

Дата поступления рукописи в редакцию: 05.06.2026 г.
Дата принятия рукописи в печать: 25.06.2026 г.

DOI: 10.24412/2782-3849-2026-6-200-204

МАЙСТРЕНКО Григорий Александрович,

кандидат юридических наук, старший научный сотрудник Научно-исследовательского института
Федеральной службы исполнения наказаний России, Москва, Россия,

e-mail: g.maystrenko@yandex.ru

КРИМИНАЛЬНОЕ ИСПОЛЬЗОВАНИЕ ДИПФЕЙКОВ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРОБЛЕМЫ КВАЛИФИКАЦИИ И ДОКАЗЫВАНИЯ

Аннотация. В статье исследуется криминальное использование дипфейков и иных синтетических аудио-, фото- и видеоматериалов, создаваемых с применением технологий искусственного интеллекта. Обосновывается, что дипфейк не должен превращаться в самостоятельный универсальный состав преступления: общественная опасность возникает не из факта алгоритмической генерации, а из использования результата при мошенничестве, вымогательстве, нарушении неприкосновенности частной жизни, незаконном обороте персональных и биометрических данных, фальсификации доказательств и распространении социально опасной дезинформации. Особое внимание уделено проблеме проверки цифровых материалов в уголовном судопроизводстве.

Ключевые слова: дипфейк, искусственный интеллект, уголовное право, уголовный процесс, цифровые доказательства, электронные следы, биометрические персональные данные, мошенничество, фальсификация доказательств, судебная экспертиза.

MAISTRENKO Grigoriy Aleksandrovich,

PhD in Law, Senior Researcher of Research Institute of the Federal Penitentiary Service of Russia, Moscow,
Russia

CRIMINAL USE OF DEEPPFAKES AND ARTIFICIAL INTELLIGENCE: QUALIFICATION AND PROOF ISSUES

Annotation. The article examines the criminal use of deepfakes and synthetic audiovisual materials generated by artificial intelligence systems. The author argues that deepfake technology as such should not be criminalized in isolation from its socially harmful use. Criminal law should respond to the use of synthetic content as a means of fraud, extortion, privacy invasion, illegal processing of biometric data, evidence falsification and dangerous disinformation. The article also proposes procedural standards for verifying digital evidence and preserving its integrity in criminal proceedings.

Key words: deepfake, artificial intelligence, criminal law, criminal procedure, digital evidence, electronic traces, biometric personal data, fraud, evidence falsification, forensic examination.

Генеративный искусственный интеллект изменил содержание цифровой преступности. Если классическая компьютерная преступность была связана преимущественно с неправомерным доступом, вредоносными программами и оборотом охраняемой информации, то современная ИИ-преступность все чаще строится на имитации доверия. Синтезированный голос руководителя, «видеозвонок» родственника, искусственное обращение должностного лица или порочащий интимный ролик воздействуют на потерпевшего сильнее, чем обычный текстовый обман. Аудиовизуальная убедительность становится самостоятельным криминальным ресурсом. Для уголовного права это создает

вопрос о пределах криминализации. Технология глубокого синтеза имеет законные сферы применения: образование, кинопроизводство, реставрация архивных материалов, научная визуализация, сопровождение лиц с ограниченными возможностями. Поэтому ошибочно объявлять преступным сам дипфейк как технологический результат. Но столь же ошибочно не замечать, что реалистичная имитация голоса и лица превращается в средство хищения, давления, дискредитации, незаконной обработки биометрии и фальсификации доказательств. Действующий УК РФ уже содержит нормы, применимые к таким деяниям, включая мошенничество, вымогательство,

клевету, нарушение неприкосновенности частной жизни, преступления в сфере компьютерной информации и фальсификацию доказательств [5].

Для уголовного процесса проблема состоит в ином: суд и следствие больше не могут исходить из того, что аудио- или видеозапись сама по себе обладает повышенной доказательственной силой. УПК РФ не выделяет электронные доказательства в самостоятельный вид, а цифровые файлы обычно вводятся через категории вещественных доказательств, иных документов, протоколов следственных действий или заключений эксперта [6]. В условиях дипфейков такая конструкция сохраняет формальную пригодность, но требует дополнительных гарантий проверки происхождения, целостности и технической подлинности цифрового материала.

Дипфейк следует понимать как синтетический или существенно модифицированный аудиовизуальный материал, создающий у адресата впечатление, что конкретное лицо произнесло слова, совершило действия или находилось в обстоятельствах, которых в действительности не было. Его особенность состоит не только в недостоверности содержания, но и в присвоении идентичности. Виновный использует доверие, которое потерпевший связывает с голосом, лицом, статусом или социальной ролью другого человека. Именно поэтому дипфейк отличается от обычного монтажа, поддельного аккаунта или клеветнического сообщения.

Наиболее очевидный сценарий - это мошенничество. Синтезированный голос директора организации может использоваться для распоряжения о переводе денежных средств; «видеосообщение» родственника - для выманивания денег; имитация сотрудника банка - для получения кода доступа. Квалификация в таких случаях должна строиться по признакам хищения путем обмана или злоупотребления доверием. Пленум Верховного Суда РФ при разъяснении мошенничества исходит из значения способа введения потерпевшего в заблуждение, что позволяет включать цифровую имитацию в традиционную конструкцию состава [7]. Однако использование дипфейка повышает интенсивность обмана. Текстовое сообщение обычно воспринимается с большей осторожностью, чем голос или изображение знакомого лица. Поэтому дипфейк не должен растворяться в общем признаке обмана. В составах, где имитация личности объективно облегчает причинение вреда, ее целесообразно закреплять как квалифицирующий способ. Речь идет прежде всего о мошенничестве,

вымогательстве, клевете, нарушении неприкосновенности частной жизни и фальсификации доказательств.

Второй блок рисков связан с вымогательством и принуждением. Синтетический интимный материал, «компрометирующее» видео или аудиозапись с угрозой распространения могут использоваться для получения денег, имущественных прав, передачи доступа к аккаунтам или совершения действий в интересах виновного. В зависимости от содержания угрозы содеянное может квалифицироваться по статьям о вымогательстве, нарушении неприкосновенности частной жизни, обороте порнографических материалов, клевете или незаконной обработке персональных данных.

Третий блок - публично опасные дипфейки. Синтетическое обращение должностного лица, военного командира, руководителя медицинской организации или оператора критической инфраструктуры способно вызвать панику, нарушить управление, спровоцировать незаконные действия. В литературе справедливо подчеркивается, что общественная опасность дипфейка состоит не в самой технологии, а в ее способности повышать убедительность вредоносной информации [8]. Поэтому уголовно-правовая реакция должна зависеть от содержания сообщения и наступивших последствий, а не от технологического ярлыка.

Дипфейк почти всегда использует признаки конкретного человека: лицо, голос, мимику, походку, интонацию. Эти признаки имеют двойственную природу. С одной стороны, они являются элементами индивидуального образа личности; с другой — могут использоваться для автоматизированной идентификации и аутентификации. Российское законодательство о биометрической идентификации исходит из повышенного режима охраны таких данных [9]. Поэтому криминальное использование дипфейков следует рассматривать как посягательство не только на информацию, но и на цифровую идентичность. Статья 272.1 УК РФ имеет для данной темы принципиальное значение. Она охватывает незаконное использование, передачу, сбор и хранение компьютерной информации, содержащей персональные данные, полученной неправомерным путем, и предусматривает повышенную ответственность за деяния с биометрическими персональными данными [10]. При создании голосового клона или видеоимитации злоумышленник обычно использует массив исходных аудио- и видеоданных, которые могут быть получены через утечку, скрытую запись, неправомерный доступ к аккаунту или сбор из закрытых источников.

В то же время действующая

редакция статьи 272.1 УК РФ ориентирована преимущественно на незаконный оборот уже имеющейся компьютерной информации. Она не всегда прямо отвечает на вопрос, охватывается ли алгоритмическая переработка биометрических данных в новый синтетический объект, если результат не был распространен либо если исходные данные были собраны из открытых источников. Поэтому в 2026 году в Государственную Думу был внесен законопроект № 1133088-8, направленный на расширение ответственности применительно к незаконной автоматизированной обработке персональных данных при создании дипфейков [11].

Поддерживая саму постановку проблемы, необходимо предостеречь от чрезмерно широкой криминализации. Автоматизированная обработка изображения или голоса не должна становиться преступлением сама по себе. Уголовная ответственность допустима при наличии совокупности признаков: незаконность получения или использования данных, отсутствие согласия субъекта, вредоносная цель, создание угрозы существенного вреда либо использование результата в ином преступлении. Иначе уголовный закон будет распространяться на бытовые, образовательные и художественные практики, что противоречит принципу правовой определенности. Оптимальной, на наш взгляд, представляется дифференцированная модель. Если исходные биометрические данные получены незаконно, применима статья 272.1 УК РФ в совокупности с иными составами при наличии самостоятельного вреда. Если данные получены законно, но использованы вопреки цели согласия, уголовная ответственность должна наступать только при наличии обмана, вымогательства, нарушения частной жизни, клеветы или иного конкретного состава. Если данные были общедоступны, решающим должен быть не факт обработки, а вредоносное использование синтетического результата.

Главный вызов дипфейков для уголовного процесса состоит в разрушении визуальной очевидности доказательства. Видеоизображение и голосовая запись традиционно воспринимались как более убедительные источники, чем текст или пересказ. Но синтетический материал может выглядеть правдоподобнее реальной записи, а подлинная запись может быть объявлена дипфейком как линия защиты. Поэтому суд должен оценивать не только содержание файла, но и его происхождение, целостность, техническую историю и связь с иными доказательствами.

Минимальный процессуальный стандарт верификации должен включать четыре элемента. Первый - фиксация источника получения: устройство, аккаунт, ссылка, мессенджер,

облачное хранилище, камера наблюдения. Второй - обеспечение целостности: создание копии, расчет контрольных сумм, описание носителя и программной среды. Третий - установление истории распространения: кем, когда и через какой канал материал был получен или передан. Четвертый - техническая проверка признаков синтетической генерации или существенной модификации. Такой стандарт не требует немедленного создания новой системы доказательств, но предполагает развитие процессуальных правил для электронных материалов. В научной литературе обоснованно отмечается, что цифровые доказательства отличаются от бумажных документов зависимостью от метаданных, формата файла, журналов событий, программного окружения и цепочки хранения. [1] Без учета этих характеристик проверка допустимости и достоверности становится формальной. Особую роль должен играть специалист. При осмотре телефона, компьютера, облачного сервиса или сетевой страницы следователь может не обладать знаниями, необходимыми для корректного изъятия данных. Ошибка при копировании способна уничтожить метаданные, изменить дату файла или создать сомнение в целостности материала. Участие специалиста в исследовании электронных доказательств поэтому является не технической услугой, а процессуальной гарантией достоверности [4].

Судебная экспертиза по делам о дипфейках должна быть комплексной. Традиционная фоноскопическая или видеотехническая экспертиза сохраняет значение, но должна дополняться анализом артефактов генерации, синхронизации голоса и мимики, следов компрессии, метаданных, сетевых журналов и признаков использования конкретных моделей синтеза. Общие основы судебно-экспертной деятельности закреплены федеральным законом, однако методики исследования синтетического аудиовизуального контента нуждаются в развитии [12]. Процессуальная проблема возникает и при использовании результатов оперативно-розыскной деятельности. Если аудио- или видеоматериал был получен, очищен, усилен, реконструирован либо смонтирован с применением ИИ, это обстоятельство должно быть раскрыто при введении материала в уголовное дело. Закон об оперативно-розыскной деятельности не освобождает сторону обвинения от обязанности показать, что представленный суду объект является именно тем цифровым следом, который был зафиксирован в ходе мероприятия [13].

Дипфейк может использоваться не только для совершения преступления, но и для

создания ложной доказательственной базы. Если синтетическая запись предъявляется как реальная фиксация события, речь может идти о фальсификации доказательств. В таких случаях техническая поддельность материала является лишь первым уровнем анализа. Следствию необходимо установить, кто создал файл, кто передал его участникам процесса, знал ли передающий о синтетическом происхождении и с какой целью материал вводился в уголовное дело.

Граница между допустимой реконструкцией и фальсификацией должна быть четкой. Реконструкция события, визуализация версии, схема движения лиц или предметов допустимы как вспомогательный материал, если их искусственный характер прямо обозначен, исходные данные раскрыты, а содержание не подменяет доказательство. Фальсификация возникает тогда, когда синтетический файл предъявляется как подлинная запись факта или как реальный результат оперативно-розыскного мероприятия. Следует закрепить процессуальное правило: любой аудио-, фото- или видеоматериал, подвергавшийся алгоритмической обработке после фиксации события, должен сопровождаться указанием на характер обработки, использованное программное средство, цель обработки и наличие исходника. Допустимыми без специального раскрытия могут быть только операции, не изменяющие содержание: копирование, архивирование, создание резервной копии, конвертация при сохранении исходного файла и контрольной суммы.

Значение имеет и международный аспект. Дипфейки часто создаются на зарубежных платформах, распространяются через трансграничные сервисы и хранятся в облачной инфраструктуре. Конвенция ООН против киберпреступности формирует рамку международного сотрудничества и обмена электронными доказательствами [14]. Для российской практики это означает необходимость описывать цифровой объект технически точно: хеш-сумма, аккаунт, ссылка, время публикации, IP-адреса, журналы доступа, параметры файла. Без такой детализации международный запрос может оказаться неисполнимым.

Список литературы:

[1] Изаксон Р.А. Цифровизация уголовного судопроизводства: цифровое уголовное дело, искусственный интеллект и электронные доказательства // CyberLeninka. 2025.

[2] Морозова И.Г. К вопросу о необходимости правового регулирования дипфейков // CyberLeninka. 2025.

[3] Стародубов А.А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024.

[4] Туршин А.И. Участие специалиста в исследовании электронных доказательств в уголовном судопроизводстве // ВВ: Административное право и практика администрирования. 2025.

[5] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

[6] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства РФ. 2001. № 52 (ч. I). Ст. 4921.

[7] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда РФ. 2018. № 2.

[8] Стародубов А.А. Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. 2024. URL: <https://vestnikkui.ru/ru/nauka/article/75454/view> (дата обращения: 03.06.2026).

[9] Федеральный закон от 29.12.2022 № 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных...» // Собрание законодательства РФ. 2023. № 1 (ч. I). Ст. 20.

[10] УК РФ. Ст. 272.1 «Незаконное использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные...» // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/deefeade19003ba8266e85fbf42fc31f60ed3c698/ (дата обращения: 03.06.2026).

[11] Законопроект № 1133088-8 «О внесении изменений в статью 272.1 Уголовного кодекса Российской Федерации» // Система обеспечения законодательной деятельности Государственной Думы. URL: <https://sozd.duma.gov.ru/bill/1133088-8> (дата обращения: 03.06.2026).

[12] Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // Собрание законодательства РФ. 2001. № 23. Ст. 2291.

[13] Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства РФ. 1995. № 33. Ст. 3349.

[14] Конвенция Организации Объединенных Наций против киберпреступности: резолюция Генеральной Ассамблеи ООН А/

RES/79/243 от 24.12.2024. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243> (дата обращения: 03.06.2026).

References:

[1] Isaxon R.A. Digitalization of criminal proceedings: digital criminal case, artificial intelligence and electronic evidence//CyberLeninka. 2025.

[2] Morozova I.G. On the need for legal regulation of deepfakes//CyberLeninka. 2025.

[3] Starodubov A.A. Deepfake (deepfake) and the criminal law//Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2024.

[4] A.I. Turshin. Specialist participation in the study of electronic evidence in criminal proceedings//NB: Administrative law and administration practice. 2025.

[5] Criminal Code of the Russian Federation of 13.06.1996 No. 63-FZ//Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

[6] Code of Criminal Procedure of the Russian Federation of 18.12.2001 No. 174-FZ//Collection of Legislation of the Russian Federation. 2001. No. 52 (part I). Art. 4921.

[7] Resolution of the Plenum of the Supreme Court of the Russian Federation of 30.11.2017 No. 48 "On judicial practice in cases of fraud, embezzlement and embezzlement" //Bulletin of the Supreme Court of the Russian Federation. 2018. № 2.

[8] Starodubov A.A. Deepfake (deepfake) and the criminal law//Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2024. URL: <https://vestnikkui.ru/ru/nauka/article/75454/>

view (access date: 03.06.2026).

[9] Federal Law of 29.12.2022 No. 572-FZ "On the identification and (or) authentication of individuals using biometric personal data..." //Collection of legislation of the Russian Federation. 2023. No. 1 (part I). Art. 20.

[10] OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION. Art. 272.1 "Illegal use and (or) transfer, collection and (or) storage of computer information containing personal data..." //SPS" ConsultantPlus. " URL: https://www.consultant.ru/document/cons_doc_LAW_10699/deefead19003ba8266e85fbf42fc31f60ed3c698/ (access date: 03.06.2026).

[11] Bill No. 1133088-8 "On Amendments to Article 272.1 of the Criminal Code of the Russian Federation" //System for Ensuring the Legislative Activities of the State Duma. URL: <https://sozd.duma.gov.ru/bill/1133088-8> (access date: 03.06.2026).

[12] Federal Law of 31.05.2001 No. 73-FZ "On State Judicial Expert Activities in the Russian Federation" //Collection of Legislation of the Russian Federation. 2001. № 23. Art. 2291.

[13] Federal Law of 12.08.1995 No. 144-FZ "On Operational-Search Activities" //Collection of Legislation of the Russian Federation. 1995. № 33. Art. 3349.

[14] United Nations Convention against Cybercrime: UN General Assembly resolution A/RES/79/243 of 24.12.2024. URL: <https://www.un.org/ru/documents/treaty/A-RES-79-243> (Accessed: 03.06.2026).



ЮРКОМПАНИ
www.law-books.ru

Юридическое издательство «ЮРКОМПАНИ»
издает научные журналы:

- Научно-правовой журнал «Образование и право», рекомендованный ВАК Министерства науки и высшего образования России (специальности 12.00.01, 12.00.02), выходит 1 раз в месяц.
- Научно-правовой журнал «Право и жизнь», рецензируемый (РИНЦ, E-Library), выходит 1 раз в 3 месяца.