходимо четко прописать в ГК РУз, кто имеет права на использование образа и голоса человека, включая случаи, когда это касается умерших лиц (право на звук и изображение).

6. Внести уточнения в Закон Республики Узбекистан «О персональных данных», как технологии дипфейков соотносятся с законом о защите персональных данных, чтобы предотвратить использование изображений без согласия;

7. Разработать рекомендации и стандарты для использования технологий дипфейков в медиа и рекламе, чтобы обеспечить прозрачность и честность;

8. Включить в образовательные программы информацию о технологиях дипфейков, их возможностях и рисках, чтобы повысить осведомленность общества.

9. Создать регулирующий орган или комитет, который будет отслеживать использование технологий дипфейков и их влияние на общество. Эти изменения помогут создать более безопасную и этичную среду для использования технологий дипфейков.

**БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ:**

1. Конституция Республики Узбекистан. – Т.: Узбекистан, 2023. – С. 19-21.

2. URL: https://datareportal.com/reports/digital-2025-global-overview-report (дата доступа: 10.06.2025).

3. URL: https://datareportal.com/reports/digital-2025-uzbekistan (дата доступа: 10.06.2025).

4. Для представителей средств массовой информации и общественности организован пресс-тур, посвященный деятельности Центра кибербезопасности Оперативно-розыскного департамента Министерства внутренних дел Республики Узбекистан. URL: https://gov.uz/ru/iiv/news/view/57775. (дата доступа 10.03.2025).

5. Christopher Doss, Jared Mondschein, Dule Shu, Tal Wolfson, Denise Kopecky, Valerie A.Fitton-Kane, Lance Bush, Conrad Tucker. Deepfakes and scientifc knowledge dissemination // Scientific Reports. – volume 13, Article number: 13429 (2023). URL: https://www.nature.com/articles/s41598-023-39944-3.

6. Bahar Uddin Mahmud, Afsana Sharmin. Deep Insights of Deepfake Technology : A Review // DUJASE. – 2020. – Vol. 5. – (1 & 2). (January & July) – p.p. 13-23.

7. Добробаба М.Б. Дипфейки как угроза правам человека // LEX RUSSICA. – 2022. – Т.75. – № 11. – С. 112-119.

8. Архипцев И.Н., Александров А.Н., Максименко А.В., Озеров К.И. Порнографический дипфейк: вымысел или реальность? // Социально-политические науки. – 2021. – Т.11. – № 1. – С. 69-74.

9. Фалалеев М.А., Ситдикова Н.А., Нечай Е.Е. Дипфейк как феномен политической коммуникации // Вестник ЗабГУ. – 2021. – Т. 27. – № 6. – С. 101-106.

10. Желудков М.А., Алексеева А.П. Обеспечение защищенности биометрических персональных данных от использования в криминальных целях // Вестник Санкт-Петербургского университета МВД России. – 2025. – № 2 (106). – С. 159-169.

11. 2023 State of Deepfakes Realities, Threats and Impact. Режим доступа: URL: https://www.securityhero.io/state-of-deepfakes/. (дата доступа: 25.06.2025).

12. Долгиева М. М. Квалификация дипфейк-мошенничества и киберпохищения человека // Актуальные проблемы российского права. – 2024. – Т. 19. – № 11 (168). – С. 106-113.

13. Внимание, подделка! Появились дипфейк-видео от имени известных лиц с призывами вступать в российскую армию. URL: https://kun.uz/ru/87868316. (дата доступа: 25.06.2025).

14. S.146 - TAKE IT DOWN Act. URL: https://www.congress.gov/bill/119th-congress/senate-bill/146 (дата обращения: 29.03.2025).

15. URL: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=2019 2 0200AB730 (дата обращения: 29.03.2025).

16. Consultant behind deepfaked Biden robocall fined $6m as new charges filed. US elections 2024. Retrieved from https://www.theguardian.com/us-news/article/2024/ may/23/biden-robocall-indicted-primary

17. Introduction to Foreign Interference (Countermeasures) Act (FICA). URL: https://www.mha.gov.sg/fica (дата обращения 29.05.2025).

18. Положения об управлении углубленным синтезом информационных услуг Интернета. Документы департамента Государственного совета. Правительственная сеть Китая. URL: https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm (дата обращения: 12.04.2025).

19. URL: https://www.cac.gov.cn/2022-12/11/c_1672221949318230.htm

20. 2024 Регламент Европейского Союза об искусственном интеллекте, АНО «Цифровая экономика». URL: https://ai.gov.ru/knowledgebase/dokumenty-po-razvitiyu-ii-v-drugikhstranakh/2024_reglament_evropeyskogo_soyuza_ob_ iskusstvennom_intellekte_ano_cifrovaya_ekonomika_/ (дата обращения 29.04.2025).

21. Lexology Search. URL: https://www.lexology.com/ (дата обращения 29.08.2024)

22. Постановление Девятого арбитражного апелляционного суда по делу № А40-200471/2023. URL: https:// kad.arbitr.ru/Card/4d7f0305-69af-44fe-8841-a59e84aa7deb (дата обращения: 25.06.2025).

23. В Казахстане стремительно распространяются дипфейки. URL: https://stopfake.kz/ru/archives/24326. (Дата доступа: 07.06.2025.)

24. URL: https://www.youtube.com/watch?v=yca9K40eAfc&t=2705s