Научная статья
УДК 34:004.8

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ДИПФЕЙКОВ: АНАЛИЗ ЗАРУБЕЖНОГО ОПЫТА И ПЕРСПЕКТИВЫ ДЛЯ РОССИИ И КАЗАХСТАНА

Гаврилова Ю. А., Умитчинова Б. А.
Казахстанско-Американский свободный университет, г. Усть-Каменогорск, Казахстан

Аннотация. *Статья посвящена сравнительному анализу зарубежных моделей правового регулирования дипфейков (deepfakes) в США, Европейском союзе, Китае с целью выявления оптимальных подходов для формирования эффективной политики правового регулирования в Российской Федерации и Республике Казахстан. 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 российского и казахстанского законодательства в сфере искусственного интеллекта.*

Ключевые слова: *дипфейки, правовое регулирование, искусственный интеллект, маркировка синтетического контента, национальная безопасность.*

LEGAL REGULATION OF DEEPFAKES: ANALYSIS OF FOREIGN EXPERIENCE AND PROSPECTS FOR RUSSIA AND KAZAKHSTAN

Gavrilova Yu. A., Umitchinova B. A.
Kazakhstan-American Free University, Ust-Kamenogorsk, Kazakhstan

Abstract. *The article is devoted to a comparative analysis of foreign models of legal regulation of deepfakes in the United States, the European Union, and China in order to identify optimal approaches for developing an effective legal regulatory policy in the Russian Federation and the Republic of Kazakhstan. Based*

on the comparative analysis, the following key elements of effective regulation are identified: mandatory labeling of synthetic content, technical and organizational requirements for AI developers, transparent moderation mechanisms, expanded rights of data subjects, and differentiated liability of providers. Proposals are formulated for the development of Russian and Kazakh legislation in the field of artificial intelligence.

Keywords: *deepfakes, legal regulation, artificial intelligence, synthetic content labeling, national security.*

В последние годы наблюдается расширение сфер применения технологий дипфейков – от создания изображений, аудио- и видеоконтента до использования в политике, здравоохранении, финансовом секторе, транспорте и образовании. При том, что дипфейковые технологии являются быстро и широко развивающимися, они одновременно являются малоизученными [1], хотя юридическая наука активно включается в изучение правовых инструментов, связанных с дипфейками, предлагая различные концепции их регулирования.

Для правовой системы использование дипфейков порождает новые вызовы, связанные с нарушением таких фундаментальных прав человека, как право на неприкосновенность частной жизни, защиту персональных данных, чести и достоинства. Для правоохранительных органов и судебной системы дополнительную сложность представляет выявление, расследование и правовая квалификация правонарушений, совершенных с применением технологий искусственного интеллекта. Существенным фактором остается недостаточная подготовленность следователей, судей и адвокатов к работе с цифровыми доказательствами и алгоритмами ИИ. Усиление общественной опасности подобных деяний и появление новых форм злоупотреблений выявляют пробелы в институтах юридической ответственности.

Вместе с тем их использование открывает широкие возможности для творчества, науки и инноваций, а в ряде случаев может рассматриваться как

форма реализации свободы выражения мнений [2]. С применением дипфейков воссоздаются образы исторических личностей, разрабатываются виртуальные музейные экспозиции, создаются вспомогательные технологии для лиц с ограниченными возможностями. «Так, определенным людям, потерявшим в результате болезни или аварии возможность разговаривать, данные приложения помогут синтезировать голос, практически не отличающийся от их натурального» [3].

Следовательно, ключевая задача правового регулирования дипфейков заключается не в запрете технологии как таковой, а в выработке баланса между ее легитимным использованием «во благо» и предотвращением нарушений прав и свобод человека. При этом, как отмечает Добробаба М. Б. «перед законодателем стоит задача разработать и внедрить комплекс мер, применение которых позволит минимизировать возможность нарушения прав граждан дипфейк-технологиями» [4].

Поиск оптимального баланса видится в анализе и обобщении зарубежного опыта правового регулирования дипфейков, на основе которого возможно определить правовые инструменты, а их совершенствование будет способствовать защите личных прав и интересов граждан, обеспечению безопасности и стабильности в информационном пространстве.

Одними из первых нормативных шагов, направленных на противодействие злоупотреблениям дипфейк-технологиями, стали меры, принятые в Соединенных Штатах Америки на уровне отдельных штатов. Так, в 2019 году в штате Техас был принят Закон S.B. No. 751, которым установлена уголовная ответственность за создание и распространение сфальсифицированных видеоматериалов с умыслом повлиять на исход избирательного процесса.

Дальнейшее развитие правового регулирования получило отражение в законодательстве штата Калифорния, где с 1 января 2025 года вступил в силу Закон о защите демократии от дипфейкового обмана (AB 2655). Указанный акт возлагает на онлайн-платформы обязанность в течение 72 часов с момента уведомления удалять контент, который в период за 120 дней до выборов является существенно вводящим в заблуждение.

Наряду с регулированием политических дипфейков, значительное внимание в США уделяется борьбе с порнографическими нейрофейками. В ряде штатов, включая Индиану, Техас и Вирджинию, установлена уголовная ответственность за распространение порнографических дипфейков, предусматривающая наказание в виде лишения свободы сроком до одного года. В таких штатах, как Флорида, Южная Дакота и Вашингтон, на законодательном уровне в понятие детской порнографии были включены дипфейковые материалы. Особенно жесткий подход реализован в Луизиане, где с августа 2023 года предусмотрено наказание в виде лишения свободы на срок от пяти до двадцати лет за создание или распространение дипфейков, изображающих несовершеннолетних.

Анализ указанных примеров свидетельствует о том, что в США правовое противодействие дипфейкам носит децентрализованный и фрагментарный характер, охватывая преимущественно сферы избирательных процессов и защиты от порнографических злоупотреблений. Подобная модель регулирования обусловлена федеративным устройством государства и отсутствием единого федерального закона, комплексно регулирующего использование дипфейк-технологий. Опережая законодательство, ряд IT-компаний (Google, Microsoft, Adobe) уже начали встраивать невидимые метки в генерируемые изображения и аудио, позволяющие впоследствии

обнаруживать их происхождение (подчеркивается важность «цифровых водяных знаков») [5].

В отличие от американского подхода, Европейский союз формирует более системную и унифицированную модель регулирования, интегрируя вопросы, связанные с дипфейками, в рамки общеевропейского цифрового права. Данная модель основывается на сочетании норм о защите персональных данных, обязанностях цифровых платформ и принципах прозрачности функционирования цифрового контента.

Ключевое значение в этом контексте имеет Регламент ЕС 2016/679 (GDPR), устанавливающий правовой режим обработки персональных данных. Хотя данный акт прямо не упоминает дипфейки, его положения применимы в тех случаях, когда такие материалы содержат персональные данные, включая биометрические характеристики – изображение лица или голос человека (статья 4 GDPR). Статьи 6 и 9 Регламента закрепляют требование наличия законных оснований для обработки персональных данных, в том числе согласия субъекта, а статья 17 предоставляет право требовать удаления соответствующей информации, что может распространяться и на дипфейковый контент.

Значительный вклад в формирование общеевропейского подхода внес Закон ЕС об искусственном интеллекте (Artificial Intelligence Act, 2024), являющийся первым обязательным нормативным актом, комплексно регулирующим использование ИИ. В числе прочего он содержит положения, направленные на противодействие недобросовестному использованию синтетического контента. Так, статья 50 (пункт 4) закрепляет обязанность указывать факт генерации или модификации изображений, видео- или аудиоматериалов с применением искусственного интеллекта. Принципиально важным является то, что европейский законодатель делает акцент не на

запрете такого контента, а на информировании пользователей о его искусственном происхождении. Этот первый всеобъемлющий акт о ИИ вводит риск-ориентированный подход: запрещает «неприемлемые» применения ИИ и устанавливает требования прозрачности.

Центральным нормативным актом, закрепляющим данные подходы, является Акт о цифровых услугах (Digital Services Act, DSA, 2022). Он устанавливает обязанности онлайн-платформ по выявлению, маркировке и удалению незаконного контента, включая дипфейки. Особая ответственность возлагается на крупные платформы и поисковые системы, которые обязаны активно противодействовать системным рискам, связанным с распространением дипфейков и их потенциальным воздействием на демократические процессы, публичный дискурс и избирательные кампании [5, с. 301-302].

При этом DSA закрепляет важные процессуальные гарантии защиты прав пользователей. Так, статья 17 обязывает платформы при удалении контента уведомлять его автора и указывать правовые основания принятого решения. Дополнительные статьи (20-24) предусматривают создание внутренних механизмов рассмотрения жалоб, возможность обжалования решений о модерации, обязанность информирования пользователей о причинах ограничений, соблюдение принципа пропорциональности при приостановлении сервисов, а также ежегодную публичную отчетность о практике модерации.

В совокупности данные нормы формируют модель ответственного цифрового посредничества, при которой онлайн-платформы действуют в условиях правовой определенности, транспарентности и подотчетности, обеспечивая защиту фундаментальных прав пользователей под контролем как государственных институтов, так и гражданского общества.

В последние годы государства Азиатского региона вырабатывают комплексные модели правового реагирования на распространение дипфейк-технологий, рассматривая их как источник угроз манипулирования общественным сознанием, дезинформации и нарушения прав личности. Несмотря на различия в правовых традициях и институциональных механизмах, в регионе прослеживается общая тенденция к усилению государственного участия в регулировании синтетических медиа, внедрению обязательных требований по идентификации искусственно сгенерированного контента, а также установлению уголовной ответственности за неправомерное использование технологий искусственного интеллекта.

Наиболее развитая и институционально выстроенная система регулирования сформирована в Китайской Народной Республике. С 10 января 2023 года в КНР действуют Положения об управлении синтетическим контентом, утвержденные совместным приказом Государственного управления интернет-информации, Министерства промышленности и информатизации и Министерства общественной безопасности (Приказ № 12). Указанный нормативный акт закрепляет комплекс обязательств для поставщиков услуг, использующих технологии искусственного интеллекта для создания или модификации аудио-, видео- и визуальных материалов.

Ключевым элементом регулирования является требование обязательной идентификации синтетического контента. В соответствии со статьей 17 Положений любая информация, созданная с применением технологий глубокого синтеза, должна сопровождаться четким указанием на ее искусственное происхождение. Одновременно статья 6 прямо запрещает использование дипфейк-сервисов для создания, воспроизведения или распространения ложной новостной информации. Тем самым китайский

законодатель закрепляет превентивный запрет на использование технологий глубокого синтеза в целях дезинформации.

Особое внимание уделяется институциональным и техническим механизмам управления рисками. Статьи 7 и 13 устанавливают требования по созданию систем экстренного реагирования, а также регламентируют процедуры выявления, обработки и удаления незаконного контента, включая взаимодействие с уполномоченными государственными органами. Эти нормы корреспондируют с целями регулирования, сформулированными в статье 3, где приоритет отдается защите национальной безопасности и общественных интересов, а также с общим запретом на распространение информации, способной нанести ущерб общественному порядку или государственным интересам. Дополнительно Положения предусматривают скоординированную систему государственного надзора с четким распределением компетенций между органами власти (ст. 3), а также специальные меры по управлению рисками и обеспечению информационной безопасности (ст. 26).

В целом китайский подход можно охарактеризовать как модель технологического нормативизма, при которой административный контроль, технические требования и обязательная маркировка контента интегрированы в единую систему превентивного управления синтетическими медиа. Ответственность провайдеров услуг глубокого синтеза дополнительно опирается на положения Закона о кибербезопасности (2017) и Закона о безопасности данных (2021), что придает регулированию устойчивый и комплексный характер. В целом, «подход законодателя Китая к регулированию дипфейков является наиболее оптимальным и отвечающим требованиям современности, а потому может стать примером построения национального правового регулирования этой сферы» [7].

Сопоставление правового регулирования дипфейков в США, ЕС, КНР свидетельствует о принципиальных различиях в методологических основаниях противодействия злоупотреблениям технологиями глубокого синтеза. В Соединенных Штатах регулирование носит преимущественно децентрализованный и сегментарный характер, реализуясь на уровне отдельных штатов и охватывая ограниченный круг наиболее социально чувствительных сфер. Европейский союз, напротив, формирует комплексную и унифицированную модель, основанную на принципах превентивной прозрачности, ответственности цифровых платформ и процессуальных гарантий защиты прав пользователей. Китайская Народная Республика демонстрирует более жесткий подход, характеризующийся высоким уровнем государственного вмешательства и сочетанием правовых, административных и технологических инструментов контроля.

Анализ зарубежных подходов к правовому регулированию дипфейков послужил основой для разработки определенных правовых инструментов, ориентированных на институциональное управление рисками синтетических медиа: обязательная идентификация синтезированного контента; установление технических и организационных требований к разработчикам систем искусственного интеллекта; формирование прозрачных процедур модерации; обеспечение защиты прав субъектов данных; а также внедрение специализированных механизмов уведомления, апелляции и ответственности цифровых посредников.

Проанализируем российское и казахстанское законодательство именно сквозь призму правового регулирования дипфейков, показывая, какие инструменты уже присутствуют имплементарно, а какие отсутствуют или требуют нормативного развития. Схематично анализ рассматриваемых критериев представлен в таблице.

Таблица – Сравнительно-правовой анализ правового регулирования дипфейков (США, ЕС, КНР, РФ, РК)

Правовые инструменты	США	ЕС	КНР	РК	РФ
Обязательная идентификация (маркировка) синтезированного контента	Фрагментарная: отдельные федеральные акты и акты штатов (в основном для политической рекламы и выборов); универсального требования нет	Обязательная маркировка синтетического контента в соответствии с Artificial Intelligence Act (2024); принцип превентивной прозрачности	Обязательная маркировка синтетического контента по «Положениям об управлении глубоким синтезом» (2023)	Обязательная маркировка товаров, работ и услуг, произведенных с использованием ИИ (ст. 21 Закона РК «Об ИИ», 2025)	Отсутствует универсальное требование; маркировка не закреплена нормативно
Технические и организационные требования к разработчикам ИИ	Ограниченные; акцент на саморегулирование и отраслевые стандарты	Дифференцированные требования в зависимости от уровня риска ИИ-систем (AI Act)	Жесткие требования к провайдерам ИИ, включая контроль обучающих данных и алгоритмов	Общие принципы управления рисками, безопасности и ответственности; нет специальных требований к генеративным системам	Отсутствуют специальные требования к разработчикам генеративных моделей
Прозрачные процедуры модерации синтетического контента	Определяются платформами; государство вмешивается точечно (misinformation, elections)	Регламентированы в DSA: обязанности платформ по выявлению, удалению и отчетности	Централизованная модель: платформы обязаны выявлять и удалять дипфейки	Принципы прозрачности и объяснимости закреплены, но процедуры модерации не детализированы	Модерация осуществляется по общим нормам; специальных процедур для дипфейков нет
Защита прав субъектов данных / цифровой идентичнос	Фрагментарная защита через privacy law и tort law; нет единого подхода	Развитая система прав (GDPR): право на удаление, информирование, защиту	Обязанность получения согласия лица на использова	Принцип защиты данных закреплен, но отсутствуют специальные	Общая защита чести, достоинства и персональны

ти		биометрии	ние и изменение биометрических данных	права на удаление дипфейков	х данных; цифровая идентичность не выделена
Механизмы уведомления и апелляции	Зависит от платформ; государственные гарантии минимальны	Обязательные механизмы уведомления и апелляции (DSA)	Централизованный контроль, жалобы рассматриваются через государственные механизмы	Отсутствуют специальные процедуры уведомления и апелляции по дипфейкам	Универсальных механизмов уведомления и апелляции не предусмотрено
Ответственность цифровых посредников	Ограниченная ответственность (Section 230 CDA); исключения – узкие	Дифференцированная ответственность платформ, разработчиков и провайдеров	Расширенная ответственность платформ и провайдеров	Ответственность провайдеров предусмотрена, но не разграничены роли разработчиков, поставщиков и платформ	Ответственность фрагментарная; специальные составы отсутствуют

В целом, российское и казахстанское законодательство в настоящее время не содержат специальных норм, прямо направленных на регулирование технологий дипфейков и иных форм синтетических медиа. Регулятивное воздействие осуществляется опосредованно – через совокупность норм гражданского, информационного, административного и уголовного права, что свидетельствует о фрагментарном и реактивном характере правового регулирования. Однако принятие Закона Республики Казахстан «Об искусственном интеллекте» от 17 ноября 2025 года знаменует собой важный этап в формировании правовых основ регулирования систем искусственного интеллекта, включая технологии генерации и модификации медиаконтента.

Впервые на уровне национального законодательства Казахстана закрепляется понятие *«синтетические результаты деятельности систем*

искусственного интеллекта», а в п. 1 ст. 21 Закона закреплено прямое и императивное требование маркировать товары, работы и услуги, произведенные или оказываемые с использованием систем искусственного интеллекта. С точки зрения обязательной идентификации (маркировки) синтезированного контента, действующее право не устанавливает универсальной обязанности по обозначению искусственно сгенерированных аудиовизуальных материалов. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» оперирует категорией достоверности информации и вводит обязанности по ограничению распространения противоправного контента, однако не разграничивает естественный и синтетический медиаконтент. Российские ученые Н. Ф. Бодров и А. К. Лебедева особо подчеркивают необходимость «установления обязанности технологических компаний и пользователей, создающих генеративный контент, использовать водяные знаки для маркирования контента в целях информирования иных лиц о генеративной природе контента» [5].

Таким образом, механизм маркировки, являющийся ключевым элементом зарубежных моделей регулирования дипфейков, в российском праве отсутствует, что затрудняет превентивное выявление манипулятивных материалов.

В части установления требований к разработчикам и поставщикам систем искусственного интеллекта российское регулирование также носит рамочный характер. Национальная стратегия развития искусственного интеллекта на период до 2030 года, утвержденная Указом Президента РФ от 10 октября 2019 г. № 490, и подготавливаемые подходы к регулированию ИИ ориентированы преимущественно на стимулирование инноваций, а не на институциональное управление рисками. Законодательство не содержит

специальных обязанностей для разработчиков генеративных моделей в части предотвращения создания дипфейков, внедрения технических средств обнаружения синтетического контента либо ведения учета его использования. В результате ответственность за последствия применения таких технологий фактически переносится на конечных пользователей или распространителей. Закон РК «Об искусственном интеллекте» закрепляет базовые принципы управления рисками, безопасности, ответственности и подконтрольности (статьи 4, 11, 18), однако данные положения носят общий характер и не дифференцируют требования применительно к генеративным системам, создающим синтетические медиа.

Отсутствие специализированных норм, адресованных именно разработчикам и поставщикам генеративных моделей, придает регулированию дипфейков рамочный, а не целенаправленный характер. В этой связи обоснованным представляется предложение о дополнении Закона РК специальной статьей, посвященной регулированию дипфейков, предусматривающей не только обязанность маркировки, но и критерии отнесения контента к дипфейковому, а также требования к его удалению.

Процедуры модерации контента в российской правовой системе возложены преимущественно на владельцев информационных ресурсов и цифровые платформы. Закон № 149-ФЗ и подзаконные акты предусматривают обязанности по удалению запрещенной информации, как и п. 3 ст. 4, ст. 7 Закона РК, однако не устанавливают специальных стандартов модерации именно дипфейков. Отсутствие нормативного разграничения между легальным синтетическим контентом и вредоносными дипфейками приводит к тому, что модерация осуществляется постфактум и в значительной степени на усмотрение платформ, без единых критериев и процедур. Соответственно, необходимо нормативно закрепить обязанность

провайдеров выявлять дипфейковый контент на основе утвержденных критериев, документировать решения по модерации и соблюдать установленные сроки реагирования. В данном контексте это позволит рассматривать маркировку как самостоятельный правовой инструмент защиты личности, обеспечивающий баланс между свободой использования технологий синтетических медиа и необходимостью предотвращения злоупотреблений, связанных с искажением идентичности и нарушением прав на персональные и биометрические данные [8].

С точки зрения защиты прав субъектов данных, российское законодательство предоставляет определенные механизмы, которые потенциально применимы к дипфейкам. Так, нормы гражданского права о защите чести, достоинства и деловой репутации, а также право на изображение гражданина (ст. 152 и 152.1 ГК РФ) могут использоваться для защиты лиц, чья цифровая репрезентация была искажена. Вместе с тем данные нормы разрабатывались для традиционных форм распространения информации и не учитывают специфику синтетического медиаконтента, включая сложность доказывания факта искусственной генерации и источника создания дипфейка. В сфере персональных и биометрических данных Федеральный закон «О персональных данных» формально охватывает изображения и голос как биометрические данные, однако не содержит специальных положений, регулирующих их трансформацию с использованием технологий глубокого синтеза. В отличие от китайского подхода, российское право не устанавливает прямой обязанности получения согласия лица на изменение его биометрических характеристик в процессе создания синтетического контента, что создает нормативный пробел в защите цифровой идентичности личности.

Защита прав субъектов данных занимает значимое место в Законе РК «Об искусственном интеллекте». В статьях 4, 10 и 21 подчеркивается приоритет защиты конфиденциальности и персональных данных. Вместе с тем Закон не формирует автономного набора прав, специфически ориентированных на защиту от дипфейков. В частности, отсутствует норма, закрепляющая право субъекта на удаление дипфейкового контента, аналогичное праву на удаление данных, предусмотренному ст. 17 GDPR, а также процедурные гарантии реализации данного права, сопоставимые с механизмами, предусмотренными Digital Services Act. Это свидетельствует о необходимости институционализации права на защиту цифровой идентичности в условиях распространения синтетических медиа.

Механизмы уведомления, апелляции и ответственности цифровых посредников в российском праве развиты преимущественно в контексте противоправной информации в целом. Законодательство предусматривает возможность блокировки ресурсов, удаления контента и привлечения к административной ответственности, однако не формирует специализированной процедуры рассмотрения споров, связанных с дипфейками, включая право субъекта на оперативное уведомление, обжалование решений модераторов и компенсацию причиненного вреда. Ответственность цифровых посредников носит ограниченный характер и, как правило, возникает лишь при неисполнении предписаний государственных органов.

С точки зрения ответственности, Закон РК «Об искусственном интеллекте» закрепляет общий принцип ответственности провайдеров на всех этапах жизненного цикла ИИ и допускает возмещение вреда по аналогии с гражданским законодательством. Однако в Законе отсутствует четкое

разграничение статусов и обязанностей разработчиков моделей ИИ, поставщиков решений и платформ-посредников.

Таким образом, анализ российского законодательства показывает, что отдельные элементы институционального управления рисками синтетических медиа присутствуют лишь фрагментарно и не образуют целостного правового механизма. Отсутствие нормативного определения дипфейка, обязательной маркировки, специальных требований к разработчикам ИИ и процедур защиты цифровой идентичности свидетельствует о необходимости перехода от косвенного регулирования к формированию самостоятельного правового режима синтетического медиаконтента. Именно в этом направлении представляется целесообразным развитие российской модели правового регулирования дипфейков с учетом зарубежного опыта и национальных правовых традиций.

Закон Республики Казахстан «Об искусственном интеллекте» интегрирует отдельные элементы модели превентивной прозрачности, сформированной под влиянием европейского и азиатского опыта, однако в целом остается рамочным технологическим актом, а не специализированным инструментом комплексного регулирования дипфейков. Его дальнейшее развитие в направлении детализации процедур модерации, закрепления специальных прав субъектов данных и дифференциации ответственности цифровых посредников позволит приблизить казахстанскую модель к современным международным стандартам и обеспечить баланс между развитием инноваций, защитой прав человека и требованиями национальной безопасности.

Сравнительный анализ показывает, что наиболее институционально выстроенные модели правового регулирования дипфейков сформированы в Европейском союзе и Китайской Народной Республике, где обязательная

маркировка, дифференцированная ответственность и процедурная прозрачность образуют целостный правовой механизм. Казахстанская модель занимает промежуточное положение, интегрируя элементы превентивной прозрачности, но сохраняя рамочный характер регулирования. Российская Федерация и США демонстрируют фрагментарный подход, основанный преимущественно на косвенном применении общих норм и саморегулировании, что снижает эффективность управления рисками синтетических медиа.

Библиография

1. Бодров Н. Ф., Лебедева А. К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования. 2023. № 11. URL: https://cyberleninka.ru/article/n/ponyatie-dipfeyka-v-rossiyskom-prave-klassifikatsiya-dipfeykov-i-voprosy-ih-pravovogo-regulirovaniya (дата обращения: 03.02.2026). DOI: 10.25136/2409-7136.2023.11.69014.

2. 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. URL: https://ssrn.com/abstract=3497144 (дата обращения: 04.02.2026). DOI:10.1093/jiplp/jpz167.

3. Токолов А. В. Правовое регулирование дипфейков // Вестник экономической безопасности. 2025. № 2. URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-dipfeykov (дата обращения: 05.02.2026). DOI: 10.24412/2414-3995-2025-2-141-147.

4. Добробаба М. Б. Дипфейки как угроза правам человека // Lex Russica. 2022. № 11 (192). URL: https://cyberleninka.ru/article/n/dipfeyki-kak-ugroza-pravam-cheloveka (дата обращения: 06.02.2026). DOI: 10.17803/1729-5920.2022.192.11.112-119.

5. Бодров Н. Ф., Лебедева А. К. Перспективы правового регулирования и алгоритм маркировки генеративного контента // Пенитенциарная наука. 2024. № 4 (68). URL: https://cyberleninka.ru/article/n/perspektivy-pravovogo-regulirovaniya-i-algoritm-markirovki-generativnogo-kontenta (дата обращения: 08.02.2026). DOI: 10.46741/2686-9764.2024.68.4.001.

6. Romero Moreno F. Generative AI and deepfakes: a human rights approach to tackling harmful content // International Review of Law, Computers & Technology. 2024. Vol. 38. No. 3. P. 297-326. DOI:10.13140/RG.2.2.20397.05604.

7. Дремлюга Р. И., Моисейцев В. В., Парин Д. В., Романова Л. И. Национальное правовое регулирование использования и распространения реалистичных аудиовизуальных поддельных материалов (deepfake): опыт Китая // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. № 4. URL: https://cyberleninka.ru/article/n/natsionalnoe-pravovoe-regulirovanie-ispolzovaniya-i-rasprostraneniya-realistichnyh-audiovizualnyh-poddelnyh-materialov-deepfake (дата обращения: 05.02.2026). DOI: 10.24866/1813-3274/2022-4/91-104.

8. Виноградов В. А., Кузнецова Д. В. Зарубежный опыт правового регулирования технологии «дипфейк» // Право. Журнал Высшей школы экономики. 2024. № 2. URL: https://cyberleninka.ru/article/n/zarubezhnyy-opyt-pravovogo-regulirovaniya-tehnologii-dipfeyk (дата обращения: 08.02.2026). DOI: 10.17323/2072-8166.2024.2.215.240.

References

1. Bodrov N. F., Lebedeva A. K. The concept of deepfake in Russian law, classification of deepfakes and issues of their legal regulation. *Yuridicheskie issledovaniya*. 2023; 11. Available at: https://cyberleninka.ru/article/n/ponyatie-dipfeyka-v-rossiyskom-prave-klassifikatsiya-dipfeykov-i-voprosy-ih-pravovogo-regulirovaniya (accessed: 03.02.2026). (In Russ.).

2. Meskys E., Kalpokienė J., Jurcys P., Liaudanskas A. Regulating Deep Fakes: Legal and Ethical Considerations. *Journal of Intellectual Property Law & Practice*. 2020; 15 (1): 24-31. Available at: https://ssrn.com/abstract=3497144 (accessed: 04.02.2026).

3. Tokolov A.V. Legal regulation of deepfakes. *Vestnik ehkonomicheskoj bezopasnosti*. 2025; 2. Available at: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-dipfeykov (accessed: 05.02.2026). (In Russ.).

4. Dobrobaba M. B. Deepfakes as a threat to human rights. *Lex Russica*. 2022; 11 (192). Available at: https://cyberleninka.ru/article/n/dipfeyki-kak-ugroza-pravam-cheloveka (accessed: 06.02.2026). (In Russ.).

5. Bodrov N. F., Lebedeva A. K. Prospects of legal regulation and algorithm of labeling generative content. *Penitenciarnaya nauka*. 2024; 4 (68). Available at: https://cyberleninka.ru/article/n/perspektivy-pravovogo-regulirovaniya-i-algoritm-markirovki-generativnogo-kontenta (accessed: 08.02.2026). (In Russ.).

6. Romero Moreno F. Generative AI and deepfakes: a human rights approach to tackling harmful content. *International Review of Law, Computers & Technology*. 2024; 38 (3): 297-326.

7. Dremlyuga R. I., Moiseitsev V. V., Parin D. V., Romanova L. I. National legal regulation of the use and distribution of realistic audiovisual fake materials (deepfake): the experience of China. *Aziatsko-Tikhookeanskij region: ehkonomika, politika, pravo*. 2022; 4. Available at: https://cyberleninka.ru/article/n/natsionalnoe-pravovoe-regulirovanie-ispolzovaniya-i-rasprostraneniya-realistichnyh-audiovizualnyh-poddelnyh-materialov-deepfake (accessed: 05.02.2026). (In Russ.).

8. Vinogradov V. A., Kuznetsova D. V. Foreign experience in the legal regulation of deepfake technology. *Pravo. Journal of the Higher School of Economics*. 2024; 2. Available at: https://cyberleninka.ru/article/n/zarubezhnyy-opyt-pravovogo-regulirovaniya-tehnologii-dipfeyk (accessed: 02/08/2026). (In Russ.).

Информация об авторах

Гаврилова Юлия Александровна, кандидат юридических наук, доцент, Казахстанско-Американский свободный университет, г. Усть-Каменогорск, Казахстан, e-mail: gavriloyuliya@yandex.ru

Умитчинова Ботагоз Аспандиаровна, PhD, ассоциированный профессор-исследователь, Казахстанско-Американский свободный университет, г. Усть-Каменогорск, Казахстан, e-mail: umitchinova.botagoz@mail.ru

Information about the authors

Yuliya A. Gavrilova, Candidate of Legal Sciences, Associate Professor, Kazakhstan-American Free University, Ust-Kamenogorsk, Kazakhstan, e-mail: gavriloyuliya@yandex.ru

Umitchinova Botagoz Aspandiyarovna, PhD, Associate Research Professor, Kazakhstan-American Free University, Ust-Kamenogorsk, Kazakhstan, e-mail: umitchinova.botagoz@mail.ru

Для цитирования

Гаврилова Ю. А., Умитчинова Б. А. Правовое регулирование дипфейков: анализ зарубежного опыта и перспективы для России и Казахстана // Журнал Высокотехнологичное право. − 2026. Т. 2, № 1. − С. 162-181.

For citation

Gavrilova Yu. A., Umitchinova B. A. Legal regulation of deepfakes: analysis of foreign experience and prospects for Russia and Kazakhstan // Journal of High-tech Law. − 2026. Vol. 2, No. 1. − Pp.162-181.

Поступила в редакцию / Received 09.02.2026
Поступила после рецензирования / Received after review 24.02.2026
Принята к публикации / Accepted 27.03.2026