Дата поступления рукописи в редакцию: 07.06.2026 г.
Дата принятия рукописи в печать: 29.06.2026 г.
DOI: 10.24412/2076-1503-2026-6-406-412

ПЕТРОВА Наталья Дмитриевна,
кандидат юридических наук, доцент кафедры общетеоретических правовых дисциплин СЗФ ФГБОУ ВО «РГУП им. В.М. Лебедева», Санкт-Петербург, Россия,
e-mail: nava2009@yandex.ru

АНТОНОВ Александр Дмитриевич,
студент 2 курса специалитета СЗФ ФГБОУВО «РГУП им. В.М. Лебедева», Санкт-Петербург, Россия,
e-mail: alexandrant356@gmail.com

ПРОБЛЕМА ЭФФЕКТИВНОГО ПРАВОВОГО РЕГУЛИРОВАНИЯ И ПРИМЕНЕНИЯ ТЕХНОЛОГИИ ДИПФЕЙК В РОССИИ: ТЕОРИЯ И ПРАКТИКА

Аннотация. *Статья посвящена правовой природе дипфейков и проблемам их нормативного регулирования в Российской Федерации. Дипфейк рассматривается как комплексное явление, затрагивающее сферу личных неимущественных прав, информационной безопасности и интеллектуальной собственности, и предложена классификация синтезированного контента по целевому назначению. Проведён сравнительный обзор трёх зарубежных моделей регулирования, а именно китайской, американской и европейской. Основная проблематика связана с пробелами российского законодательства, среди которых отсутствие легального определения дипфейка, неопределённость правового режима синтезированного голоса и неготовность судебно-экспертной системы к работе с результатами генеративного искусственного интеллекта. В качестве первоочередных мер обозначены законодательное закрепление термина, введение обязательной маркировки синтезированного контента и модернизация экспертных методик.*

Ключевые слова*: дипфейк, синтезированный контент, искусственный интеллект, охрана изображения, персональные данные, маркировка.*

PETROVA Natalya Dmitrievna,
Candidate of Law, Associate Professor, Department of General Theoretical Legal Disciplines, NWF FGBOUVO "RGUP named after V.M. Lebedev", St. Petersburg, Russia

ANTONOV Aleksandr Dmitrievich,
2nd year specialist student NWF FGBOUVO "RGUP named after V.M. Lebedev", St. Petersburg, Russia

PROBLEM OF EFFECTIVE LEGAL REGULATION AND APPLICATION OF DEEPFAKE TECHNOLOGY IN RUSSIA: THEORY AND PRACTICE

Annotation. *The article examines the legal nature of deepfakes and the challenges of their normative regulation in the Russian Federation. The deepfake is considered as a complex phenomenon affecting personal non-property rights, information security and intellectual property, and a classification of synthesized content by intended purpose is proposed. A comparative overview of three foreign regulatory models is provided, namely the Chinese, the American and the European. The main problems stem from gaps in Russian legislation, including the absence of a legal definition*

of deepfake, the uncertain legal status of synthesized voice and the unpreparedness of the forensic expert system for dealing with generative artificial intelligence outputs. Priority measures include legislative consolidation of the term, the introduction of mandatory labeling of synthesized content and the modernization of forensic examination methods.

Key words: *deepfake, synthesized content, artificial intelligence, image protection, personal data, labeling.*

Говоря о дипфейках, первая же проблема, с которой сталкивается любой юрист - это отсутствие в российском законодательстве самого термина. В Российской Федерации нет легального определения, записанного в каком-то кодексе или федеральном законе. Отсюда и возникает путаница из-за которой суды и правоведы пытаются «притянуть» дипфейк к уже существующим понятиям, но получается это не очень удачно [4; с. 349]. Чаще всего его пытаются рассматривать либо как разновидность недостоверной информации, либо как изображение гражданина, которое охраняется статьей 152.1 Гражданского кодекса. Проблема в том, что дипфейк- это не просто ложная информация и не просто чужая фотография, которую взяли без спроса. Это синтез, создание нового объекта, которого в реальности никогда не было. И закон пока не знает, как с таким объектом обращаться [7; с. 322].

Пытаясь навести какой-то порядок, специалисты предлагают классифицировать дипфейки не по техническим признакам - как именно работал алгоритм, а именно по цели создания. И здесь довольно четко выделяются три большие группы. Первая - это развлекательные дипфейки. Люди ради шутки подставляют лицо друга в смешной ролик или оживляют героев известных картин. С правовой точки зрения это, конечно, тоже использование чужого изображения без согласия, но так как вред обычно минимален, дело редко доходит до серьезных разбирательств, если только сам «герой» не обидится на шутку. Вторая группа - коммерческие. Например, когда рекламируют товар с помощью цифровой копии умершего актера или когда блогер продает курсы, используя свой синтезированный аватар. Здесь вопросы уже серьезнее, касающиеся наследования прав на образ, налогов, обмана потребителя. И третья, самая опасная группа -это вредоносные дипфейки. Сюда входят и политические фальшивки, когда кандидату приписывают слова, которых он не говорил, и мошенничество с подделкой голоса начальника для перевода денег, и, что совсем отвратительно, создание порнографических материалов с лицом человека без его ведома. Именно для этой последней категории и нужно самое жесткое регулирование, потому что оно защищает не абстрактную информацию, а конкретного человека, его достоинство и безопасность [6; с. 25]. И пока закон не научится отличать безобидную шутку от реальной угрозы, путаница будет только нарастать.

Когда начинаешь разбираться в зарубежном опыте регулирования дипфейков, быстро приходит понимание того, что единого шаблона в мире нет. Большинство исследователей сходятся на том, что сложилось три основных модели — американская, европейская и китайская. Различаются они прежде всего тем, кого или что ставят в центр регулирования. В США смотрят на конкретную сферу применения, в Европе — на весь жизненный цикл технологии, а в Китае — на того, кто предоставляет сервис [2; с. 55].

В США исторически вообще очень неохотно вторгались в регулирование интернета. Там еще в 1996 году приняли Communications Decency Act, а внутри него есть знаменитая секция 230, которая дала онлайн-платформам широчайший иммунитет от ответственности за контент, созданный пользователями. Проще говоря, если кто-то выложил на сайте дипфейк, судиться надо с автором, а площадка остается в стороне. Именно поэтому на федеральном уровне в Америке долгое время не принимали единого закона о дипфейках, а предпочитали действовать точечно — через иски о клевете, о нарушении права на публичность и через законодательство отдельных штатов. Например, Калифорния и Техас одними из первых криминализовали порнографические дипфейки. Однако в последнее время ситуация начала меняться. В мае 2025 года был подписан первый федеральный закон, напрямую ограничивающий вредоносные дипфейки, Take It Down Act [2; с. 56]. Он касается прежде всего интимных изображений, созданных без согласия, и обязывает платформы удалять такой контент в течение 48 часов после обращения жертвы. Если же платформа не реагирует, последуют серьезные штрафы и даже уголовная ответственность для распространителей до трех лет лишения свободы. Так что можно сказать, что американская модель, долгое время бывшая «мягкой», сегодня заметно ужесточается.

Китай пошёл принципиально иным путём, причём с самого начала. Там регулирование дипфейков встроено в общую систему контроля за интернетом, и главная идея — максимальная прозрачность и отслеживаемость. Китайские власти приняли целый пакет нормативных актов, которые введены в действие с сентября 2025 года, и там

установлено жесткое правило. Любой сгенерированный или измененный искусственным интеллектом контент будь то изображение, видео, аудио или даже текст должен быть промаркирован. Причём маркировка двойная. Видимая (например, водяной знак, который замечает обычный пользователь) и невидимая (зашифрованная цифровая подпись в метаданных файла, которую могут считать алгоритмы). Более того, китайский закон прямо запрещает любые попытки удалить или изменить такую маркировку. Если платформа обнаружит контент без водяного знака, она обязана потребовать от пользователя заявления о том, что это сгенерированный материал, а в противном случае пометить его как «предположительно синтетический». Такой тотальный контроль, конечно, вызывает споры о приватности и свободе слова, но с точки зрения эффективности модель весьма показательна.

Европейский Союз, как это часто бывает, выбрал срединный путь. Ключевой документ здесь — Акт об искусственном интеллекте (EU AI Act), который официально вступил в силу и поэтапно вводится в действие. В нем регулирование строится по принципу управления рисками. Технологии делятся на категории, и генеративный ИИ, включая дипфейки, попадает в категорию ограниченного риска. Статья 52 этого Акта содержит требования по прозрачности, причем важнейшая из них касается как раз синтезированного контента. Если ИИ используется для создания или изменения изображения, звука либо видео, которые выглядят как настоящие, пользователи должны быть проинформированы об этом. Европейские эксперты, которые анализировали применение этих норм на практике, подчеркивают, что простого уведомления недостаточно. Предупреждение должно быть действительно доступным для самых разных людей, включая лиц с ограниченными возможностями, и должно предоставлять ровно столько информации, сколько нужно в конкретной ситуации, не перегружая зрителя. Поэтому лучшей практикой считается многослойный подход. Короткое и заметное предупреждение на самом изображении или в начале ролика плюс возможность перейти к более подробной информации, если человеку это интересно. Кроме того, в Европе действует GDPR, и тут возникает интересная коллизия. Синтез лица или голоса может считаться обработкой биометрических данных, что требует особо серьезных правовых оснований.

Сравнивая все три модели, видно, что каждая отражает более широкие правовые традиции и культурные установки своих стран. Китай делает ставку на превентивный контроль и прослеживаемость, США долгое время полагались на саморегуляцию и судебные иски и только сейчас вводят федеральные запреты, а Европа пытается соблюсти баланс между защитой прав граждан и поддержкой инноваций. Интересно, что исследователи, изучавшие этот вопрос, приходят к выводу, что ни одна из трех моделей пока не является идеальной, и самое слабое место у них общее, то, что все они фокусируются на создателях контента, платформах и распространителях, но практически не работают с аудиторией, то есть с теми, кто этот контент потребляет и может стать жертвой обмана. Повышение цифровой грамотности пользователей - это тот элемент, которого не хватает всем трем системам.

Когда переходишь к российским реалиям, первое, что бросается в глаза, что у нас есть набор разрозненных правовых норм, которые вроде бы по отдельности что-то регулируют, но в единую систему не складываются. Проблема даже не в том, что законов мало, потому что их как раз довольно много, а в том, что они не были рассчитаны на технологии синтеза и сегодня работают по принципу закрывания быстро образующихся пробелов, за которыми трудно поспеть [13].

Начать стоит, пожалуй, с самого очевидного-гражданско-правовой защиты. У нас есть статья 152.1 ГК РФ «Охрана изображения гражданина», которая прямо говорит, что обнародование и дальнейшее использование изображения гражданина допускается только с его согласия. Как упоминалось ранее нету правовой нормы регулирующей использование голоса в Гражданском кодексе. Эта проблема вскрылась осенью 2024 года и в Госдуму был внесён законопроект № 718834-8, предлагавший дополнить ГК РФ статьей 152.3 «Охрана голоса гражданина» [3; с. 112], почти полностью повторяющей конструкцию 152.1. Но Совет при Президенте по кодификации этот законопроект не поддержал, указав, что действующая статья 150 ГК РФ и так содержит открытый перечень нематериальных благ, а значит, голос можно защищать через неё, плюс есть законодательство о персональных данных и запись голоса может рассматриваться как обработка биометрических данных. На практике же судам гораздо удобнее, когда норма прямо прописана в кодексе, а не выводится через толкование открытого перечня.

Даже если говорить об изображении, статья 152.1 ГК РФ имеет важное ограничение. Согласие не требуется, когда гражданин позировал за плату. И здесь возникает серая зона. Если модель или актёр получил гонорар за съемку, означает ли это автоматическое согласие на синтез его цифрового двойника нейросетью? Кодекс на этот вопрос не отвечает, а договорная практика в индустрии пока только формируется.

Теперь перейдем к публично-правовому блоку. Здесь есть важная статья 207.3 УК РФ — распространение заведомо ложной информации об использовании Вооруженных Сил РФ. Законодатель ввел ее в 2022 году, и практика по ней активно нарабатывается. Например, в апреле 2026 года Преображенский районный суд Москвы приговорил к шести годам колонии настоятеля буддийского центра за пост в фейсбуке, который был квалифицирован именно по пункту «д» части 2 статьи 207.3 -распространение военных «фейков» по мотиву ненависти [5]. Но, стоит заметить, что речь там шла о текстовой публикации. Дипфейк — это видео или аудио, и подделка здесь гораздо сложнее и опаснее, потому что создает иллюзию документальности. Однако состав статьи 207.3 УК РФ сформулирован через «заведомо ложную информацию», а не через способ её создания. Это значит, что дипфейк может быть и правдивым по содержанию, но порочащим по форме, и тогда уголовная ответственность не наступит. Пленум Верховного Суда по применению этой статьи в части, касающейся именно синтезированного контента, пока отсутствует, что оставляет суды без четких ориентиров.

Так же есть административные составы. К примеру статья 13.15 КоАП РФ о злоупотреблении свободой массовой информации, которая в том числе охватывает распространение недостоверной общественно значимой информации под видом достоверных сообщений. Но и здесь все упирается в доказывание. Чтобы наказать за дипфейк, суду и сторонам надо сначала установить, что это действительно синтез, а не подлинная запись.

Отдельного внимания заслуживает избирательное законодательство. Здесь произошли, пожалуй, самые заметные подвижки. В апреле 2026 года Госдума приняла, а Совет Федерации одобрил закон, запрещающий использовать в агитационных материалах изображения и голоса людей, созданные с помощью информационных технологий, а также образы вымышленных или умерших лиц. Это первый в российском законодательстве случай прямого упоминания синтезированного контента в контексте выборов. Однако, как справедливо отмечают эксперты, запретить-то запретили, но механизма оперативного выявления таких материалов в ходе короткой агитационной кампании закон не предусматривает.

Теперь о самом сложном- о доказывании. Это та проблема, которая в судах возникает постоянно и которую признают все без исключения специалисты. Российский процесс построен на принципе свободной оценки доказательств (статья 17 УПК РФ, статья 67 ГПК РФ), но при этом судья обязан исследовать их непосредственно и проверять на относимость, допустимость и достоверность. Когда перед судьей лежит видеозапись, он психологически склонен ей доверять. Это так называемый эффект «презумпции достоверности» аудиовизуального доказательства. Дипфейк эту презумпцию разрушает. Проблема усугубляется состоянием судебно-экспертной деятельности. Минюст неоднократно возвращался к обсуждению поправок в закон о регулировании экспертизы, настаивая на создании реестра аттестованных экспертов и мониторинге их заключений. Но пока это только планы.

Показательный случай разобрал Верховный Суд РФ, когда отменил приговор из-за некомпетентности эксперта. Оценщик вместо осмотра реальных труб просто поискал аналоги в интернете. Если эксперт допускает такие ошибки при оценке металлолома, то что говорить о сложнейшей компьютерно-технической экспертизе видеофайла на предмет синтеза. Для выявления дипфейка нужна мультимодальная экспертиза: спектрограмма голоса, анализ частоты моргания, поиск цифровых артефактов. Но четкого стандарта такой экспертизы ни в одном процессуальном кодексе не прописано, как нет и утвержденной методики. Более того, сам Верховный Суд в постановлениях неоднократно напоминал, что суд не может слепо доверять заключению эксперта, а должен оценивать его в совокупности с другими доказательствами — но в случае с высокотехнологичным дипфейком у судьи зачастую просто нет инструментов для такой оценки.

Таким образом, российская ситуация выглядит так, что нормы материального права есть, но они мозаичны и не всегда «попадают» в специфику синтезированного контента, а в избирательном праве уже появился прямой запрет дипфейков, но без механизма его реализации, но а главная проблема лежит в процессуальной плоскости — неготовность экспертной системы и отсутствие у судов навыков критической оценки цифровых аудиовизуальных доказательств.

Исходя из выше перечисленной практики и существующих норм можно сказать, что дипфейки вскрывают большой перечень проблем. Как определить термин, как наказывать мошенников, как защитить честь и достоинство. Но есть несколько точечных, почти бытовых ситуаций, в которых даже идеально прописанный закон рискует провалиться. Именно эти пробелы показывают, насколько эта проблема актуальна и сложна для законодателя, и правоприменителя.

Первая и, пожалуй, самая тонкая грань проходит между преступлением и шуткой. Представим, что человек создаёт дипфейк-ролик, где известный политик танцует смешной танец, и выкладывает его в сеть. Это пародия или вторже-

ние в частную жизнь? С одной стороны, у нас есть пункт 3 статьи 1274 Гражданского кодекса, который разрешает создавать пародии и карикатуры без согласия автора или правообладателя оригинала. С другой — статья 152.1 ГК РФ, которая требует согласия гражданина на обнародование его изображения. Постановление Пленума Верховного Суда РФ от 23 апреля 2019 года № 10 разъясняет, что пародия -это самостоятельное произведение, и автор оригинала не вправе её запрещать. Однако на практике суды сталкиваются с серьёзными трудностями при определении, что именно является пародией, а что-незаконным использованием чужого образа [10; С. 63].

Президиум Высшего Арбитражного Суда ещё в 2013 году сформулировал важный критерий. Оригинальное произведение должно быть в центре нового, а не просто фоном или вспомогательным средством. Это значит, что просто вставить чужое лицо в развлекательный ролик нельзя автоматически считать пародией -нужно именно творчески переосмысливать оригинал. Но как применить этот критерий к дипфейку, где «оригиналом» выступает сам человек, а не его произведение? Грань действительно очень тонкая, и суды вынуждены решать такие дела, по сути, на основе собственного усмотрения.

Вторая острая точка -трудовые отношения. Работодатели сегодня активно осваивают цифровые инструменты и создают корпоративные видеоролики, обучающие материалы, рекламные презентации. И здесь возникает вопрос, может ли начальник использовать лицо или голос подчинённого, синтезированные нейросетью, без отдельного согласия? Трудовой кодекс такого сценария не предусматривает. Статья 64 ТК РФ запрещает необоснованный отказ в приёме на работу, статья 86 - требует согласия работника на обработку его персональных данных. Но является ли создание цифрового аватара обработкой персональных данных? А если работник уже давал согласие на фотосъёмку для пропуска — распространяется ли оно на синтез нейросетью? Ответов на эти вопросы в действующем регулировании нет. Более того, закон о персональных данных запрещает работодателю хранить избыточную информацию о сотруднике и обязывает удалять её после достижения цели обработки. Это означает, что любую информацию, собранную без чётко прописанной и законной цели, может быть признано незаконным. На практике это создаёт ситуацию правовой неопределённости и работодатель не знает границ дозволенного, и работник не понимает, как защитить свой цифровой образ.

Третья, самая сложная проблема — судебное доказывание. У судье есть право оценивать доказательства по своему внутреннему убеждению. Раньше это работало неплохо и видя документ или запись судья мог судить об их достоверности. Но сегодня, дипфейки голоса и фото уже неотличимы от настоящих записей, а в скором времени это коснётся и видео. И здесь старая система даёт сбой. Для выявления дипфейка нужна мультимодальная экспертиза. Но ни в одном российском процессуальном кодексе нет утверждённого стандарта проведения такой экспертизы, не говоря уже о реестре аттестованных специалистов. Судья, не обладая специальными познаниями, вынужден либо слепо доверять заключению эксперта, либо полагаться на интуицию — и то, и другое разрушает саму идею справедливого правосудия. Именно поэтому исследователи и настаивают на разработке новых методик судебно-экспертного исследования синтезированного контента, без которых любые материально-правовые запреты рискуют остаться лишь декларациями.

Подводя итог всему вышесказанному, хочется сразу отмести самое простое и, на первый взгляд, соблазнительное решение -взять и всё запретить. Практика показывает, что этот путь тупиковый. Технологии развиваются с такой скоростью, что любой жёсткий запрет устареет ещё до того, как его научатся применять, да и дипфейки бывают не только вредоносными. Они используются в кино, в образовании, в искусстве, и тотальный запрет здесь просто обессмыслит целые индустрии. Да и технически проконтролировать такой запрет невозможно

Раскрыв все возможные проблемы можно говорить о трех конкретных шагах для совершенствования законодательства.

В самом начале дать дипфейку легальное определение. Пока такого определения нет ни в одном федеральном законе, суды и правоприменители вынуждены «подтягивать» дипфейки под существующие нормы. Нужен единый термин, который охватывал бы и видео, и аудио, и фото, синтезированные нейросетями, и был бы встроен в отраслевое законодательство.

Второе это обязательная маркировка синтезированного контента. Причём идея не об утопической идее «давайте заставим всех маркировать всё». Как раз недавняя история с законопроектом о маркировке ИИ-контента показала, к чему приводит непродуманный подход. Комитет Госдумы по информационной политике отклонил эту инициативу, и причины были совершенно разумными. Авторы не пояснили, на каком этапе ставится метка, кто отвечает за её сохранность при пересылке, кто ставит её изначально, разработчик нейросети или пользователь. Более того, как отметил первый зампред IT-комитета Антон Горел-

кин [12], маркировать при таком подходе пришлось бы уже 90 процентов всего интернета, а мошенники при этом маркировать свои подделки, естественно, не станут. Значит, речь должна идти о другом. Ввести требование маркировки не для всех подряд, а для крупных сервисов и платформ, которые предоставляют пользователям инструменты генерации контента. Именно разработчик нейросети должен на уровне кода вшивать машиночитаемую метку в файл, а не пользователь ставить галочку «я создал дипфейк». И за удаление такой метки должна быть установлена ответственность.

Шаг третий, без которого первые два просто не заработают-это модернизация судебной экспертизы. Сегодня, как мы видели, судья остаётся один на один с видеофайлом и не имеет инструментов понять, настоящий он или синтезированный. А специалисты МВД уже прямо говорят, что при расследовании таких дел нужно переходить к аппаратной фиксации и поиску цифровых следов, подтверждать синтетический материал программными средствами, а не полагаться только на показания. В научной среде тоже активно обсуждается эта проблема. Так, профессор Е.Р. Россинская в статье 2025 года пишет о необходимости модернизации существующих экспертных методик и разработки новых, основанных на применении нейросетевых технологий, а также о важности подготовки кадров с компетенциями в области анализа данных и машинного обучения [8; с. 110]. Пока же получается замкнутый круг: закон может сколько угодно запрещать вредоносные дипфейки, но если суд не в состоянии отличить подделку от оригинала, никакого наказания не будет.

Кроме того, законодатель уже начинает двигаться в правильном направлении. В феврале 2026 года в Госдуме подготовили поправки в Уголовный кодекс, которые предлагают считать использование дипфейков отягчающим обстоятельством при совершении преступления [11]. Авторы поправок прямо отмечают, что дипфейки остаются востребованным инструментом у злоумышленников, повышают убедительность мошеннических схем и затрудняют расследование, а в УК до сих пор нет специальных правил учёта этого обстоятельства при назначении наказания. Такой подход -не запрещать дипфейки как явление, а усиливать ответственность за их преступное использование — представляется наиболее сбалансированным.

В конечном счёте, главный вызов для права состоит не в том, чтобы остановить прогресс, а в том, чтобы научиться с ним работать. Дипфейк — это лишь инструмент, и сам по себе он нейтрален. Всё зависит от того, в чьих руках он оказывается. Задача права не раздавить технологию, а создать такие правила игры, при которых добросовестные пользователи и разработчики защищены, а злоумышленники несут неотвратимое наказание. Легальное определение термина, обязательная маркировка на уровне сервисов-генераторов и оснащение судов и следствия современными экспертными методиками-это три столпа, на которых может держаться такая система. И начинать строить её нужно уже сейчас, пока поток синтезированного контента не захлестнул нас окончательно.

Список литературы:

[1] Архиереев Н. В. Правовое регулирование создания и использования дипфейков / Н. В. Архиереев // Правовое государство: теория и практика. — 2025. — Т. 21, № 2 (80). — С. 24–30.

[2] Астапенко П. Н. Сравнительный анализ правового регулирования искусственного интеллекта в России, Китае, США и Европейском союзе / П. Н. Астапенко // Закон и право. — 2025. — № 6. — С. 52–57.

[3] Бодров Н. Ф. Дипфейк. Технологии, правовое регулирование и судебно-экспертное исследование : монография / Н. Ф. Бодров, А. К. Лебедева. — Москва : Проспект, 2026. — 224 с.

[4] Бодров Н. Ф. Перспективы правового регулирования и алгоритм маркировки генеративного контента / Н. Ф. Бодров, А. К. Лебедева // Пенитенциарная наука. — 2024. — Т. 18, № 4 (68). — С. 346–354.

[5] Киндеева К. Настоятель буддийского центра в Москве получил шесть лет колонии за фейки // РБК. URL: https://www.rbc.ru/rbcfreenews/69f0b8e59a79476f6d14a16a (дата обращения: 21.04.2026).

[6] Куприянов А. А. Почему нужно срочное регулирование в области дипфейков / А. А. Куприянов // Уголовный процесс. — 2024. — URL: https://e.ugpr.ru/1118901 (дата обращения: 21.04.2026).

[7] Модонов Н. В. Распространение ложных сведений с использованием дипфейков: правовые аспекты и ответственность / Н. В. Модонов // Молодой ученый. — 2024. — № 50 (549). — С. 320–323.

[8] Россинская Е. Р. Цифровизация судебно-экспертной деятельности : учебное пособие для вузов под научной редакцией Е. Р. Россинской, А. А. Саркисян. — Москва : Юрайт, 2025. — 138 с.

[9] Хохлова Е. В. Уголовно-правовые и цивилистические аспекты охраны голоса / Е. В. Хохлова // Известия Юго-Западного государственного университета. Серия: История и право. — 2025. — Т. 15, № 1. — С. 96–111.

[10] Юрьева Л. А. Охрана изображения гражданина в условиях развития цифровой реальности / Л. А. Юрьева, Ю. А. Горбуль // Вестник Омского университета. Серия: Право. — 2022. — Т. 19, № 3. — С. 61–69.

[11] В Госдуму внесен законопроект об уголовной ответственности за дипфейки // Парламентская газета. — 2026. — 27 января. — URL: https://www.pnp.ru/
social/v-gosdumu-vnesli-zakonoproekt-ob-ugolovnoy-otvetstvennosti-za-dipfeyki.html (дата обращения: 20.04.2026).

[12] Профильный комитет ГД отклонил проект о маркировке контента, сгенерированного ИИ // Интерфакс : [новостной ресурс]. — 2026. — 15 апреля. — URL: https://www.interfax.ru (дата обращения: 20.04.2026).

[13] Бодров Н.Ф., Лебедева А.К. Дипфейк. Технологии, правовое регулирование и судебно-экспертное исследование: монография. — М.: Проспект, 2026. — 224 с.

References:

[1] Arkhiereev N. V. Legal Regulation of the Creation and Use of Deepfakes / N. V. Arkhiereev // The Rule of Law: Theory and Practice. - 2025. - Vol. 21, No. 2 (80). - Pp. 24-30.

[2] Astapenko P. N. Comparative Analysis of Legal Regulation of Artificial Intelligence in Russia, China, the USA and the European Union / P. N. Astapenko // Law and Right. - 2025. - No. 6. - Pp. 52-57.

[3] Bodrov N. F. Deepfake. Technologies, Legal Regulation and Forensic Research: Monograph / N. F. Bodrov, A. K. Lebedeva. - Moscow: Prospect, 2026. - 224 p.

[4] Bodrov, N. F. “Prospects for Legal Regulation and an Algorithm for Labeling Generative Content” / N. F. Bodrov, A. K. Lebedeva // Penitentiary Science. — 2024. — Vol. 18, No. 4 (68). — Pp. 346–354.

[5] Kindeeva, K. “The Abbot of a Buddhist Center in Moscow Received a Six-Year Prison Sentence for Fakes” // RBC. URL: https://www.rbc.ru/rbc-freenews/69f0b8e59a79476f6d14a16a (accessed on April 21, 2026).

[6] Kupriyanov, A. A. “Why Urgent Regulation is Needed in the Field of Deepfakes” / A. A. Kupriyanov // Criminal Procedure. — 2024. — URL: https://e.ugpr.ru/1118901 (date of access: 21.04.2026).

[7] Modonov N. V. Dissemination of false information using deepfakes: legal aspects and liability / N. V. Modonov // Young scientist. — 2024. — No. 50 (549). — P. 320–323.

[8] Rossinskaya E. R. Digitalization of forensic activity: a textbook for universities edited by E. R. Rossinskaya, A. A. Sarkisyan. — Moscow: Yurait, 2025. — 138 p.

[9] Khokhlova E. V. Criminal and civil aspects of voice protection / E. V. Khokhlova // Bulletin of the South-West State University. Series: History and Law. — 2025. — Vol. 15, No. 1. — P. 96–111.

[10] Yuryeva, L. A. Protection of a Citizen’s Image in the Context of the Development of Digital Reality / L. A. Yuryeva, Yu. A. Gorbul // Bulletin of Omsk University. Series: Law. — 2022. — Vol. 19, No. 3. — P. 61–69.

[11] A bill on criminal liability for deepfakes has been submitted to the State Duma // Parliamentary Newspaper. — 2026. — January 27. — URL: https://www.pnp.ru/
social/v-gosdumu-vnesli-zakono-proekt-ob-ugolovnoy-otvetstvennosti-za-dipfeyki.html (accessed: April 20, 2026).

[12] The State Duma’s relevant committee rejected the bill on labeling AI-generated content // Interfax: [news resource]. - 2026. - April 15. - URL: https://www.interfax.ru (accessed: 20.04.2026).

[13] Bodrov N.F., Lebedeva A.K. Deepfake. Technologies, legal regulation and forensic research: monograph. - M .: Prospect, 2026. - 224 p.