ВЕСТНИК ИНСТИТУТА ЗАКОНОДАТЕЛЬСТВА
И ПРАВОВОЙ ИНФОРМАЦИИ
РЕСПУБЛИКИ КАЗАХСТАН
НАУЧНО-ПРАВОВОЙ ЖУРНАЛ
ISSN 2788-5283
eISSN 2788-5291
ТОМ 81, НОМЕР 1(2026), 263-276

УДК 34.05
ГРНТИ 10.19.6
DOI 10.52026/2788-5291_2026_81_1_263
Научная статья

© Ю.А. Гаврилова[1*], Б.А. Умитчинова[2], Г.А. Мензюк[3], 2026
[1,2,3]Казахстанско-Американский свободный университет, Усть-Каменогорск, Казахстан
(e-mail: [1]gavriloyuliya@yandex.kz; [2]umitchinova.botagoz@mail.ru; [3]menzjuk@mail.ru)

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАРУБЕЖНЫХ ПРАКТИК ПРАВОВОГО РЕГУЛИРОВАНИЯ ДИПФЕЙКОВ (DEEPFAKES): БАЛАНС МЕЖДУ ИННОВАЦИЯМИ, ЗАЩИТОЙ ПРАВ ЧЕЛОВЕКА И ОБЕСПЕЧЕНИЕМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Аннотация. Статья посвящена сравнительному анализу зарубежных моделей правового регулирования дипфейков (deepfakes) в США, Европейском союзе, Китае и Республике Корея с целью выявления оптимальных подходов для формирования эффективной политики правового регулирования в Казахстане. На основе изучения нормативных актов, доктринальных источников и статистических данных исследуются основные угрозы, связанные с распространением синтетического медиаконтента: вмешательство в демократические процессы, репутационные риски, финансовое мошенничество, нарушение права на частную жизнь и защиту персональных данных. Особое внимание уделено анализу американских фрагментарных решений на уровне штатов, европейской модели превентивной прозрачности (GDPR, AI Act, Digital Services Act), а также азиатского технологического нормативизма, ярко выраженного в КНР, и норм уголовно-правовой защиты личности в Республике Корея. На основе сравнительного анализа выделены такие ключевые элементы эффективного регулирования, как обязательная маркировка синтетического контента, технические и организационные требования к разработчикам ИИ, прозрачные механизмы модерации, расширенные права субъектов данных и дифференцированная ответственность провайдеров. Формулируются предложения по развитию казахстанского законодательства с учетом принятия Закона РК «Об искусственном интеллекте» (2025). Уточнение механизмов модерации, закрепление специальных прав субъектов данных и детализация ответственности платформ создадут условия для сближения казахстанского регулирования синтетического медиаконтента с лучшими международными практиками, что позволит гармонично сочетать развитие инноваций, защиту прав человека и гарантии национальной безопасности.

Ключевые слова: дипфейки (deepfakes); правовое регулирование; искусственный интеллект; маркировка синтетического контента; национальная безопасность.

Введение

С каждым годом в мире возрастает количество правонарушений, связанных с deepfake-технологиями. По данным исследований английской компании Sumsub с 2022 по 2023 год, рост deepfake-подделок в Северной Америке составил 1740%, Азиатско-Тихоокеанском регионе - 1530%, Европе (включая Великобританию) 780%, на Ближнем Востоке и в Африке - 450%, Латинской Америке - 410%[1].

Несмотря на научно-технологический прогресс, связанный с развитием искусственного интеллекта, подобные технологии нейрофейки (deepfakes AI) представляют угрозу национальной безопасности обществу, государству, человеку.

Deepfakes AI подвергают опасности политические коммуникации в обществе через создание поддельных видео- и аудиосюжетов с участием лидеров государств, что может не просто ввести в заблуждение общественность, дезинформировать ее, но и расколоть общество, усилить межнациональный вопрос, «манипулировать реальным миром» [1]. Причем политические deepfakes снижают доверие населения к социальным сетям, а в долгосрочной перспективе могут негативно отразиться на гражданской онлайн-культуре населения [2]. Вышеуказанные причины послужили основанием признать deepfakes в США угрозой национальной безопасности на государственном уровне [3].

* автор для корреспонденции. E-mail: gavriloyuliya@yandex.kz.

[1] Sumsub Research: Global Deepfake Incidents Surge Tenfold from 2022 to 2023 // URL: https://sumsub.com/newsroom/sumsub-research-global-deepfake-incidents-surge-tenfold-from-2022-to-2023 (дата обращения: 02.07.2025).

Deepfakes представляют угрозу для физических и юридических лиц по средством нанесения репутационных атак и совершения финансового мошенничества. Так, по данным агентства Thomson Reuters в 2024 году в Южной Корее рассмотрено более 800 дел о сексуальных преступлениях с использованием deepfake видео. [4].

В последнем отчете организации Home Security Heroes отмечено, что в 2023 году количество фейковых видеороликов в интернете составило 95820, что на 550% больше, чем в 2019 году. Из них 98% составляют порнографические дипфейки[2].

Также распространенными стали случаи финансового мошенничества с имитацией голоса и внешности человека при проведении телефонных переговоров. Так, сотрудник международной компании, находящейся в Гонконге, перевел 23 млн евро мошенникам, создавшим с помощью искусственного интеллекта видеоролик с голосом его директора, якобы просившего перевести ему около 200 млн гонконгских долларов[3].

Таким образом, распространение deepfake-технологий несет комплексную угрозу государству, обществу, индивиду. При этом за последние годы прослеживаются усложнение и широкий охват сфер применения deepfake-технологий: от использования изображений, видео и аудио до политики, здравоохранения, финансов, транспорта, образования.

В рамках правового поля использование deepfake-технологий влечет возникновение новых вызовов, касающихся нарушения таких основополагающих прав и свобод человека, как право на частную жизнь, защиту персональных данных, чести и достоинства. Для правопорядка и правосудия дипфейки опасны сложностью раскрытия, расследования и квалификации таких преступлений. Очень часто следователи, судьи, адвокаты слабо подготовлены к работе с технологиями искусственного интеллекта. Более того, усиление степени общественной опасности, а также появление новых видов правонарушений, связанных с deepfake-технологиями, выявляет существенные пробелы, связанные с институтом ответственности.

С другой стороны, как отмечает Edvinas Meskys и др., технология дипфейка открывает безграничные возможности в творческих и научных целях для создания новых контентов. С этой позиции развитие и использование дипфейков является выражением свободы слова [5], что, в свою очередь, является гарантированным конституционным правом. Так, например, с помощью дипфейков оживают исторические личности, в музеях создаются виртуальные экскурсии. Дипфейки помогают создавать инструменты для людей с ограниченными возможностями – синтезировать голос для людей, потерявших речь. В законотворческой деятельности искусственный интеллект имеет большой потенциал [6]. Другими словами, положительное значение дипфейков имеет место там, где они служат полезным социальным, культурным, научным или экономическим целям. Поэтому «законодательная база должна быть хорошо сбалансирована» [7, с. 262].

Таким образом, важно не запретить технологию дипфейка, а создать баланс между ее законным использованием и «во» благо и недопущением ущемления прав человека с точки зрения правового регулирования. Необходим баланс между свободой выражения, правом на изображение и безопасностью, где под запрет попадают лишь вредоносные и манипулятивные формы deepfake-контента. Законодателю предстоит выработать гибкий правовой механизм, который одновременно позволит развивать синтетические медиа в научных, художественных и образовательных целях и эффективно пресекать их злоупотребление.

Поиск такого баланса лежит в плоскости изучения наилучших зарубежных практик, на основе которых можно построить авторскую модель, полезную для Казахстана, где с учетом активного роста цифровизации

[2] State of Deepfakes. Realities, Threats, and Impact. 2023 // URL: https://www.securityhero.io/state-of-deepfakes/#key-findings (дата обращения: 04.08.2025).

[3] Angestellter fällt auf Deepfake-Videocall rein – und überweist 23 Millionen Euro // URL: https://www.welt.de/kmpkt/article249947774/Kriminalitaet-Angestellter-faellt-auf-Deepfake-Videocall-rein-und-ueberweist-23-Millionen-Euro.html (дата обращения: 07.08.2025).

угроза злоупотребления дипфейками становится проблемой национальной безопасности.

Материалы и методы

Материалы исследования включают нормативно-правовые акты зарубежных государств, регулирующие вопросы использования технологий искусственного интеллекта и синтетического медиаконтента, а также научные статьи, аналитические обзоры и статистические данные, характеризующие масштабы распространения и угрозы дипфейков. В качестве основного эмпирического массива использованы документы США (законодательство отдельных штатов), Европейского союза (GDPR, Artificial Intelligence Act, Digital Services Act), Китайской Народной Республики (Положения об управлении синтетическим контентом, 2023), Республики Корея (Act on Special Cases Concerning the Punishment of Sexual Crimes, Personal Information Protection Act), а также материалы международных исследовательских организаций и независимых аналитических центров.

Методологическая база исследования опирается на комплекс методов юридической науки. Ведущим является сравнительно-правовой метод, позволивший сопоставить модели регулирования дипфейков в США, ЕС и странах Азии, выявить общие принципы, различия и степень их применимости для Казахстана. Использован формально-юридический метод для анализа понятийного аппарата, а именно: категорий «синтетический контент», «генеративная система», «обязательная маркировка».

Использован метод моделирования, который выступает не просто вспомогательным инструментом, а ключевым методологическим механизмом, обеспечивающим переход от описания зарубежного опыта к обоснованию авторской правовой модели регулирования дипфейков как сложного межотраслевого цифрового явления.

Результаты и обсуждение

Одним из первых законодательных актов, направленных на борьбу с распространением дипфейков, стал принятый в 2019 году в штате Техас (США) Закон S.B. No. 751, который предусматривает уголовную ответственность за фальсификацию видео с намерением повлиять на результаты выборов[4].

1 января 2025 года в Калифорнии вступил в силу Закон о защите демократии от дипфейкового обмана (AB 2655), согласно которому в периоды, начинающиеся за 120 дней до выборов, платформы обязаны в течение 72 часов с момента сообщения об этом удалять существенно вводящий в заблуждение контент, включая сфальсифицированные аудио- или видеоматериалы, предназначенные для создания ложного впечатления о действиях или заявлениях политического кандидата с целью обмана избирателей или нанесения ущерба репутации кандидата[5].

Кроме борьбы с дипфейками на политическом уровне, отдельные штаты США принимают законодательство, направленное на борьбу с порнографическими нейрофейками. Так, например, в штатах Индиана, Техас и Вирджиния введены санкции, предусматривающие уголовную ответственность до одного года тюремного заключения за распространение порнографических дипфейков. А во Флориде, Южной Дакоте и Вашингтоне на законодательном уровне в определение детской порнографии включили понятие «дипфейки»[6]. В Луизиане с 1 августа 2023 года вступила в силу норма о наказании в виде лишения свободы на срок от 5 до 20 лет за дипфейк, изображающий несовершеннолетнего[7].

Таким образом, приведенные примеры показывают, что в США борьба с дипфейками осуществляется на уровне отдельных штатов, фрагментарно, охватывая в основном такие сферы, как выборы и борьба с порнографическими нейрофейками. Подобная модель регулирования обусловлена федеративным устройством и отсутствием единого федерального закона, комплексно охватывающего проблему.

Европейский союз выстраивает

[4] AN ACT relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election // URL: https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm (дата обращения: 07.09.2025).

[5] United States of America. Signed Defending Democracy from Deepfake Deception Act of 2024 (AB 2655) // URL: https://digitalpolicyalert.org/event/22654-signed-defending-democracy-from-deepfake-deception-act-of-2024-ab-2655 (дата обращения: 08.09.2025).

[6] States race to restrict deepfake porn as it becomes easier to create // URL: https://missouriindependent.com/2024/04/16/states-race-to-restrict-deepfake-porn-as-it-becomes-easier-to-create/ (дата обращения: 08.09.2025).

[7] Louisiana. §14:73.13. Unlawful deepfakes [Effective August 1, 2023] // URL: https://foundationra.com/deepfake-ai-laws/ (дата обращения: 09.09.2025).

более унифицированный и системный подход, интегрируя вопросы регулирования дипфейков в общеевропейское цифровое право, что проявляется в сочетании норм о защите персональных данных, ответственности онлайн-платформ и обязательных стандартов прозрачности цифрового контента.

Важным документом европейского цифрового права является Регламент ЕС 2016/679 GDPR[8], регулирующий вопросы, связанные с персональными данными. Хотя Регламент не содержит прямых норм, касающихся дипфейков, тем не менее его нормы будут применимы, если такие материалы содержат персональные данные, включая биометрические данные физического лица, например изображение или голос (статья 4 GDPR). Статьи 6, 9 Регламента требуют наличия оснований для обработки персональных данных, среди которых согласие субъекта данных на их обработку. Статья 17 GDPR устанавливает право субъекта требовать удаления своих персональных данных, включая возможные дипфейковые контенты.

Закон об искусственном интеллекте ЕС (Artificial Intelligence Act, 2024 г.) является первым обязательным для исполнения документом, где установлены общие правила использования ИИ в ЕС. В Законе находят отражение нормы, направленные на борьбу с дипфейками и некорректным использованием сгенерированного содержания искусственным интеллектом. Например, в пункте 4 статьи 50 прописано требование на указание генерации или модификации контента (изображение, видео, аудио) с помощью ИИ. В контексте нашего исследования важно отметить, что европейский цифровой законодатель не блокирует контент, а информирует потребителя о том, что это возможно дипфейк, сгенерированый искусственным интеллектом. То есть цифровое доверие, не запрещающее, а признающее искусственную природу дипфейка, является основой баланса между прогрессом и нормативными ограничениями в рамках европейского права. Можно сказать, что в ЕС формируется такая философия цифрового правового регулирования, которая основана на принципе превентивной прозрачности. Более того, прозрачность должна проявляться не только в обязательном требовании маркировки контента, но и в прозрачностьи надзора, на который указывает F.Romero Moreno, акцентируя внимание на борьбе с дипфейками [8]. По мнению исследователя, система, которая будет удалять дипфейк, должна быть прозрачна, т.е. автор должен знать, кто определил ложность контента, на каком основании, как можно проверить и оспорить это решение. Независимость надзора предусматривает создание негосударственных контрольных инструментов, принимающих решения о блокировке или удалении контента.

Ключевым актом в этом направлении является Акт о цифровых услугах (Digital Services Act, DSA, 2022), предусматривающий обязанности платформ маркировать, выявлять и реагировать путем удаления незаконного контента, включая deepfakes. F. Romero Moreno подчеркивает его особую актуальность «для крупных платформ и поисковых систем, которые должны активно противодействовать ”системным рискам”, связанным с дипфейками, и их потенциалу наносить ущерб демократическим процессам, открытому дискурсу и выборам посредством дезинформации» [8, с. 301-302]. При этом статьей 17 Акта о цифровых услугах предусмотрено, что, удаляя дипфейк, платформа обязана уведомить автора и указать правовое основание удаления. Как раз эта статья указывает на существование баланса между использованием технологий искусственного интеллекта в модерации цифрового контента и защитой прав пользователей. Онлайн-платформа не просто удаляет контент deepfake-материалов, а соблюдает процессуальные гарантии пользователей. В дополнение к этой статье приняты нормы, предусматривающие процедурные и институциональные гарантии, обеспечивающие справедливость, обжалование и прозрачность решений. Так, статьи 20-24 Акта устанавливают обязанность провайдеров создавать внутренние механизмы рассмотрения жалоб и обеспечивать возможность обжалования решений о модерации

[8] Общий регламент по защите данных ЕС (General Data Protection Regulation) // URL: https://gdpr-info.eu/art-6-gdpr (дата обращения: 10.09.2025).

контента (ст. 20–21); обязанность информировать пользователей о причинах удаления контента и их правах на защиту (ст. 22); предусматривают принцип пропорциональности при приостановлении обслуживания (ст. 23); требование ежегодной публичной отчетности о действиях по модерации контента и жалобах (ст. 24).

Совокупно эти положения закрепляют модель ответственного цифрового посредничества, при которой онлайн-платформы обязаны соблюдать стандарты прозрачности, правовую определенность и защиту фундаментальных прав пользователей, а их деятельность подлежит контролю как со стороны государства, так и со стороны общества.

В последние годы государства Азии формируют комплексные подходы к регулированию дипфейк-технологий как ответ на угрозы манипуляции общественным мнением, распространения дезинформации и нарушений прав личности. Несмотря на различия в правовых системах, региональная тенденция демонстрирует усиление государственного контроля, развитие норм об обязательной маркировке синтетического контента и введение уголовной ответственности за незаконное использование технологий искусственного интеллекта.

Наиболее развитое регулирование установлено в Китайской Народной Республике. С 10 января 2023 года вступили в силу Положения об управлении синтетическим контентом, Приказ № 12 Государственного управления интернет-информации Министерства промышленности и информатизации и Министерства общественной безопасности Китайской Народной Республики[9].

Данный акт закрепляет обязанность поставщиков сервисов, использующих технологии ИИ для создания или изменения изображений, видео или аудио, явно маркировать синтетический контент. В соответствии со статьей 17 любая deepfake-информация должна содержать указания об ее искусственном происхождении, а статья 6 прямо устанавливает: «Поставщикам и пользователям сервисов дипфейк-новостей запрещено использовать сервисы дипфейк для создания, воспроизведения, публикации или распространения ложной новостной информации». Более того, обязанность по внедрению механизмов экстренного (чрезвычайного) реагирования и общие требования к системам управления информационной безопасностью, которые включают обработку незаконного контента, предусмотрены статьями 7 и 13. Статья 7 требует наличия системы реагирования на чрезвычайные ситуации, а статья 13 описывает, как именно должно происходить удаление (обработка) незаконного контента и взаимодействие с государственными органами в таких случаях. Это требование тесно связано с целями, указанными в статье 3 («...обеспечения национальной безопасности и общественных интересов...») и общим запретом на распространение информации, создающей угрозу национальной безопасности или наносящей ущерб общественным интересам, закрепленным в статье 6. В КНР создана скоординированная структура государственных органов, ответственных за надзор и управление услугами глубокого синтеза с четким распределением полномочий (ст.3), мерами при рисках и безопасности (ст. 26).

Таким образом, китайская модель носит характер технологического нормативизма, так как государство сочетает административный надзор, технический контроль и обязательное маркирование контента, формируя систему превентивного управления рисками синтетических медиа. При этом ответственность провайдеров интегрирована в действующие Закон о кибербезопасности (2017) и Закон о безопасности данных (2021), что усиливает правовой статус регулирования рассматриваемой сферы.

Борьба с дипфейковым контентом является объектом регулирования Закона Южной Кореи - Act on Special Cases Concerning the Punishment of Sexual Crimes (2012)[10], который в 2020 году был дополнен нормами, связанными с мани-

[9] Положение об управлении синтетическим контентом. Приказ № 12 Государственного управления интернет-информации, Министерства промышленности и информатизации Китайской Народной Республики и Министерства общественной безопасности Китайской Народной Республики // URL: https://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm (дата обращения: 10.10.2025).

[10] Act on Special Cases Concerning the Punishment of Sexual Crimes (Republic of Korea, 2012) // URL: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=68812&type=part&key=9 (дата обращения: 15.10.2025).

пуляциями с медиа, имеющими сексуальный характер (ст. 14-2 «Распространение ложных видеопродуктов»). Закон признает их создание, распространение, владение, приобретение как серьезное сексуальное преступление, предусматривая уголовное наказание в виде максимального срока лишения свободы – 7 лет.

При этом правовую основу для борьбы с дипфейками заложил еще Закон Южной Кореи - Personal Information Protection Act, 2003 года[11]. В Законе, регулирующем сбор, использование и раскрытие личной информации, прямой термин «дипфейки» не упоминается, так как документ носит законодательный характер и устанавливает общие правила защиты данных. Однако этот документ борется с угрозами, которые несут дипфейки, устанавливая строгие требования к защите личной информации, предотвращению ее несанкционированного использования и обеспечению ее точности. В целом южнокорейская модель отличается акцентом на уголовно-правовой защите личности и рассматривает deepfake как разновидность цифрового насилия и посягательства на человеческое достоинство.

Сравнительный анализ американской, европейской и азиатских моделей правового регулирования дипфейков показывает, что разные системы опираются на различные методологические подходы к борьбе с дипфейками: от децентрализованного и фрагментарного регулирования в США до европейской системной модели превентивной прозрачности, далее - к жесткому государственно-технологическому нормативизму (КНР и Южная Корея). Несмотря на различные подходы, государства стремятся адаптироваться к вызовам искусственного интеллекта и обеспечить баланс между технологическим развитием, защитой прав человека и сохранением общественной безопасности.

Анализ зарубежного опыта правового регулирования дипфейков позволил сформировать авторскую модель, включающую такие основные требования, как:

- обязательное маркирование синтезированного контента;
- установление технических и организационных требований к разработчикам ИИ;
- прозрачные механизмы модерации;
- защиту прав субъектов данных;
- специализированные процедуры уведомления, апелляции и ответственности провайдеров.

В отличие от европейского подхода, имеющего более антропоцентрический подход, основанный на информировании пользователя о синтетической природе контента и обеспечении процессуальных гарантий пользователей, модераторов, авторская модель исходит из необходимости институционального управления рисками дипфейков в контексте соблюдения баланса между быстро развивающимися информационными технологиями, защитой прав человека и обеспечением национальной безопасности.

Заимствуя у азиатской модели элементы обязательной маркировки синтетического контента, а также усиленного требования к провайдерам, авторская модель не стремится к жесткому директивному технологическому контролю. Предлагается сохранить приоритет защиты прав субъектов данных и конституционных свобод, включая свободу выражения мнений.

При этом оригинальный вклад автора заключается в формировании многоуровневой системы дифференцированной ответственности, где государству необходимо формировать нормативно-институциональные условия, платформам следует обеспечить процедурную модерацию, а разработчики несут ответственность за проектирование безопасной архитектуры моделей, предусматривающей механизмы предотвращения генерации вредоносного синтетического контента, а также за правомерность и этичность использования обучающих данных, особенно содержащих биометрическую информацию.

Разработанная авторская модель регулирования дипфейков представляет собой практическое воплощение доктринального подхода, направленного на институциональное управление циф-

[11] Personal Information Protection Act (Republic of Korea, 2003) // URL: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01 (дата обращения:09.11.2025).

ровыми рисками при сохранении баланса между защитой прав человека, свободой выражения мнений и требованиями национальной безопасности. Важность современной правовой доктрины подчеркивал отечественный ученый-юрист Р.К. Сарпеков, поскольку «теоретические основы и научные концепции способствуют формированию оптимальной модели механизма правового регулирования общественных отношений в сфере использования цифровых технологий» [9].

Таким образом, предложенная модель представляет собой не компиляцию зарубежных практик, а самостоятельную конструкцию, адаптированную к казахстанской правовой системе.

Рассматривая правовое регулирование ИИ в РК, Н. Саулен, А.А. Макарцев, Д.Б. Тебаев отмечают, что «у Казахстана накоплен значительный опыт. Весь процесс цифровизации был обеспечен правовой основой…» [10, с.239]. Однако в настоящее время в Казахстане нет специального законодательного акта, направленного на борьбу с deepfake-контентом. В научной литературе отсутствует и единый концептуальный подход к пониманию правовой природы дипфейков. Это можно объяснить их междисциплинарным характером [11], высоким и быстрым уровнем технологического развития [12], различиями национальных моделей регулирования [13], вариативностью юридического определения дипфейка [14].

Отсутствие единого доктринального подхода и высокая вариативность правового осмысления дипфейков в мировой научной литературе не означают отсутствия нормативного реагирования на уровне национальных правовых систем. В этом контексте особый интерес представляет принятие в Республике Казахстан Закона «Об искусственном интеллекте» от 17 ноября 2025 года, который закладывает основы регулирования функционирования систем ИИ, включая технологии синтетического контента, и открывает новое поле для осмысления правового статуса дипфейков в национальном праве.

В проект Закона первоначально было введено понятие «генеративная система ИИ», а законодатель обязывал информировать пользователей о том, что результат является синтетическим и может вводить в заблуждение. Другими словами, речь шла о том, что обязательным маркирование является не для любого синтетического контента, что характерно для европейского принципа превентивной прозрачности, а только для того контента, который в результате использования генеративной системы «может ввести в заблуждение»[12]. Однако в текст Закона уже введено жесткое, прямое и обязательное требование маркировать синтетический контент: пункт 1 статьи 21 гласит «товары, работы и услуги произведены или оказываются с использованием систем искусственного интеллекта»[13]. Также Закон вводит понятие «синтетические результаты деятельности систем искусственного интеллекта - изображение, видео, аудио, тексты или их комбинации, созданные или измененные системой искусственного интеллекта, имитирующие внешность, голос, поведение физического лица или события, которые фактически не происходили» (ст.1)[14]. Таким образом, обязательная маркировка синтетического контента приблизила казахстанский закон к уровню европейских требований, предусмотренных Artificial Intelligence Act, 2024 г., что, в свою очередь, поддерживает развитие цифровых технологий посредством реализации принципа цифрового доверия.

Что касается установления технических и организационных требований к разработчикам ИИ, то Закон закладывает базовые принципы управления рисками (ст. ст. 4, 11, 18), безопасности и защищенности (ст. ст. 4, 11), ответственности и подконтрольности (ст. ст. 4, 11), но не дифференцирует требования к генеративным системам ИИ, создающим синтетические медиа. Это придает регулированию дипфейков общий, а не специали-

[12] Проект Закона Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК «Об искусственном интеллекте» // URL: https://online.zakon.kz/Document/?doc_id=34868071 (дата обращения: 10.11.2025).

[13] Закон Республики Казахстан от 17 ноября 2025 года № 230-VIII ЗРК «Об искусственном интеллекте» // URL: https://adilet.zan.kz/rus/docs/Z2500000230 (дата обращения: 18.11.2025).

[14] Там же.

зированный характер. Предлагаем дополнить Закон *статьей о регулировании дипфейков, предусматривающую не только обязанность маркировки синтетических медиа, имитирующих внешность человека, но и признаки дипфейкового контента, требования к удалению дипфейков.*

Следующий элемент нашей модели - прозрачные механизмы модерации - отражается в п.3 ст. 4 и ст. 7 Закона РК «Об искусственном интеллекте» на уровне принципов «прозрачности и объяснимости». Однако пока не закреплено прямо детализированных механизмов, связанных с процедурой модерации (кто и как выявляет дипфейки, как доказывается синтетический контент, вводящий в заблуждение, как удаляется подобный контент, внутренние процедуры рассмотрения жалоб и т.п.). Целесообразно предусмотреть в Законе *обязанность провайдеров выявлять дипфейковый-контент на основе утвержденных критериев и принимать меры по его удалению. Ввести нормы, связанные с порядком документирования решений по модерации контента, сроках реагирования.*

Защита прав субъектов данных, с точки зрения авторской модели, достаточно детально отражена в статьях 4, 10, 21 Закона РК «Об искусственном интеллекте», где подчеркивается важность принципа защиты конфиденциальности и данных. Вместе с тем, автономного специфичного набора прав, связанных с дипфейковым контентом, в рассматриваемом нормативном документе не прослеживается. Отсутствует четкая норма, регулирующая право на удаление дипфейка (как это предусмотрено ст. 17 GDPR), а также связанные с этим правом процедуры обращения субъекта с требованием удаления незаконного контента (как это отражено в DSA). Видится необходимым *установить требования к созданию внутреннего механизма рассмотрения жалоб пользователей по схеме: порядок подачи жалобы – сроки рассмотрения - право на обжалование.*

В контексте авторской модели актуальны положения Закона «Об искусственном интеллекте» об ответственности провайдеров (собственников/ владельцев) на всех этапах жизненного цикла ИИ, а также механизма возмещения вреда по аналогии с существующим гражданским законодательством РК. В то же время не прослеживается разграничение статусов разработчиков, поставщиков, модераторов контента, отсутствуют специальные составы правонарушений, касающиеся непредоставления маркировки, нарушения обязанности по информированию о синтетичном контенте и т.п. Уместно *разграничить в статьях 8, 24, 30 Закона ответственность разработчика модели - за архитектуру и обучающие данные; поставщика модели – за внедрение и модификацию; платформы-посредника – за распространение синтетического контента. Отдельной статьей закрепить такой состав правонарушения, как отсутствие маркировки синтетического контента, создаваемого или распространяемого с использованием систем генеративного искусственного интеллекта.* Обозначенные предложения коррелируют с позицией казахстанского ученого-юриста Б.А. Аманжоловой о том, что на современном этапе развития правового регулирования в Республике Казахстан не введены специальные составы преступлений, связанные с применением искусственного интеллекта [15].

Предлагаемое разграничение ответственности между разработчиками моделей искусственного интеллекта, поставщиками и платформами-посредниками, а также введение самостоятельного состава правонарушения, связанного с отсутствием маркировки синтетического контента, отражает не только технический, но и институционально-правовой аспект защиты цифровой идентичности личности. В данном контексте маркировка выступает не просто элементом прозрачности алгоритмически генерируемого контента, а ключевым механизмом предотвращения несанкционированного вмешательства в цифровую идентичность гражданина.

Отсутствие маркировки лишает пользователей возможности распознавать синтетическую природу контента, что, в свою очередь, создает риск неконтролируемого воспроизведения и тиражирования цифровых образов

реальных лиц и подрывает контроль субъекта над собственной цифровой репрезентацией. Именно на этом акцентирует внимание F. Romero Moreno, подчеркивая «необходимость интеграции технических средств выявления синтетического контента и адаптивных правовых рамок для защиты прав человека и обеспечения доверия в цифровой среде» [8]. Тем самым подтверждается, что маркировка и механизмы правовой ответственности за ее отсутствие имеют не только технологическое, но и правозащитное значение.

При этом данная проблема не может рассматриваться исключительно в плоскости частноправовых обязанностей разработчиков и платформ. Она затрагивает более широкий институциональный уровень функционирования цифрового пространства, в рамках которого именно государство формирует базовые условия доверия к цифровым средам и инфраструктурам. В этой связи обоснованной представляется позиция A. Giannopoulou, согласно которой государство как гарант гражданской (цифровой) идентичности несет формальную ответственность за то, чтобы предоставляемая им инфраструктура цифровой идентичности не приводила к ограничению прав и возможностей граждан и, как следствие, к подрыву доверия к государственному сектору [16].

Данная позиция логически дополняет предлагаемую модель распределенной ответственности, поскольку подчеркивает, что введение обязательной маркировки синтетического контента и механизмов ответственности за ее отсутствие является не только задачей частных акторов (разработчиков и платформ), но и функцией публичной власти в рамках обеспечения целостности цифровой идентичности и доверия к государственным цифровым институтам. Казахстанский ученый Е.В. Мицкая справедливо подчеркивает, что невозможно остановить распространение фейковых новостей без вмешательства государства. Ни один частный субъект не в состоянии остановить распространение такого рода информации [17]. Следовательно, защита от немаркированного синтетического контента должна рассматриваться как элемент государственной политики в сфере цифровой идентичности и информационной безопасности, а не только как техническая или корпоративная обязанность участников рынка искусственного интеллекта.

Таким образом, Закон РК «Об искусственном интеллекте» интегрирует отдельные элементы модели превентивной прозрачности, сформированной под влиянием европейского и азиатского опыта, однако остается преимущественно общим технологически рамочным актом, а не специализированным инструментом комплексного регулирования дипфейков. Его развитие в направлении детализации процедур модерации, специальных прав субъектов данных и ответственности платформ позволит приблизить казахстанскую модель к современным международным стандартам регулирования синтетического медиаконтента, обеспечив баланс между развитием инноваций, защитой прав человека и обеспечением национальной безопасности Республики Казахстан.

Заключение

В результате проведенного анализа сформулируем основные выводы, полученные в статье:

– во-первых, правовое регулирование дипфейков в мире остается фрагментарным, что обусловлено междисциплинарной природой этого феномена, высокой технологической динамикой и вариативностью его юридического определения;

– во-вторых, Закон Республики Казахстан «Об искусственном интеллекте» (2025) заложил институциональные основы регулирования синтетического контента, однако требует специализированных норм, направленных именно на противодействие дипфейкам;

– в-третьих, обязательная маркировка синтетического контента должна рассматриваться не только как инструмент прозрачности, но и как механизм защиты цифровой идентичности личности, поскольку немаркированные дипфейки создают высокие риски несанкционированного использования цифрового образа физического лица;

– в-четвертых, эффективное регули-

рование дипфейков невозможно без дифференциации ответственности разработчиков моделей ИИ, поставщиков решений и платформ-посредников на основе распределения рисков на всех стадиях жизненного цикла искусственного интеллекта. При этом государство в условиях цифровизации должно выступать гарантом защиты цифровой идентичности граждан;

– в-пятых, предлагаемая авторская модель представляет собой адаптированную для Казахстана нормативную конструкцию, сочетающую элементы европейской прозрачности, азиатской превентивности и оригинальный подход к защите цифровой идентичности как объекта правовой охраны, что позволит обеспечить баланс между технологическим развитием, правами человека и требованиями национальной безопасности.

Список литературы:

1. Karnouskos S. Artificial Intelligence in Digital Media: The Era of Deepfakes // IEEE Transactions on Technology and Society. 2020. Vol. 1. № 3. P. 138–147.

2. Vaccari C., Chadwick A. Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news // Social Media + Society. 2020. Vol. 6. № 1. Available from: https://doi.org/10.1177/2056305120903408.

3. Добробаба М.Б. Дипфейки как угроза правам человека // Lex Russica. 2022. № 11 (192). С. 1–15. Режим доступа: https://cyberleninka.ru/article/n/dipfeyki-kak-ugroza-pravam-cheloveka (дата обращения: 10.09.2025).

4. Yim H. South Korea to criminalise watching or possessing sexually explicit deepfakes // Reuters. 2024. Режим доступа: https://www.reuters.com/world/asia-pacific/south-korea-criminalise-watching-or-possessing-sexually-explicit-deepfakes-2024-09-26 (дата обращения: 03.10.2025).

5. Meskys E., Kalpokienė J., Jurcys P., Liaudanskas A. Regulating Deep Fakes: Legal and Ethical Considerations // Journal of Intellectual Property Law & Practice. 2020. Vol. 15. Issue 1. P. 24–31. Режим доступа: https://ssrn.com/abstract=3497144 (дата обращения: 15.10.2025).

6. Аубакирова И.У., Молдабеков Б.С. Внедрение технологии искусственного интеллекта в законотворческую деятельность: современные вызовы, риски и перспективы // Вестник Института законодательства и правовой информации Республики Казахстан. 2024. № 1 (76). Режим доступа: https://cyberleninka.ru/article/n/vnedrenie-tehnologii-iskusstvennogo-intellekta-v-zakonotvorcheskuyu-deyatelnost-sovremennye-vyzovy-riski-i-perspektivy (дата обращения: 29.01.2026).

7. Łabuz M. Regulating Deep Fakes in the Artificial Intelligence Act // ACIG. 2023. Vol. 2. № 1. P. 252–291.

8. Romero Moreno F. Generative AI and deepfakes: a human rights approach to tackling harmful content // International Review of Law, Computers & Technology. 2024. Vol. 38. № 3. P. 297–326.

9. Сарпеков Р.К. Цифровизация правового пространства // Вестник Института законодательства и правовой информации Республики Казахстан. 2020. № 4 (62). Режим доступа: https://cyberleninka.ru/article/n/tsifrovizatsiya-pravovogo-prostranstva-1 (дата обращения: 29.01.2026).

10. Нуржан С., Макарцев А.А., Тебаев Д.Б. Применение инструментов искусственного интеллекта в законодательном процессе и классическая парадигма законотворчества: проблемы интеграции // Вестник Института законодательства и правовой информации Республики Казахстан. 2025. № 2 (80). С. 235–244.

11. Alanazi S., Asif S., Caird-Daley A. et al. Unmasking deepfakes: a multidisciplinary examination of social impacts and regulatory responses // Human-Intelligent Systems Integration. 2025. Article 00060. Режим доступа: https://link.springer.com/article/10.1007/s42454-025-00060-4 (дата обращения: 26.11.2025).

12. Johnson P. C., Laurell C., Ots M., Sandström C. Digital innovation and the effects of artificial intelligence on firms' research and development – Automation or augmentation, exploration or exploitation? // Technological Forecasting & Social Change. 2022. Vol. 179. Article 121636. DOI: https://doi.org/10.1016/j.techfore.2022.121636 (дата обращения: 26.11.2025).

13. Abbas F., Chesterman S., Taeihagh A. Building trust in the generative AI era: a systematic review of global regulatory frameworks to combat the risks of mis-, dis-, and mal-information // AI & Society. 2025. DOI: https://doi.org/10.1007/s00146-025-02698-9 (дата обращения: 26.11.2025).

14. Meškys E., Liaudanskas A., Kalpokienė J., Jurčys P. Regulating Deep Fakes: Legal and Ethical Considerations // Journal of Intellectual Property Law & Practice. 2020. Vol. 15. Issue 1. P. 24–31. Режим доступа: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3497144 (дата обращения: 26.11.2025).

15. Фазилов Ф.М., Аманжолова Б.А. Искусственный интеллект и уголовное право в Узбекистане и Казахстане // Universum: экономика и юриспруденция. 2025. № 10 (132). Режим доступа: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-ugolovnoe-pravo-v-uzbekistane-i-kazahstane (дата обращения: 29.01.2026).

16. Giannopoulou A. Digital Identity Infrastructures: a Critical Approach of Self-Sovereign Identity // Digital Society. 2023. Vol. 2. № 2. Article 18. DOI: https://doi.org/10.1007/s44206-023-00049-z (дата обращения: 26.11.2025).

17. Мицкая Е.В. Вопросы правового противодействия технологии deepfake // Российско-азиатский правовой журнал. 2025. № 1. Режим доступа: https://cyberleninka.ru/article/n/voprosy-pravovogo-protivodeystviya-tehnologii-deepfake (дата обращения: 29.01.2026).

© Ю.А. Гаврилова[1], Б.А. Умитчинова[2], Г.А. Мензюк[3], 2026
[1,2,3] Қазақстан-Американдық еркін университеті, Өскемен, Қазақстан
(e-mail: [1]gavriloyuliya@yandex.kz; [2]umitchinova.botagoz@mail.ru; [3]menzjuk@mail.ru)

ТЕРЕҢ ФЕЙКТЕРДІ ҚҰҚЫҚТЫҚ РЕТТЕУДІҢ ШЕТЕЛДІК ТӘЖІРИБЕЛЕРІН САЛЫСТЫРМАЛЫ ТАЛДАУ (DEEPFAKES): ИННОВАЦИЯ, АДАМ ҚҰҚЫҚТАРЫН ҚОРҒАУ ЖӘНЕ ҰЛТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ АРАСЫНДАҒЫ ТЕПЕ-ТЕҢДІК

Аннотация. Мақала Қазақстанда құқықтық реттеудің тиімді саясатын қалыптастыру үшін оңтайлы тәсілдерді анықтау мақсатында АҚШ, Еуропалық Одақ, Қытай және Корея Республикасындағы дипфейктерді (deepfakes) құқықтық реттеудің шетелдік модельдерін салыстырмалы талдауға арналған. Нормативтік актілерді, доктриналық дереккөздерді және статистикалық деректерді зерделеу негізінде синтетикалық медиа контенттің таралуына байланысты негізгі қауіптер зерттелінеді: демократиялық процестерге араласу, беделді тәуекелдер, қаржылық алаяқтық, жеке өмірге және жеке деректерге құқықты бұзу. Штат деңгейіндегі американдық фрагменттік шешімдерді, алдын алу ашықтығының еуропалық моделін (GDPR, AI Act, Digital Services Act), сондай-ақ ҚХР-да айқын көрсетілген азиялық технологиялық нормативизмді және Корея Республикасындағы жеке тұлғаны қылмыстық-құқықтық қорғау нормаларын талдауға ерекше назар аударылды. Салыстырмалы талдау негізінде синтетикалық контентті міндетті таңбалау, ЖИ жасаушыларға қойылатын техникалық және ұйымдастырушылық талаптар, модерацияның ашық тетіктері, деректер субъектілерінің кеңейтілген құқықтары және провайдерлердің сараланған жауапкершілігі сияқты тиімді реттеудің негізгі элементтері анықталады. «Жасанды интеллект туралы» (2025) ҚР Заңының қабылдануын ескере отырып, қазақстандық заңнаманы дамыту бойынша ұсыныстар тұжырымдалуда. Модерация тетіктерін нақтылау, деректер субъектілерінің арнайы құқықтарын бекіту және платформалардың жауапкершілігін нақтылау синтетикалық медиа контентті қазақстандық реттеуді үздік халықаралық тәжірибелермен жақындастыру үшін жағдай жасайды, бұл инновацияларды дамытуды, адам құқықтарын қорғауды және ұлттық қауіпсіздік кепілдіктерін үйлесімді ұштастыруға мүмкіндік береді.

Түйінді сөздер: дипфейктер (deepfakes); құқықтық реттеу; жасанды интеллект; синтетикалық мазмұнды таңбалау; ұлттық қауіпсіздік.

© Y.A. Gavrilova[1], B.A. Umitchinova[2], G.A. Menzyuk[3], 2026
[1,2,3]Kazakh-American Free University, Ust-Kamenogorsk, Kazakhstan
(e-mail: [1]gavriloyuliya@yandex.kz; [2]umitchinova.botagoz@mail.ru; [3]menzjuk@mail.ru)

COMPARATIVE ANALYSIS OF FOREIGN PRACTICES IN THE LEGAL REGULATION OF DEEPFAKES: BALANCING INNOVATION, HUMAN RIGHTS PROTECTION, AND NATIONAL SECURITY

Abstract. This article provides a comparative analysis of international models of deepfakes regulation in the United States, the European Union, China, and the Republic of Korea, with the aim of identifying optimal approaches for developing effective legal regulation policies in Kazakhstan. Based on regulatory documents, doctrinal sources, and statistical data, the article examines the main threats associated with the dissemination of synthetic media content: interference in democratic processes, reputational risks, financial fraud, and violation of privacy and personal data. Particular attention is paid to the analysis of fragmented state-level solutions in the United States, the European model of preventive transparency (GDPR, AI Act, Digital Services Act), as well as Asian technological norms, particularly pronounced in China, and criminal law protections in the Republic of Korea. Based on a comparative analysis, key elements of effective regulation are identified, including mandatory labeling of synthetic content, technical and organizational requirements for AI developers, transparent moderation mechanisms, expanded rights for data subjects, and differentiated responsibilities for providers. Proposals are formulated for the development of Kazakhstani legislation, taking into account the adoption of the Law of the Republic of Kazakhstan “On Artificial Intelligence” (2025). Clarifying moderation mechanisms, enshrining special rights for data subjects, and specifying platform responsibilities will create conditions for aligning Kazakhstani regulation of synthetic media content with best international practices, thereby harmoniously combining innovation, human rights protection, and national security guarantees.

Keywords: deepfakes; legal regulation; artificial intelligence; synthetic content labeling; national security

References:

1. Karnouskos S. Artificial Intelligence in Digital Media: The Era of Deepfakes // IEEE Transactions on Technology and Society. 2020. Vol. 1. № 3. P. 138–147.

2. Vaccari C., Chadshhick A. Deepfakes and disinformation: Ehploring the impact of synthetic political video on deception, uncertainty, and trust in neshhs // Social Media + Society. 2020. Vol. 6. № 1. Available from: https://doi.org/10.1177/2056305120903408.

3. Dobrobaba M.B. Dipfejki kak ugroza pravam cheloveka // Lex Russica. 2022. № 11 (192). S. 1–15. Rezhim dostupa: https://cyberleninka.ru/article/n/dipfeyki-kak-ugroza-pravam-cheloveka (data obrashhenija: 10.09.2025).

4. Yim H. South Korea to criminalise watching or possessing sexually explicit deepfakes // Reuters. 2024. Rezhim dostupa: https://www.reuters.com/world/asia-pacific/south-korea-criminalise-watching-or-possessing-sexually-explicit-deepfakes-2024-09-26 (data obrashhenija: 03.10.2025).

5. Meskys E., Kalpokienė J., Jurcys P., Liaudanskas A. Regulating Deep Fakes: Legal and Ethical Considerations // Journal of Intellectual Property Law & Practice. 2020. Vol. 15. Issue 1. P. 24–31. Rezhim dostupa: https://ssrn.com/abstract=3497144 (data obrashhenija: 15.10.2025).

6. Aubakirova I.U., Moldabekov B.S. Vnedrenie tehnologii iskusstvennogo intellekta v zakonotvorcheskuju dejatel'nost': sovremennye vyzovy, riski i perspektivy // Vestnik Instituta zakonodatel'stva i pravovoj informacii Respubliki Kazahstan. 2024. № 1 (76). Rezhim dostupa: https://cyberleninka.ru/article/n/vnedrenie-tehnologii-iskusstvennogo-intellekta-v-zakonotvorcheskuyu-deyatelnost-sovremennye-vyzovy-riski-i-perspektivy (data obrashhenija: 29.01.2026).

7. Łabuz M. Regulating Deep Fakes in the Artificial Intelligence Act // ACIG. 2023. Vol. 2. № 1. P. 252–291.

8. Romero Moreno F. Generative AI and deepfakes: a human rights approach to tackling harmful content // International Review of Law, Computers & Technology. 2024. Vol. 38. № 3. P. 297–326.

9. Sarpekov R.K. Cifrovizacija pravovogo prostranstva // Vestnik Instituta zakonodatel'stva i pravovoj informacii Respubliki Kazahstan. 2020. № 4 (62). Rezhim dostupa: https://cyberleninka.ru/article/n/tsifrovizatsiya-pravovogo-prostranstva-1 (data obrashhenija: 29.01.2026).

10. Nurzhan S., Makarcev A.A., Tebaev D.B. Primenenie instrumentov iskusstvennogo intellekta v zakonodatel'nom processe i klassicheskaja paradigma zakonotvorchestva: problemy integracii // Vestnik Instituta zakonodatel'stva i pravovoj informacii Respubliki Kazahstan. 2025. № 2 (80). S. 235–244.

11. Alanazi S., Asif S., Caird-Daley A. et al. Unmasking deepfakes: a multidisciplinary examination of social impacts and regulatory responses // Human-Intelligent Systems Integration. 2025. Article 00060. Available from: https://link.springer.com/article/10.1007/s42454-025-00060-4 (data obrashhenija: 26.11.2025).

10. Johnson P. C., Laurell C., Ots M., Sandström C. Digital innovation and the effects of artificial intelligence on firms' research and development – Automation or augmentation, exploration or exploitation? // Technological Forecasting & Social Change. 2022. Vol. 179. Article 121636. DOI: https://doi.org/10.1016/j.techfore.2022.121636 (data obrashhenija: 26.11.2025).

11. Abbas F., Chesterman S., Taeihagh A. Building trust in the generative AI era: a systematic review of global regulatory frameworks to combat the risks of mis-, dis-, and mal-information // AI & Society. 2025. DOI: https://doi.org/10.1007/s00146-025-02698-9 (data obrashhenija: 26.11.2025).

12. Meškys E., Liaudanskas A., Kalpokienė J., Jurčys P. Regulating Deep Fakes: Legal and Ethical Considerations // Journal of Intellectual Property Law & Practice. 2020. Vol. 15. Issue 1. P. 24–31. Rezhim dostupa: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3497144 (data obrashhenija: 26.11.2025).

13. Giannopoulou A. Digital Identity Infrastructures: a Critical Approach of Self-Sovereign Identity // Digital Society. 2023. Vol. 2. No. 2. Article 18. DOI: https://doi.org/10.1007/s44206-023-00049-z (data obrashhenija: 26.11.2025).

14. Meškys E., Liaudanskas A., Kalpokienė J., Jurčys P. Regulating Deep Fakes: Legal and Ethical Considerations // Journal of Intellectual Property Law & Practice. 2020. Vol. 15. Issue 1. P. 24–31. Rezhim dostupa: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3497144 (data obrashhenija: 26.11.2025).

15. Fazilov F.M., Amanzholova B.A. Iskusstvennyj intellekt i ugolovnoe pravo v Uzbekistane i Kazahstane // Universum: jekonomika i jurisprudencija. 2025. № 10 (132). Rezhim dostupa: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-i-ugolovnoe-pravo-v-uzbekistane-i-kazahstane (data obrashhenija: 29.01.2026).

16. Giannopoulou A. Digital Identity Infrastructures: a Critical Approach of Self-Sovereign Identity // Digital Society. 2023. Vol. 2. № 2. Article 18. DOI: https://doi.org/10.1007/s44206-023-00049-z (data obrashhenija: 26.11.2025).

17. Mickaja E.V. Voprosy pravovogo protivodejstvija tehnologii deepfake // Rossijsko-aziatskij pravovoj zhurnal. 2025. № 1. Rezhim dostupa: https://cyberleninka.ru/article/n/voprosy-pravovogo-protivodeystviya-tehnologii-deepfake (data obrashhenija: 29.01.2026).

Авторлар туралы мәліметтер:

Гаврилова Юлия Александровна – хат-хабарларға арналған автор, заң ғылымдарының кандидаты, қауымдастырылған профессор (доцент), Қазақстан-Американдық еркін университетінің профессоры, М.Горький көшесі, 76, 070000, Өскемен, Қазақстан.

ORCID: https://orcid.org/0000-0002-1096-4079;

Scopus Author ID: 57191410604;

E-mail: gavriloyuliya@yandex.kz.

Умитчинова Ботагоз Аспандиаровна – философия докторы (PhD), Қазақстан-Американдық еркін университетінің қауымдастырылған профессоры, М. Горький көшесі, 76, 070000, Өскемен, Қазақстан.

ORCID: https://orcid.org/0000-0003-4358-4459;

Scopus Author ID: 57697529500;

E-mail: umitchinova.botagoz@mail.ru.

Мензюк Галина Анатольевна – заң ғылымдарының кандидаты, БҒСБК доценті, Қазақстан-Американдық еркін университетінің профессоры, М. Горький көшесі, 76, 070000, Өскемен, Қазақстан.

ORCID: https://orcid.org/0000-0003-4597-7459;
E-mail: menzjuk@mail.ru.

Алғыс. Авторлар сарапшылық пікірі мен сындарлы көзқарасы үшін рецензенттерге алғыс білдіреді.

Дәйексөз келтіру үшін. Гаврилова Ю.А., Умитчинова Б.А., Мензюк Г.А**.** Терең фейктерді құқықтық реттеудің шетелдік тәжірибелерін салыстырмалы талдау (deepfakes): инновация, адам құқықтарын қорғау және ұлттық қауіпсіздікті қамтамасыз ету арасындағы тепе-теңді // Қазақстан Республикасының Заңнама және құқықтық ақпарат институтының Жаршысы. Ғылыми-құқықтық журнал. 2026;81(1). 263-276. DOI - https:// doi.org/10.52026/2788-5291_2026_81_1_263.

Авторлардың қосқан үлесі:

Гаврилова Ю. А. – қолжазба мәтінінің негізгі дамуын жүзеге асырды: мақала құрылымын дайындау, ғылыми мәселені тұжырымдау, әдебиеттер мен нормативтік дереккөздерді талдау, теориялық және аналитикалық бөліктерді жазу, қорытындылар мен ұсыныстарды қалыптастыру.

Умитчинова Б. А. – зерттеу идеясының авторы: ғылыми мәселені қоюға бастамашы болды, жұмыстың тұжырымдамасы мен жалпы зерттеу логикасын әзірледі, талдаудың негізгі бағыттары мен ғылыми жаңалығын анықтады.

Мензюк Г. А. – мәтінді ғылыми редакциялауды және түзетуді жүзеге асырды: мазмұнды және стилистикалық өңдеуді жүргізді, тұжырымдарды нақтылады, бөлімдердің логикалық байланысын және академиялық талаптарға сәйкестігін қамтамасыз етті.

Мүдделер қақтығысы туралы ақпарат. Авторлар мүдделер қақтығысының жоқтығын туралы мәлімдейді.

Қаржыландыру көзі. Авторлар зерттеу жүргізу кезінде қаржыландырудың жоқтығын туралы мәлімдейді.

Мақала редакцияға келіп түсті: 19.11.2025; рецензиялаудан кейін келіп түсті: 29.01.2025; басып шығаруға қабылданды: 31.03.2026.

Авторлар қолжазбаның соңғы нұсқасын оқып, мақұлдады.

Сведения об авторах:

Гаврилова Юлия Александровна – автор для корреспонденции, кандидат юридических наук, ассоциированный профессор (доцент), Казахстанско-Американского свободного университета, улица М.Горького, 76, 070000, Усть-Каменогорск, Казахстан.
ORCID: https://orcid.org/0000-0002-1096-4079;
Scopus Author ID: 57191410604;
E-mail: gavriloyuliya@yandex.kz.

Умитчинова Ботагоз Аспандиаровна – доктор философии (PhD), ассоциированный профессор Казахстанско-Американского свободного университета, улица М. Горького, 76, 070000, Усть-Каменогорск, Казахстан.
ORCID: https://orcid.org/0000-0003-4358-4459;
Scopus Author ID: 57697529500;
E-mail: umitchinova.botagoz@mail.ru.

Мензюк Галина Анатольевна – кандидат юридических наук, доцент ККСОН, профессор Казахстанско-Американского свободного университета, улица М. Горького, 76, 070000, Усть-Каменогорск, Казахстан.
ORCID: https://orcid.org/0000-0003-4597-7459;
E-mail: menzjuk@mail.ru.

Благодарности. Авторы выражают благодарность рецензентам за экспертное мнение и конструктивный подход.

Для цитирования. Гаврилова Ю.А., Умитчинова Б.А., Мензюк Г.А. Сравнительный анализ зарубежных практик правового регулирования дипфейков (deepfakes): баланс между инновациями, защитой прав человека и обеспечением национальной безопасности // Вестник Института законодательства и правовой информации Республики Казахстан. Научно-правовой журнал. 2026;81(1): 263-276. DOI – https:// doi.org/10.52026/2788-5291_2026_81_1_263.

Вклад авторов:

Гаврилова Ю.А. **–** осуществляла основную разработку текста рукописи: подготовка структуры статьи, формулировка научной проблемы, анализ литературы и нормативных источников, написание теоретической и аналитической частей, формирование выводов и рекомендаций.

Умитчинова Б.А. **–** автор идеи исследования: инициировала постановку научной проблемы, разработала концепцию и общую исследовательскую логику работы, определила ключевые

направления анализа и научную новизну.

Мензюк Г.А. – осуществляла научное редактирование и корректировку текста: проводила содержательную и стилистическую правку, уточняла формулировки, обеспечивала логическую связность разделов и соответствие академическим требованиям.

Информация о конфликте интересов. Авторы заявляют об отсутствии конфликта интересов.

Источник финансирования. Авторы заявляют об отсутствии финансирования при проведении исследования.

Статья поступила в редакцию: 19.11.2025; поступила после рецензирования: 29.01.2026; принята в печать: 31.03.2026.

Авторы прочитали и одобрили окончательный вариант рукописи.

Information about the authors:

Gavrilova Yuliya Aleksandrovna – corresponding authors, Candidate of Law, Associate Professor of the Kazakh-American Free University, 76, M. Gorky Street, 070000, Ust-Kamenogorsk, Kazakhstan.
ORCID: https://orcid.org/0000-0002-1096-4079;
Scopus Author ID: 57191410604;
E-mail: gavriloyuliya@yandex.kz.
Umitchinova Botagoz Aspandyarovna – PhD, Associate Professor of the Kazakh-American Free University, 76, M.Gorky Street, 070000, Ust-Kamenogorsk, Kazakhstan.
ORCID: https://orcid.org/0000-0003-4358-4459;
Scopus Author ID: 57697529500;
E-mail: umitchinova.botagoz@mail.ru.
Menzyuk Galina Anatolyevna – Candidate of Law, Associate Professor of CCES, Professor of the Kazakh-American Free University, 76, M. Gorky Street, 76, 070000, Ust-Kamenogorsk, Kazakhstan.
ORCID: https://orcid.org/0000-0003-4597-7459;
E-mail: menzjuk@mail.ru.

Acknowledgements The authors would like to express their gratitude to the reviewers for their expert opinions and constructive feedback.

For citation: Gavrilova Y.A., Umitchinova B.A., Menzyuk G.A. Comparative analysis of foreign practices in the legal regulation of deepfakes: balancing innovation, human rights protection, and national security» // Bulletin of Institute of Legislation and Legal Information of the Republic of Kazakhstan. Scientific and legal journal. 2026;81(1): 263-276. DOI – https:// doi.org/10.52026/2788-5291_2026_81_1_263.

Contribution of the authors:

Y. A. Gavrilova – was primarily responsible for the manuscript's development: preparing the article's structure, formulating the scientific problem, analyzing literature and regulatory sources, writing the theoretical and analytical sections, and formulating conclusions and recommendations.

B. A. Umitchinova – was the author of the research idea: she initiated the formulation of the scientific problem, developed the concept and overall research logic of the work, and defined the key areas of analysis and scientific novelty.

G. A. Menzyuk – was responsible for the scientific editing and proofreading of the text: she made substantive and stylistic corrections, clarified wording, ensured the logical coherence of the sections, and ensured compliance with academic requirements.

Conflict of interest statement. The authors declares that there is no conflict of interest.

Funding. The authors received no specific funding for this work.

Received: 19.11.2025; revised: 29.01.2026; accepted for publication: 31.03.2026.

The authors have read and approved the final manuscript.