Дата поступления рукописи в редакцию: 16.07.2026 г. DOI: 10.24412/2224-9133-2026-8-426-434
Дата принятия рукописи в печать: 01.09.2026 г.

МАЙСТРЕНКО Григорий Александрович,
кандидат юридических наук, старший научный сотрудник ФКУ НИИ ФСИН России, ORCID -0000-0001-5668-615X,
e-mail: g.maystrenko@yandex.ru

ПРЕСТУПНОЕ ИСПОЛЬЗОВАНИЕ ДИПФЕЙКОВ В МЕХАНИЗМЕ ПОСЯГАТЕЛЬСТВА НА ЦИФРОВУЮ ИДЕНТИЧНОСТЬ

Аннотация. *Статья посвящена уголовно-правовой оценке использования дипфейков как средства посягательства на цифровую идентичность человека. Цель исследования состоит в определении достаточности действующих норм Уголовного кодекса Российской Федерации и разработке модели их точечного совершенствования, исключающей технологически нейтральную гиперкриминализацию. На основе формально-юридического, системного и сравнительно-правового методов анализируются нормы о клевете, нарушении неприкосновенности частной жизни, мошенничестве, вымогательстве, преступлениях в сфере компьютерной информации и незаконном обороте порнографических материалов, а также законопроект № 718538-8. Обосновывается, что дипфейк в большинстве случаев выполняет инструментальную функцию и не образует самостоятельного объекта уголовно-правового запрета. Выявлены проблемы квалификации деяний при конкуренции статей 159, 159.6 и 272.1 УК РФ, а также пробел в защите от несанкционированных интимных синтетических материалов. Предлагается гибридная модель: легальное определение синтетического аудиовизуального материала; учет его целевого использования в качестве ограниченного отягчающего обстоятельства; специальный состав за умышленное создание, распространение либо угрозу распространения интимного дипфейка без согласия изображенного лица. Сформулированы критерии разграничения уголовно наказуемого поведения, гражданско-правового деликта и допустимого творческого использования технологии.*

Ключевые слова: *дипфейк; цифровая идентичность; искусственный интеллект; мошенничество; биометрические данные; синтетический контент; криминализация; уголовная ответственность.*

MAISTRENKO Grigory Aleksandrovich,
Candidate of Law, Senior Researcher, Federal State Budgetary Institution Research Institute of the Federal Penitentiary Service of Russia

CRIMINAL USE OF DEEPFAKES AS AN ENCROACHMENT ON DIGITAL IDENTITY

Annotation. *The article examines the criminal-law assessment of deepfakes used as instruments of encroachment on an individual's digital identity. The study aims to determine whether the existing provisions of the Criminal Code of the Russian Federation are sufficient and to design a targeted model of legislative improvement that avoids technology-neutral overcriminalization. Using formal legal, systemic, and comparative methods, the author analyses provisions on defamation, privacy violations, fraud, extortion, computer-information offences, unlawful trafficking in pornographic materials, and Draft Law No. 718538-8. It is argued that, in most cases, a deepfake performs an instrumental function and should not automatically constitute an independent object of criminal prohibition. Particular attention is paid to the delimitation of Articles 159, 159.6, and 272.1 of the Criminal Code and to the protection gap concerning non-consensual intimate synthetic media. A hybrid regulatory model is proposed: a statutory definition of synthetic audiovisual material; narrowly framed aggravation where such material substantially facilitates an intentional offence; and a specific offence covering intentional creation, dissemination, or threatened dissemination of an intimate deepfake without the depicted person's consent. Criteria are formulated to distinguish crime, civil wrongdoing, and legitimate creative use.*

Key words: *deepfake; digital identity; artificial intelligence; fraud; biometric data; synthetic media; criminalization; criminal liability.*

Введение

Генеративные модели искусственного интеллекта превратили достоверную имитацию внешности, голоса и манеры поведения конкретного человека из ресурсоемкой технической операции в массово доступную услугу. Для уголовного права принципиален не сам технологический эффект, а изменение механизма причинения вреда: цифровой образ человека отделяется от носителя, воспроизводится без его участия и используется для формирования у адресата ложного представления об источнике сообщения, воле или поведении идентифицируемого лица. Возникает особая форма посягательства на цифровую идентичность — совокупность данных и внешних признаков, посредством которых человек распознается и действует в информационной среде [12, с. 124–129].

Опасность дипфейка проявляется по нескольким направлениям. Он способен усиливать убедительность обмана при хищении денежных средств; создавать компрометирующие материалы для вымогательства; имитировать публичные заявления; использоваться в несанкционированном интимном контенте; маскировать личность виновного; подрывать доказательственную достоверность аудио- и видеозаписей. Банк России прямо относит подделку голоса и видеоизображения к растущим инструментам кибермошенничества и отмечает отсутствие доступных массовому пользователю способов надежной защиты [9, с. 11–12]. Одновременно технология имеет многочисленные правомерные применения — в кинематографе, образовании, переводе, рекламе и восстановлении культурного наследия. Поэтому уголовная политика не может строиться на презумпции вредоносности любого синтетического изображения.

Российский законодатель рассматривает проект № 718538-8, предусматривающий повышение ответственности за ряд преступлений, совершенных с использованием изображения или голоса, включая фальсифицированные либо искусственно созданные, а также биометрических персональных данных [3]. Проект затрагивает клевету, кражу, мошенничество, мошенничество в сфере компьютерной информации, вымогательство и причинение имущественного ущерба путем обмана или злоупотребления доверием. Верховный Суд Российской Федерации и Правительство Российской Федерации указали на недостаточность статистического обоснования, неопределенность терминологии, непоследовательность выбора составов и риск некорректной практики [4; 5]. По состоянию на июль 2026 г. проект сохраняет статус законодательной инициативы и не стал действующим законом.

Научная дискуссия также не выработала единой модели. Одни авторы предлагают квалифицирующий признак использования дипфейка [10, с. 97–105; 13], другие — самостоятельный состав за фальсификацию биометрических данных в целях облегчения либо сокрытия преступления [11, с. 95–110], третьи — отдельный запрет незаконного использования голоса и изображения [15, с. 372–377]. Представляется, что решение должно учитывать три требования: технологическую нейтральность уголовного закона, реальное повышение общественной опасности конкретного деяния и недопустимость дублирования уже существующих составов.

Цель настоящей статьи — определить пределы применения действующих уголовно-правовых норм к преступному использованию дипфейков и обосновать точечную модель совершенствования законодательства. Научная новизна состоит в предложении гибридного подхода, сочетающего общее определение синтетического аудиовизуального материала, ограниченный учет способа совершения преступления и специальную криминализацию несанкционированных интимных дипфейков.

1. Дипфейк как уголовно-правовой феномен и средство посягательства

В техническом смысле дипфейк представляет собой полностью или частично сгенерированный либо существенно измененный аудио-, визуальный или аудиовизуальный материал, создающий реалистичное впечатление, что определенное лицо произносило слова, совершало действия или находилось в обстоятельствах, которых в действительности не было. Для уголовного закона термин должен описывать не способ машинного обучения, а юридически значимый результат: достоверную имитацию идентифицируемого человека, способную воздействовать на волю адресата либо причинить вред охраняемым интересам. Привязка к конкретной нейросетевой архитектуре быстро устареет и создаст обходные пути для иных технологий синтеза.

Следует различать три уровня. Первый — нейтральное создание синтетического материала без противоправной цели. Второй — нарушение личных неимущественных прав, которое может повлечь удаление контента, компенсацию морального вреда и защиту изображения, но не достигает уровня преступления. Третий — использование синтетического материала в механизме

умышленного преступления либо создание особо опасного контента, причиняющего самостоятельный существенный вред. Уголовное право должно концентрироваться на третьем уровне в силу принципов вины, справедливости и экономии репрессии.

В большинстве преступных сценариев дипфейк не является предметом посягательства и не образует самостоятельного общественно опасного результата. Он выполняет роль орудия или способа: создает ложный авторитет источника, повышает правдоподобие легенды, персонализирует угрозу, автоматизирует массовое распространение либо затрудняет идентификацию виновного. Ефремова и Русскевич справедливо характеризуют такую роль как инструментальную и возражают против всеобъемлющей самостоятельной криминализации технологии [10, с. 184–186]. Аналогичный подход соответствует общей логике уголовного права: нож, средство связи или программа сами по себе нейтральны, а их правовое значение определяется включением в механизм конкретного деяния.

Вместе с тем инструментальная природа не исключает повышенной общественной опасности. Дипфейк может одновременно: а) снижать критичность потерпевшего за счет имитации доверенного лица; б) масштабировать воздействие на неопределенный круг лиц; в) создавать устойчивый репутационный след, сохраняющийся после опровержения; г) затруднять доказывание умысла и происхождения материала; д) облегчать трансграничное совершение преступления. Однако наличие этих эффектов должно устанавливаться применительно к делу, а не презюмироваться из самого факта использования искусственного интеллекта.

Категория цифровой идентичности позволяет объединить разрозненные объекты защиты: изображение, голос, биометрические признаки, учетные данные и поведенческие паттерны. Но введение самостоятельного универсального состава «кражи цифровой идентичности» без четкого результата породило бы конкуренцию с нормами о неприкосновенности частной жизни, персональных данных, мошенничестве и неправомерном доступе к компьютерной информации. Более продуктивно рассматривать цифровую идентичность как межотраслевой объект и конкретизировать уголовную ответственность через охраняемый интерес и способ причинения вреда [12].

2. Квалификация преступлений, совершаемых с использованием дипфейков

При имущественном обмане исходной нормой выступает статья 159 УК РФ. Если виновный направляет потерпевшему синтетическое аудио- или видеосообщение от имени родственника, руководителя, сотрудника банка либо должностного лица и добивается добровольного перевода денежных средств, преступление совершается путем обмана человека. Само использование компьютерной программы, мессенджера или нейросети не переводит деяние в статью 159.6 УК РФ. Мошенничество в сфере компьютерной информации предполагает ввод, удаление, блокирование, модификацию компьютерной информации либо иное вмешательство в функционирование средств ее обработки и сетей, в результате которого происходит хищение [1; 6]. Пленум Верховного Суда подчеркивает необходимость разграничивать воздействие на человека и вмешательство в информационную систему [6; 7].

Если дипфейк применяется для прохождения автоматизированной биометрической аутентификации и инициирования операции без волевого решения потерпевшего или уполномоченного сотрудника, возможна статья 159.6 УК РФ. Здесь синтетический образ выступает техническим средством воздействия на систему. Если же система только подтверждает личность, а распоряжение имуществом осуществляется человеком под влиянием ложной видеосвязи, квалификация по статье 159 сохраняется. Следовательно, граница проходит не по факту использования цифровой технологии, а по адресату обмана и непосредственному механизму изъятия имущества.

Включение дипфейка как квалифицирующего признака кражи, предложенное законопроектом № 718538-8, вызывает системное возражение. Тайное хищение исключает передачу имущества потерпевшим под влиянием обмана. Использование изображения или голоса для получения доступа к помещению, устройству либо счету может облегчать кражу, но в ряде ситуаций оно образует подделку средства идентификации или вмешательство в информационную систему. Универсальное повышение санкции только за применение цифровой имитации не объясняет, почему сопоставимые способы преодоления контроля должны оцениваться мягче. Верховный Суд обоснованно указал на отсутствие критериев выбора именно имущественных составов [4]. При вымогательстве дипфейк может выполнять две функции. Во-первых, быть предметом угрозы распространения компрометирующего материала. Если материал синтетический, это не исключает статьи 163 УК РФ: для потерпевшего существенна реальность угрозы распространения сведений, способных причинить значительный вред его правам или законным интересам, а не документальная подлинность сведений. Во-вторых, имитация голоса или изображения авторитетного либо опасного лица усиливает убедительность требования. Специальная квалификация оправдана лишь тогда, когда синтетический материал существенно повысил способность угрозы подавить волю потер-

певшего.

Для клеветы по статье 128.1 УК РФ определяющим является распространение заведомо ложных сведений, порочащих честь и достоинство либо подрывающих репутацию. Дипфейк может быть формой сообщения таких сведений, но не всякая подделка изображения равнозначна клевете: материал должен выражать проверяемое утверждение о факте, быть распространен и осознаваться виновным как ложный. Правительство справедливо отметило, что использование подлинного голоса при распространении ложных сведений уже охватывается объективной стороной клеветы [5]. Поэтому квалифицирующая формула, одновременно называющая подлинные, фальсифицированные и искусственно созданные голос или изображение, чрезмерно широка.

Статья 137 УК РФ может применяться, если при создании или распространении дипфейка незаконно собираются либо распространяются сведения о частной жизни, составляющие личную или семейную тайну. Но синтетический интимный материал нередко изображает несуществующее событие и формально не раскрывает факты частной жизни. Потерпевшему причиняется сопоставимый или больший вред — сексуализированная объективация, репутационный ущерб, риск преследования, утрата контроля над цифровым образом, — однако конструкция статьи 137 ориентирована на сведения о реальной частной жизни. Этот пробел особенно заметен применительно к взрослым потерпевшим. Статьи 242 и 242.1 УК РФ требуют самостоятельной оценки. Создание порнографического материала путем переноса лица взрослого человека на чужое тело может охватываться статьей 242 при наличии незаконных изготовления или оборота порнографических материалов, но действующая норма не строится вокруг отсутствия согласия изображенного лица и не во всех случаях обеспечивает персонализированную защиту потерпевшего. Если используется образ несовершеннолетнего, статья 242.1 содержит более строгий запрет, однако при полностью синтетическом изображении возникают вопросы установления возраста изображенного и соотношения виртуального образа с понятием материала с порнографическими изображениями несовершеннолетних. Эти вопросы требуют разъяснения Пленума Верховного Суда и экспертных методик, но не должны решаться путем автоматического расширительного толкования уголовного закона.

Дипфейк способен быть способом совершения преступлений против общественной безопасности и основ конституционного строя: публичных призывов к террористической деятельности, заведомо ложного сообщения об акте терроризма, распространения общественно значимой ложной информации, реабилитации нацизма. Верховный Суд специально отметил, что законопроект № 718538-8 необъяснимо ограничен преимущественно преступлениями против собственности, хотя синтетическая имитация может использоваться в более опасных деяниях [4]. Этот аргумент подтверждает недостаток модели точечного добавления одинакового признака в случайно выбранные статьи Особенной части. Наконец, создание поддельной аудио- или видеозаписи для представления суду, следователю или иному органу может образовывать фальсификацию доказательств при наличии предусмотренных статьей 303 УК РФ признаков. Технология усложняет проверку достоверности, но не меняет объект преступления. Важнее развивать процессуальные стандарты аутентификации, судебную экспертизу и сохранение цифровой цепочки происхождения файла, чем вводить отдельный состав «создания синтетического доказательства» [17, с. 7–11].

3. Соотношение дипфейков, биометрических данных и статьи 272.1 УК РФ

Федеральным законом от 30 ноября 2024 г. № 421-ФЗ Уголовный кодекс дополнен статьей 272.1, устанавливающей ответственность за незаконные использование, передачу, сбор или хранение компьютерной информации, содержащей персональные данные, полученной незаконным путем, а также за создание ресурсов для ее незаконного хранения и распространения [2]. Квалифицированный состав выделяет специальные категории и биометрические персональные данные. Новелла усилила охрану исходных массивов данных, которые могут использоваться при обучении моделей и создании цифровых имитаций. Однако статья 272.1 не является общей нормой о дипфейках. Во-первых, предметом выступает компьютерная информация, содержащая персональные данные, полученная незаконным путем. Если фотографии и голосовые записи были размещены самим гражданином в открытом доступе либо получены законно, формальный признак незаконного происхождения может отсутствовать. Во-вторых, сгенерированный материал может содержать правдоподобный образ лица, но не воспроизводить конкретную исходную запись. В-третьих, ответственность по статье 272.1 связана с незаконным оборотом данных, а не с последующим использованием результата синтеза для обмана, шантажа или распространения порочащих сведений.

Квалификация по совокупности возможна, когда виновный сначала незаконно получает биометрические персональные данные, а затем использует созданный на их основе дипфейк для самостоятельного преступления. Например, неправомерное приобретение массива голосовых об-

разцов и последующее мошенничество образуют разные объекты и действия. Если же доступ к данным является способом подготовки хищения и полностью охватывается более специальной нормой, вопрос совокупности должен решаться с учетом положений о конкуренции и разъяснений по преступлениям в сфере компьютерной информации [7; 24].

Необходимо также различать биометрические персональные данные и изображение или голос как таковые. Законодательство о персональных данных связывает биометрию с физиологическими и биологическими особенностями, используемыми оператором для установления личности. Обычная фотография или аудиозапись не всегда обрабатывается в целях идентификации и потому не автоматически имеет биометрический статус. Законопроект № 718538-8 пытается охватить одновременно изображение, голос и биометрические данные, но тем самым соединяет разные правовые категории и создает неопределенность [3; 5]. Например, И.Н. Мосечкин предлагает криминализовать фальсификацию биометрических данных в целях облегчения или сокрытия преступления, используя конструктивное сходство с подделкой документов [11, с. 105–110]. Подход заслуживает внимания, поскольку фиксирует специальную цель и не ограничивается дипфейк-технологией. Вместе с тем самостоятельный состав за подготовительную фальсификацию может привести к двойному вменению, когда подделка уже реализована в оконченном мошенничестве, незаконном пересечении контроля или ином преступлении. Более экономной представляется модель, при которой самостоятельная ответственность возникает лишь за создание опасного рынка средств подмены идентичности либо за специальные виды контента, а в остальных случаях способ учитывается в квалификации и наказании за основное преступление.

4. Критическая оценка законопроекта № 718538-8

Законопроект № 718538-8 имеет очевидное достоинство: он признает, что цифровая имитация личности способна качественно усиливать традиционные преступные способы и требует реакции уголовной политики. Авторы отказались от полного запрета технологии и сосредоточились на использовании изображения, голоса и биометрических данных при совершении конкретных преступлений. Тем не менее предложенная конструкция не отвечает требованиям системности и правовой определенности.

Первый недостаток — отсутствие легального определения. Формула «фальсифицированные или искусственно созданные» не устанавливает степень изменения материала, критерий реалистичности, необходимость идентифицируемости лица и значение согласия. Простая цветокоррекция, монтаж сатирического ролика или озвучивание актером также могут быть искусственно созданными. Правительство указало, что неопределенность формулировки создает риск неоднозначного и произвольного применения [5].

Второй недостаток — непоследовательный перечень преступлений. Если основанием усиления ответственности является повышенная убедительность ложного образа, признак применим не только к собственности, но и к угрозам общественной безопасности, экстремистским призывам, воспрепятствованию правосудию, незаконному доступу и преступлениям против половой неприкосновенности. Добавление одинаковой конструкции в несколько статей неизбежно оставит новые пробелы и потребует последующих поправок. Общая часть УК РФ лучше приспособлена к учету универсального способа, но и там формулировка должна быть существенно ограничена.

Третий недостаток — смешение различных форм общественной опасности. Использование подлинного изображения, незаконно полученной биометрии и полностью синтетического дипфейка не тождественно. В первом случае может нарушаться право на изображение; во втором — режим персональных данных; в третьем — создается ложная цифровая репрезентация. Для уголовной ответственности существенны цель, способ воздействия и последствия, а не только тип использованного материала.

Четвертый недостаток — отсутствие доказанной дифференциации санкций. Верховный Суд отметил, что пояснительная записка не содержит убедительных сведений и статистики о недостаточности действующего регулирования [4]. Сам по себе новый или технически сложный способ не обязательно повышает общественную опасность настолько, чтобы изменять категорию преступления. Например, примитивный аудиофильтр может оказаться менее убедительным, чем профессиональная психологическая манипуляция без искусственного интеллекта.

Пятый недостаток — риск конкуренции с новыми нормами о персональных данных. Законопроект разрабатывался параллельно с проектом, впоследствии ставшим статьей 272.1 УК РФ. Верховный Суд указывал на сходство регулирования незаконного использования биометрических данных [4]. После вступления статьи 272.1 в силу требуется заново оценить пределы дополнительной криминализации, чтобы не наказывать дважды за один и тот же элемент поведения. Таким образом, проект нуждается не в редакционной корректировке, а в смене модели. Необходимо отказаться от перечисления отдельных составов, определить юридически значимое понятие синте-

тического материала и выделить те ситуации, где существующие нормы действительно не обеспечивают защиту.

5. Зарубежные ориентиры: прозрачность, адресная криминализация и удаление контента

Зарубежные правопорядки демонстрируют отказ от единой универсальной уголовно-правовой нормы. Регламент Европейского союза об искусственном интеллекте закрепляет обязанность раскрывать искусственное происхождение или манипулирование контентом, относимым к дипфейкам, с учетом специальных исключений для художественных, сатирических и иных произведений [19]. Эта модель преимущественно превентивна: она снижает риск введения в заблуждение до наступления вреда и не подменяет уголовные запреты государств-членов.

В Соединенных Штатах федеральный TAKE IT DOWN Act, подписанный 19 мая 2025 г., установил уголовный запрет умышленного распространения определенных несанкционированных интимных визуальных изображений, включая цифровые подделки, и обязанность охватываемых платформ оперативно удалять такой контент [20]. Принципиально, что законодатель избрал не абстрактное «использование дипфейка», а конкретный вред — сексуальную эксплуатацию и утрату контроля над интимным образом. На уровне штатов регулирование дополнительно охватывает выборы, мошенничество и имперсонацию [13; 22].

Сравнительный материал показывает три полезных ориентира. Во-первых, маркировка и прослеживаемость синтетического контента должны развиваться преимущественно в информационном и платформенном регулировании. Во-вторых, уголовная ответственность оправдана при конкретизированном вреде и умышленной форме вины. В-третьих, обязанность удаления и сохранения доказательств может быть не менее эффективной для потерпевшего, чем повышение санкции. Российская модель должна сочетать уголовно-правовую охрану с быстрыми процедурами блокировки, подтверждением происхождения контента и доступом к специализированной экспертизе. Прямое заимствование зарубежных решений невозможно из-за различий в системе объектов уголовно-правовой охраны и платформенной ответственности. Однако адресная защита от интимных дипфейков и обязательная прозрачность синтетического контента соответствуют принципу минимально необходимого уголовного вмешательства и могут быть адаптированы без создания общего запрета на генеративные технологии.

6. Предлагаемая модель уголовно-правового регулирования

Предлагаемая модель включает четыре взаимосвязанных элемента. Первый — легальное определение, применимое не ко всему обороту искусственного интеллекта, а к нормам, где происхождение контента имеет значение. Под синтетическим аудиовизуальным материалом следует понимать созданные или существенно измененные с использованием автоматизированной системы изображение, звук либо их сочетание, которые способны сформировать у разумного адресата достоверное ложное впечатление, что идентифицируемое лицо совершало действия, произносило слова или находилось в обстоятельствах, не имевших места. Определение должно исключать техническую обработку, не изменяющую смысл, и учитывать явную маркировку сатиры или художественного произведения.

Второй элемент — ограниченное обстоятельство, отягчающее наказание, а не безусловный квалифицирующий признак множества составов. Пункт части первой статьи 63 УК РФ можно сформулировать следующим образом: «совершение умышленного преступления с использованием синтетического аудиовизуального материала, заведомо созданного для имитации другого лица, если такое использование существенно облегчило совершение преступления, повысило способность деяния причинить вред либо затруднило его выявление». Указание на умышленный характер, заведомость и существенное влияние исключает автоматическое усиление наказания за любое применение нейросети.

Общее отягчающее обстоятельство не должно учитываться повторно, если соответствующий признак включен в состав преступления, что прямо следует из части второй статьи 63 УК РФ. Суд обязан мотивировать, каким образом синтетическая имитация увеличила опасность. Такой подход позволяет охватить и имущественные, и террористические, и репутационные преступления без хаотичного редактирования Особенной части.

Третий элемент — специальная криминализация несанкционированного интимного дипфейка. Здесь действующие статьи 137 и 242 УК РФ не всегда отражают основной вред и отсутствие согласия потерпевшего. Целесообразно дополнить главу 19 УК РФ статьей 137.1, устанавливающей ответственность за умышленные создание с целью распространения, распространение, публичную демонстрацию либо угрозу распространения синтетического изображения идентифицируемого лица в интимной или сексуализированной ситуации без его согласия, если деяние причинило существенный вред правам и законным интересам. Квалифицирующими признаками могут быть совершение в отношении несовершеннолетнего, из корыстных побуждений, группой лиц, с использованием служебного положения, а также наступ-

ление тяжких последствий.

Предлагаемый состав должен содержать исключения для добросовестной деятельности правоохранительных органов, науки, медицины и искусства, если материал не предназначен для представления реального лица как участника интимного события и не создает неоправданного риска причинения ему вреда. Согласие должно быть конкретным: согласие на публикацию фотографии не означает согласия на ее преобразование в сексуализированный контент. Угроза распространения интимного дипфейка при имущественном требовании квалифицируется по совокупности со статьей 163 УК РФ, поскольку защищаемые объекты различаются.

Четвертый элемент — разъяснения Верховного Суда. В постановлениях о мошенничестве и компьютерных преступлениях следует закрепить: а) использование дипфейка для обмана человека квалифицируется по статье 159, а для непосредственного воздействия на автоматизированную систему — по статье 159.6; б) статья 272.1 применяется только при наличии незаконно полученной компьютерной информации с персональными данными и не поглощает последующее преступное использование синтетического материала; в) достоверность и происхождение аудио- и видеозаписи должны проверяться с учетом метаданных, цепочки хранения и экспертных исследований.

Не следует включать в статью 63 общий признак «использование искусственного интеллекта». ИИ может применяться для планирования маршрута, перевода текста, поиска информации или автоматизации законной операции, не увеличивая опасности. Уголовно значим не технологический бренд, а специально созданная ложная репрезентация личности и ее существенная роль в преступлении. Технологически нейтральный закон должен одинаково оценивать дипфейк, профессиональный монтаж, имитацию актером и иной способ, если они создают сопоставимый эффект, но учитывать повышенную масштабируемость и реалистичность автоматизированного синтеза.

Предупреждение преступлений требует мер за пределами УК РФ: обязательной маркировки коммерчески распространяемого синтетического контента; технических стандартов происхождения и цифровых водяных знаков; ускоренной процедуры удаления; обязанности платформ сохранять сведения для расследования; финансовой и медиаграмотности; подготовки экспертов. Приказ Генеральной прокуратуры № 746 уже предусматривает статистический показатель использования технологии дипфейк, что создает основу для последующей оценки распространенности [8; 10, с. 177–179]. До накопления репрезентативной статистики масштабная пенализация преждевременна. В доказывании ключевое значение имеет не только установление синтетического характера файла, но и его связь с обвиняемым, осведомленность о ложности и направленность умысла. Вероятностный вывод алгоритма обнаружения не может автоматически заменять судебную экспертизу и совокупность доказательств. Необходимо фиксировать исходные файлы, метаданные, журналы генерации, платежи за сервисы, переписку, историю загрузок и технические следы распространения. Иначе существует риск «обратного дивиденда лжеца», когда виновный объявляет подлинную запись дипфейком и использует общее недоверие к цифровым материалам.

Предложенная конструкция отвечает принципу ultima ratio. Она сохраняет применение действующих норм к большинству преступлений, учитывает реальное усиление опасности на стадии назначения наказания и закрывает наиболее очевидный персональный пробел — интимные синтетические материалы.

Заключение

Проведенное исследование позволяет сформулировать следующие выводы.

Дипфейк является технологически нейтральным результатом синтеза и в большинстве преступлений выполняет функцию орудия или способа, а не самостоятельного объекта уголовно-правового запрета. Универсальная криминализация создания синтетического контента нарушила бы принцип экономии уголовной репрессии и создала бы риск преследования правомерной творческой, образовательной и коммерческой деятельности.

Действующие нормы УК РФ в значительной мере позволяют квалифицировать преступное использование дипфейков: статья 159 применяется при обмане человека, статья 159.6 — при непосредственном вмешательстве в функционирование информационной системы; статьи 128.1, 163, 205.2, 207, 242, 242.1, 303 и иные нормы охватывают соответствующие общественно опасные результаты. Технологический способ не заменяет установление всех признаков конкретного состава.

Статья 272.1 УК РФ защищает незаконно полученную компьютерную информацию, содержащую персональные, включая биометрические, данные, но не является общей нормой о дипфейках. Ее применение возможно самостоятельно либо по совокупности, когда незаконный оборот исходных данных предшествует иному преступлению.

Список литературы:

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 10 июня

2026 г.) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

[2] О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 30 ноября 2024 г. № 421-ФЗ // Собрание законодательства Российской Федерации. 2024. № 49. Ст. 7423.

[3] О внесении изменений в Уголовный кодекс Российской Федерации : проект федерального закона № 718538-8. URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 31.07.2026).

[4] Официальный отзыв Верховного Суда Российской Федерации на проект федерального закона № 718538-8 от 20 июня 2024 г. № 4-ВС-3444/24. URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 31.07.2026).

[5] Официальный отзыв Правительства Российской Федерации на проект федерального закона № 718538-8 от 22 июля 2024 г. № ДГ-П4-23438. URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 31.07.2026).

[6] О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 (ред. от 15 декабря 2022 г.) // Бюллетень Верховного Суда Российской Федерации. 2018. № 2.

[7] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // Бюллетень Верховного Суда Российской Федерации. 2023. № 2.

[8] О государственном едином статистическом учете данных о состоянии преступности, а также о сообщениях о преступлениях, следственной работе, дознании, прокурорском надзоре : приказ Генеральной прокуратуры Российской Федерации от 9 декабря 2022 г. № 746. Доступ из СПС «КонсультантПлюс».

[9] Противодействие новым угрозам кибермошенничества : информационно-аналитический материал Банка России. Москва, 2025. URL: https://www.cbr.ru/content/document/file/174841/cyberfraudcounteringnewthreats.pdf (дата обращения: 31.07.2026).

[10] Ефремова М. А., Русскевич Е. А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. Т. 15, № 2. С. 97–105. DOI: 10.37973/VESTNIKKUI-2024-56-13..

[11] Мосечкин И. Н. Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования // Вестник Санкт-Петербургского университета. Право. 2025. Т. 16, вып. 1. С. 95–110. DOI: 10.21638/spbu14.2025.107..

[12] Ефремова М. А. Цифровая идентичность: проблемы уголовно-правовой охраны // Правопорядок: история, теория, практика. 2025. № 3 (46). С. 124–129.

[13] Джагарян Н. В., Сафонова А. М. К вопросу об уголовной ответственности за использование технологии дипфейка в Российской Федерации (с учетом опыта Соединенных Штатов Америки) // Вестник Сургутского государственного университета. 2025. Т. 13, № 1. DOI: 10.35266/2949-3455-2025-3-9..

[14] Морозов В. И., Лосев С. Г. Уголовно-правовая оценка использования «дипфейка» при совершении преступлений // Право в эпоху искусственного интеллекта: перспективные вызовы и современные задачи : сборник научных статей. Тюмень : ТюмГУ-Press, 2024. С. 387–390.

[15] Белых Е. С., Грабчев М. А. К вопросу о введении уголовной ответственности за изготовление дипфейков в преступных целях // Евразийский юридический журнал. 2024. № 5. С. 372–377. DOI: 10.24412/2224-9133-2024-5-372-377..

[16] Дремлюга Р. И. Уголовно-правовая охрана цифровой экономики и информационного общества от киберпреступных посягательств: доктрина, закон, правоприменение : монография. Москва : Юрлитинформ, 2022. 328 с.

[17] Апостолова Н. Н. Достоверность доказательств и технологии дипфейка // Российский судья. 2023. № 11. С. 7–11.

[18] Калятин В. О. Дипфейк как правовая проблема: новые угрозы или новые возможности? // Закон. 2022. № 7. С. 87–103.

[19] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. 2024. L 2024/1689.

[20] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act), Pub. L. No. 119-12, May 19, 2025.

[21] Kugler M. B., Pace C. Deepfake Privacy: Attitudes and Regulation // Northwestern University Law Review. 2021. Vol. 116. P. 611–680.

[22] Lussier N. Nonconsensual Deepfakes: Detecting and Regulating the Rising Threat to Privacy // Idaho Law Review. 2022. Vol. 58, no. 1. P. 353–388.

[23] Mansoor S. I. U. Legal Implications of Deepfake Technology: In the Context of Manipulation, Privacy, and Identity Theft // Central University of Kashmir Law Review. 2024. No. 4. P. 65–92.

[24] Русскевич Е. А. О совокупности преступлений в сфере компьютерной информации с дру-

гими преступлениями // Уголовное право. 2025. № 4. С. 76–84.

References:

[1] Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (as amended on June 10, 2026) // Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

[2] On Amendments to the Criminal Code of the Russian Federation: Federal Law of November 30, 2024 No. 421-FZ // Collection of Legislation of the Russian Federation. 2024. № 49. Art. 7423.

[3] On Amending the Criminal Code of the Russian Federation: Draft Federal Law No. 718538-8. URL: https://sozd.duma.gov.ru/bill/718538-8 (access date: 31.07.2026).

[4] Official recall of the Supreme Court of the Russian Federation on the draft federal law No. 718538-8 of June 20, 2024 No. 4-VS-3444/24. URL: https://sozd.duma.gov.ru/bill/718538-8 (access date: 31.07.2026).

[5] Official response of the Government of the Russian Federation to the draft federal law No. 718538-8 of July 22, 2024 No. DG-P4 -23438. URL: https://sozd.duma.gov.ru/bill/718538-8 (access date: 31.07.2026).

[6] On judicial practice in cases of fraud, misappropriation and embezzlement: Resolution of the Plenum of the Supreme Court of the Russian Federation of November 30, 2017 No. 48 (as amended on December 15, 2022) // Bulletin of the Supreme Court of the Russian Federation. 2018. № 2.

[7] On certain issues of judicial practice in criminal cases of crimes in the field of computer information, as well as other crimes committed using electronic or information and telecommunication networks, including the Internet: Resolution of the Plenum of the Supreme Court of the Russian Federation of December 15, 2022 No. 37 // Bulletin of the Supreme Court of the Russian Federation. 2023. № 2.

[8] On the state unified statistical accounting of data on the state of crime, as well as on reports of crimes, investigative work, inquiry, prosecutor's supervision: order of the General Prosecutor's Office of the Russian Federation of December 9, 2022 No. 746. Access from SPS "ConsultantPlus.".

[9] Countering new cyber fraud threats: Bank of Russia information and analytical material. Moscow, 2025. URL: https://www.cbr.ru/content/document/file/174841/cyberfraudcounteringnewthreats.pdf (дата обращения: 31.07.2026).

[10] Efremova M.A., Russkevich E.A. Deepfake (deepfake) and the criminal law // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2024. VOL. 15, NO. 2. S. 97-105. DOI: 10.37973/VESTNIKKUI-2024-56-13..

[11] Mosechkin I.N. Deepfake technologies and biometric data: areas of criminal law regulation // Bulletin of St. Petersburg University. Right. 2025. Vol. 16, no. 1. S. 95-110. DOI: 10.21638/spbu14.2025.107..

[12] Efremova M. A. Digital identity: problems of criminal law protection // Law and order: history, theory, practice. 2025. № 3 (46). S. 124-129.

[13] Dzhagaryan N.V., Safonova A.M. On the issue of criminal liability for the use of deepfake technology in the Russian Federation (taking into account the experience of the United States of America) // Bulletin of Surgut State University. 2025. T. 13, NO. 1. DOI: 10.35266/2949-3455-2025-3-9..

[14] Morozov V. I., Losev S. G. Criminal law assessment of the use of "deepfake" in committing crimes // Law in the era of artificial intelligence: promising challenges and modern tasks: a collection of scientific articles. Tyumen: Tyumen State University-Press, 2024. S. 387-390.

[15] Belykh E. S., Grabchev M. A. On the issue of introducing criminal liability for the manufacture of deepfakes for criminal purposes // Eurasian Legal Journal. 2024. № 5. PP. 372-377. DOI: 10.24412/2224-9133-2024-5-372-377..

[16] Dremlyuga R. I. Criminal law protection of the digital economy and information society from cybercriminal encroachments: doctrine, law, law enforcement: monograph. Moscow: Yurlitinform, 2022. 328 pp.

[17] Apostolova N. N. Reliability of evidence and deepfake technology // Russian judge. 2023. № 11. S. 7-11.

[18] Kalyatin V.O. Deepfake as a legal problem: new threats or new opportunities? // Law. 2022. № 7. S. 87-103.

[19] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. 2024. L 2024/1689.

[20] Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act), Pub. L. No. 119-12, May 19, 2025.

[21] Kugler M. B., Pace C. Deepfake Privacy: Attitudes and Regulation // Northwestern University Law Review. 2021. Vol. 116. P. 611–680.

[22] Lussier N. Nonconsensual Deepfakes: Detecting and Regulating the Rising Threat to Privacy // Idaho Law Review. 2022. Vol. 58, no. 1. P. 353–388.

[23] Mansoor S. I. U. Legal Implications of Deepfake Technology: In the Context of Manipulation, Privacy, and Identity Theft // Central University of Kashmir Law Review. 2024. No. 4. P. 65–92.

[24] Russkevich E. A. On the totality of crimes in the field of computer information with other crimes // Criminal law. 2025. № 4. S. 76-84.