Дата поступления рукописи в редакцию: 08.07.2026 г.
Дата принятия рукописи в печать: 20.07.2026 г.
DOI: 10.24412/2224-9133-2026-6-303-308

ГОЛОУХОВ Алексей Андреевич,
студент специалитета 5 курс по направлению «Судебная и прокурорская деятельность», Московский государственный юридический университет имени О. Е. Кутафина (МГЮА),
e-mail: goloukhov2003@mail.ru

УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ДИПФЕЙК-ПРЕСТУПЛЕНИЯМ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. *Распространение технологий генеративного синтеза аудиовизуальных материалов, получивших обобщающее наименование «дипфейки», породило класс общественно опасных деяний, специфика которых не получила отражения в действующем уголовном законодательстве Российской Федерации. В статье уточняется понятие дипфейка как синтетического контента, имитирующего идентифицируемое лицо с такой достоверностью, при которой средний наблюдатель не способен распознать подделку, и обосновывается, что общественная опасность подобных деяний обладает самостоятельным качеством, не сводимым к опасности базовых преступлений: она подрывает доверие к биометрическим идентификаторам, порождает асимметрию между затратами на изготовление и опровержение, сочетает массовость с правдоподобием. Далее анализируются применимые составы Особенной части УК РФ (клевета, нарушение неприкосновенности частной жизни, мошенничество, вымогательство, оборот материалов с изображением несовершеннолетних) и показывается, что они оставляют без охраны распространение сфабрикованных интимных изображений совершеннолетних. На основе сравнительно-правового исследования (ФРГ, Республика Корея, Великобритания, Австралия, США, КНР, Европейский союз) выявляются три модели криминализации. Сформулированы предложения de lege ferenda: дополнение ст. 128.1, 159, 163 УК РФ квалифицирующим признаком использования программно-аппаратных средств синтеза биометрических идентификаторов и введение ст. 137.1 УК РФ об ответственности за изготовление и распространение сфабрикованных интимных изображений идентифицируемого лица; предложения соотнесены с внесёнными в Государственную Думу законопроектами.*

Ключевые слова: *дипфейк; криминализация; синтетические медиа; квалифицирующий признак; биометрические идентификаторы; неприкосновенность частной жизни; de lege ferenda.*

GOLOUKHOV Aleksey Andreevich
5th-year Specialist Degree Student Field of Study: Judicial and Prosecutorial Activity Kutafin Moscow State Law University (MSAL)

CRIMINAL-LAW COUNTERACTION OF DEEPFAKE-RELATED CRIMES IN THE RUSSIAN FEDERATION

Annotation. *The rapid proliferation of generative synthesis technologies for audiovisual materials, commonly referred to as deepfakes, has produced a distinct category of socially dangerous acts whose specificity is not reflected in the current criminal legislation of the Russian Federation. The article first clarifies the notion of a deepfake as synthetic content imitating an identifiable person with a degree of verisimilitude that precludes recognition by an average observer without technical means, and substantiates that the social danger of such acts possesses an autonomous quality irreducible to the danger of the underlying offences: it undermines trust in biometric identifiers, generates an asymmetry between the cost of fabrication and the cost of refutation, and combines mass dissemination with persuasive plausibility. The author then examines the applicable offences of the Special Part of the Russian Criminal Code (defamation, invasion of privacy, fraud, extortion, dissemination of materials depicting minors) and demonstrates that they reflect deepfake-related*

acts only fragmentarily and leave the dissemination of fabricated intimate images of adults without protection. On the basis of a comparative study covering Germany, the Republic of Korea, the United Kingdom, Australia, the United States, China and the European Union, three models of criminalisation are identified. The article concludes with proposals de lege ferenda: supplementing Articles 128.1, 159 and 163 of the Criminal Code with an aggravating element reflecting the use of hardware and software tools for synthesising biometric identifiers, and introducing a new Article 137.1 establishing liability for the production and dissemination of fabricated intimate images of an identifiable person. The proposals are correlated with the draft laws pending before the State Duma.

Key words: *deepfake; criminalisation; synthetic media; aggravating element; biometric identifiers; privacy; de lege ferenda.*

Введение

Распространение технологий генеративного синтеза аудиовизуальных материалов, получивших обобщающее наименование «дипфейки», породило класс общественно опасных деяний, специфика которых не получила отражения в действующем уголовном законодательстве Российской Федерации. По данным Росфинмониторинга, количество зафиксированных инцидентов с использованием дипфейков за I квартал 2025 г. превысило показатель за весь 2024 г. примерно на 19 процентов, а число случаев мошенничества с применением цифровой копии голоса возросло многократно [1]. Параллельной угрозой выступает распространение сфабрикованных интимных изображений идентифицируемых лиц без их согласия. Реакцией зарубежных законодателей стало принятие в 2023–2025 гг. специальных уголовно-правовых норм.

Общая теория противодействия преступлениям в информационной сфере разработана Е. А. Русскевичем [2], проблематика искусственного интеллекта в уголовном праве — А. А. Бимбиновым [3], охрана информационной безопасности личности — М. А. Ефремовой [4]. Вместе с тем системное исследование уголовно-правового противодействия дипфейк-преступлениям с разработкой конкретных предложений de lege ferenda в отечественной науке отсутствует.

Цель исследования — выявление системного характера пробела в уголовно-правовой охране и формулирование предложений по совершенствованию УК РФ; применены формально-юридический, сравнительно-правовой и системно-структурный методы. Принципиальная посылка работы: квалифицирующий признак использования технологий синтеза необходим не для восполнения пробела, поскольку соответствующие деяния охватываются действующими составами, а для отражения типового повышения общественной опасности, обусловленного способом совершения преступления; пробел в собственном смысле охватывает лишь распространение сфабрикованных интимных изображений совершеннолетних потерпевших и восполняется самостоятельным составом.

1. Дипфейки как предмет уголовно-правового исследования

Термин «дипфейк» (от англ. deep learning и fake) обозначает синтетические аудиовизуальные материалы, созданные с использованием технологий машинного обучения и имитирующие проявления конкретного идентифицируемого лица со степенью достоверности, при которой средний наблюдатель не способен отличить их от подлинной фиксации без специальных технических средств [2, с. 14]. Предметом исследования выступают только материалы, имитирующие реальных идентифицируемых лиц, поскольку именно они порождают специфическое посягательство на охраняемые блага. Российское законодательство нормативного определения дипфейка не содержит; зарубежные дефиниции (Регламент ЕС 2024/1689, Положения КНР об управлении услугами глубинного синтеза 2022 г.) строятся на признаках искусственного происхождения контента и его способности ввести в заблуждение относительно подлинности.

Типология противоправного использования синтетических медиа включает имущественные деяния (хищение посредством обмана с использованием клонированного голоса или сфабрикованного видеообращения, вымогательство под угрозой распространения компрометирующих материалов), деяния против чести и достоинства, а также наиболее общественно опасную группу — изготовление и распространение без согласия лица сфабрикованных интимных изображений идентифицируемого лица и сексуализированных синтетических изображений несовершеннолетних.

Общественная опасность дипфейк-деяний обладает качественными особенностями, образующими самостоятельное основание для постановки вопроса о специальной охране. Во-первых, подрыв доверия к биометрическим идентификаторам (голосу, лицу, манере речи) как носителям достоверной информации: технологии синтеза девальвируют их верификационную функцию, и подлинная фиксация ставится под сомнение наравне с фальсифицированной [4, с. 53]. Во-вто-

рых, асимметрия затрат: производство правдоподобного дипфейка доступно широкому кругу лиц, тогда как опровержение требует специальных познаний и не достигает сопоставимого охвата. В-третьих, сочетание массовости распространения с правдоподобием контента: материал за несколько часов получает многомиллионную аудиторию и воспринимается как первичная фиксация. В-четвёртых, эффект цифрового воскрешения — возможность создания материалов с участием умерших лиц — порождает не решённые законом вопросы охраны их достоинства [5, с. 117]. Совокупность названных особенностей свидетельствует о том, что опасность дипфейк-преступлений не сводится к сумме опасности деяний, инструментом совершения которых выступает синтетический контент, и образует самостоятельное качество.

2. Современное состояние уголовно-правовой охраны

Действующий закон специальных норм не содержит, и правоприменение обращается к существующим составам. Применимость ст. 128.1 УК РФ формально сомнений не вызывает: синтетический материал заведомо ложен. Однако доктринальная трактовка «сведений» формировалась применительно к вербальным формам [6, с. 84], тогда как дипфейк причиняет вред иначе: он имитирует документальную фиксацию и создаёт иллюзию верифицированного факта, что составы ст. 128.1 не отражают.

Применение ст. 137 УК РФ обнажает доктринальный парадокс: предметом охраны выступают сведения о частной жизни, тогда как синтетический контент по природе ложен. Формально-догматическая позиция исключает квалификацию ввиду отсутствия подлинности сведений [7, с. 112]; функционально-телеологическая исходит из того, что охраняемым благом является сфера частной жизни как таковая [8, с. 29]. Ни одна из позиций не преодолевает пробел, поскольку норма исторически ориентирована на охрану от разглашения подлинных тайн. Неприменима и ст. 138.1 УК РФ: средства синтеза не предназначены для негласного получения информации, а создают новый контент.

Хищение с использованием клонированного голоса охватывается ст. 159 УК РФ; квалификация по ст. 159.6 исключается, когда обман направлен на физическое лицо, поскольку её диспозиция предполагает вмешательство в функционирование средств обработки компьютерной информации [9, с. 156]. Применение ст. 163 УК РФ к шантажу сфабрикованными изображениями опирается на позицию, согласно которой критерием позорящего характера сведений выступает не их истинность, а способность дискредитировать потерпевшего. И здесь способ совершения, повышающий убедительность обмана либо угрозы, самостоятельной оценки в санкции не получает.

Создание контента, имитирующего изображения несовершеннолетних, образует объективную сторону ст. 242.1 УК РФ независимо от реального участия несовершеннолетнего [10, с. 38]. Принципиально иной является ситуация с распространением сфабрикованных интимных изображений совершеннолетних: такой контент, как правило, не отвечает пониманию порнографии и не охватывается ст. 137 УК РФ. Этот пробел не может быть восполнен расширительным толкованием без нарушения принципа правовой определённости, недопустимость чего подчёркивает Конституционный Суд РФ [11]. Иные применимые составы (ст. 207.3, 280.3, 282, 303, 306, 307, 272, 273, 272.1 УК РФ) охватывают дипфейк лишь как способ совершения деяния, не отражая его специфики. Таким образом, действующая система отражает рассматриваемые деяния фрагментарно: не учитывает типового повышения опасности, обусловленного способом, и оставляет без охраны распространение сфабрикованных интимных изображений совершеннолетних потерпевших, что требует законодательного решения.

3. Зарубежный опыт

Сравнительно-правовой анализ обнаруживает три модели криминализации. Первая основывается на универсальном квалифицирующем признаке использования технологий синтеза в существующих составах и отражает экономию уголовной репрессии. Вторая состоит в специальном составе о незаконном создании и распространении сфабрикованных материалов (ФРГ — проектируемый § 201b StGB до пяти лет лишения свободы; Республика Корея — до семи лет, с криминализацией хранения и просмотра; Великобритания и Австралия — поэтапная криминализация создания и распространения синтетических интимных изображений без согласия; США — TAKE IT DOWN Act 2025 г. с обязанностью платформ удалять контент) [12; 13]. Третья — регуляторно-уголовный гибрид (КНР, Регламент ЕС 2024/1689): обязанности маркировки и идентификации дополняются уголовными санкциями за наиболее опасные деяния. Универсальный признак согласуется с экономией репрессии, но не охватывает деяний, в которых способ порождает самостоятельный объект охраны; специальный состав обеспечивает полную защиту, но требует строгого определения предмета; гибридная модель предполагает развитую систему админи-

стративного контроля, формирование которой в России находится на начальной стадии. Изложенное обосновывает комбинированный подход.

4. Направления совершенствования уголовного законодательства

Предлагаемые решения отвечают принципам криминализации (Н. Ф. Кузнецова, школа А. И. Коробеева): общественной опасности, типичности, относительной распространённости, процессуальной фиксируемости и экономии репрессии [14; 15]. Общественная опасность обоснована выше; типичность подтверждается устойчивой группой способов; распространённость — данными о росте инцидентов; процессуальная фиксируемость повышена развитием методик судебной экспертизы синтетических медиа [16, с. 91].

Первое предложение — дополнение ст. 128.1, 159, 163 УК РФ квалифицирующим признаком «с использованием программно-аппаратных средств синтеза изображения, голоса или иных биометрических идентификаторов». Признак вводится не для восполнения пробела, а для отражения в дифференциации ответственности типового и существенного повышения общественной опасности: имитация документальной фиксации придаёт обману, угрозе и порочащим сведениям убедительность, недостижимую традиционными средствами. Формулировка через категорию биометрических идентификаторов согласована с понятийным аппаратом Федерального закона от 29 декабря 2022 г. № 572-ФЗ и сохраняет технологическую нейтральность. Дополнение ст. 137 УК РФ аналогичным признаком нецелесообразно ввиду указанного доктринального парадокса; пробел в этой части восполняется самостоятельным составом.

Второе предложение — введение ст. 137.1 УК РФ об ответственности за незаконное изготовление в целях распространения и (или) распространение посредством программно-аппаратных средств синтеза изображения, имитирующего обнажённое или иное интимное состояние идентифицируемого лица либо сексуальные действия с его участием, совершённые без специального согласия лица на содержание соответствующего характера; наказание по основному составу — до трёх лет лишения свободы, по квалифицированному (публично, в том числе через сеть, либо в отношении двух и более лиц) — до пяти лет, по особо квалифицированному (в отношении несовершеннолетнего) — до восьми лет. Конструкция специального согласия исключает распространительное толкование. Разграничение со ст. 242.1 УК РФ проводится по объекту: ст. 137.1 защищает достоинство и интимную сферу идентифицируемого лица, ст. 242.1 — нравственное развитие детей; при наличии признаков обоих составов применяются правила совокупности. Размещение нормы в главе 19 УК РФ обеспечивает системную согласованность и соседство со ст. 137.

Сформулированные предложения следует соотнести с внесёнными в Государственную Думу инициативами (законопроекты № 718538-8, № 885494-8, № 1133088-8) [17]. Законопроект № 718538-8 предусматривает дополнение ст. 128.1, 158, 159, 159.6, 163, 165 УК РФ признаком использования изображения или голоса (в том числе искусственно созданных); в отзыве Правительства РФ указано на отсутствие отраслевой дефиниции и недостаточную обоснованность повышенной опасности. Законопроект № 885494-8 ограничивается дополнением перечня отягчающих обстоятельств (ст. 63 УК РФ). Настоящие предложения отличаются: формулировка опирается на понятийный аппарат Закона № 572-ФЗ (что снимает замечание об отсутствии дефиниции); перечень дополняемых составов ограничен теми, где способ типично повышает опасность (кража исключена); обоснование строится не на восполнении пробела, а на повышенной опасности способа, тогда как путь отягчающего обстоятельства недостаточен, поскольку не изменяет пределов санкции. Наконец, ни одна из инициатив не предусматривает специального состава для сфабрикованных интимных изображений, образующего ядро настоящих предложений.

Распределение ответственности подчинено принципу вины (ст. 5 УК РФ): разработчик базовой модели, не охватывающий умыслом конкретные деяния, ответственности не подлежит; лицо, дообучившее модель и предоставившее её для совершения преступления, отвечает как пособник либо подстрекатель (ч. 4, 5 ст. 33 УК РФ); конечный пользователь выступает исполнителем. Криминализация и обязательная маркировка контента, созданного искусственным интеллектом, взаимодополняют друг друга.

Заключение

Исследование подтвердило системный характер фрагментарности действующей охраны: общественная опасность дипфейк-преступлений образует самостоятельное качество, применимые составы не отражают типового повышения опасности, обусловленного способом совершения, а распространение сфабрикованных интимных изображений совершеннолетних потерпевших остаётся вне охраны. Предложено комбинированное реагирование: дополнение ст. 128.1, 159, 163 УК РФ квалифицирующим признаком использования средств синтеза биометрических

идентификаторов и введение ст. 137.1 УК РФ с трёхчастной конструкцией состава и размещением в главе 19. Дальнейшей разработки требуют процессуально-криминалистические аспекты доказывания, соотношение уголовно-правовых и регуляторных средств охраны и уголовно-правовой статус разработчиков генеративных моделей.

Список литературы:

[1] Голосовое клонирование — король атак: по сообщению о выступлении статс-секретаря — заместителя директора Росфинмониторинга на V Всероссийских академических слушаниях (МГИМО МИД России, март 2026 г.) // Право в России. URL: https://lawinrussia.ru/golosovoe-klonirovanie-korol-atak-ekspert-rasskazala-o-strashnoj-ugroze-dipfejkov/ (дата обращения: 03.05.2026).

[2] Русскевич Е. А. Уголовное право и информатизация : монография. М. : Проспект, 2023. 320 с.

[3] Бимбинов А. А. Преступления, совершаемые с использованием технологий искусственного интеллекта: проблемы квалификации // Уголовное право. 2024. № 3. С. 5–14.

[4] Ефремова М. А. Уголовно-правовая охрана информационной безопасности личности в условиях развития технологий искусственного интеллекта // Вестник Московского университета МВД России. 2024. № 4. С. 48–56.

[5] Серебренникова А. В. Цифровое посмертие и уголовно-правовая охрана достоинства умерших: постановка проблемы // Государство и право. 2025. № 2. С. 112–122.

[6] Лопашенко Н. А. Преступления против личности : учебно-практическое пособие. 3-е изд., перераб. и доп. М. : Юрлитинформ, 2023. 412 с.

[7] Кибальник А. Г. Неприкосновенность частной жизни и её уголовно-правовая охрана в цифровую эпоху // Уголовное право. 2024. № 6. С. 108–117.

[8] Дворецкий М. Ю. Информационные технологии и охрана сферы частной жизни в уголовном праве // Lex russica. 2025. № 1. С. 24–35.

[9] Чупрова А. Ю. Мошенничество в сфере компьютерной информации: проблемы доктрины и практики. М. : Юрлитинформ, 2023. 248 с.

[10] Пудовочкин Ю. Е. Уголовно-правовая охрана несовершеннолетних в условиях цифровизации // Журнал российского права. 2024. № 9. С. 32–44.

[11] Постановление Конституционного Суда РФ от 27 мая 2008 г. № 8-П // Собрание законодательства РФ. 2008. № 24. Ст. 2892.

[12] Teichmann F. Strafrechtlicher Persönlichkeitsschutz vor Deepfakes // KriPoZ — Kriminalpolitische Zeitschrift. 2025. № 6. S. 376–388.

[13] Park J. South Korea Confronts a Deepfake Crisis: Legislative Reform and Its Limits // East Asia Forum. 2024. November 19.

[14] Кузнецова Н. Ф. Преступление и преступность: избранные труды. СПб. : Юридический центр Пресс, 2003. 834 с.

[15] Полный курс уголовного права : в 5 т. / под ред. А. И. Коробеева. Т. 1 : Преступление и наказание. СПб. : Юридический центр Пресс, 2008. 1133 с.

[16] Россинская Е. Р. Судебная экспертиза синтетических медиа: проблемы методологии // Вестник криминалистики. 2024. № 4. С. 87–96.

[17] Паспорта законопроектов № 718538-8, № 885494-8, № 1133088-8 // СОЗД ГАС «Законотворчество». URL: https://sozd.duma.gov.ru (дата обращения: 09.06.2026).

References:

[1] Voice cloning is the king of attacks: according to the report on the speech of the State Secretary - Deputy Director of Rosfinmonitoring at the V All-Russian Academic Hearings (MGIMO MFA of Russia, March 2026)//Law in Russia. URL: https://lawinrussia.ru/golosovoe-klonirovanie-korol-atak-ekspert-rasskazala-o-strashnoj-ugroze-dipfejkov/ (дата обращения: 03.05.2026).

[2] Russkevich E. A. Criminal law and informatization: monograph. M.: Prospect, 2023. 320 s.

[3] Bimbinov A. A. Crimes committed using artificial intelligence technologies: qualification problems//Criminal law. 2024. № 3. S. 5-14.

[4] Efremova M. A. Criminal law protection of personal information security in the context of the development of artificial intelligence technologies// Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2024. № 4. S. 48-56.

[5] Serebrennikova A. V. Digital postmortem and criminal law protection of the dignity of the dead: posing a problem//State and law. 2025. № 2. S. 112-122.

[6] Lopashenko N. A. Crimes against the person: a teaching and practical guide. 3rd ed., Revised and add. M.: Yurlitinform, 2023. 412 s.

[7] Kibalnik A. G. Privacy and its criminal law protection in the digital age//Criminal law. 2024. № 6. S. 108-117.

[8] Butler M. Yu. Information technology and protection of privacy in criminal law//Lex russica. 2025. № 1. S. 24-35.

[9] Chuprova A. Yu. Computer information fraud: problems of doctrine and practice. M.: Yurlitinform, 2023. 248 pp.

[10] Pudovochkin Yu. E. Criminal legal protection of minors in the context of digitalization//Journal of Russian Law. 2024. № 9. S. 32-44.

[11] Decision of the Constitutional Court of the Russian Federation of May 27, 2008 No. 8-P//Collection of legislation of the Russian Federation. 2008. № 24. Art. 2892.

[12] Teichmann F. Strafrechtlicher Persönlichkeitsschutz vor Deepfakes // KriPoZ — Kriminalpolitische Zeitschrift. 2025. № 6. S. 376–388.

[13] Park J. South Korea Confronts a Deepfake Crisis: Legislative Reform and Its Limits // East Asia Forum. 2024. November 19.

[14] Kuznetsova N.F. Crime and crime: selected works. St. Petersburg: Legal Center Press, 2003. 834 pp.

[15] Full course of criminal law: in 5 tons/ed. A.I. Korobeeva. T. 1: Crime and punishment. St. Petersburg: Legal Center Press, 2008. 1133 pp.

[16] Rossinskaya E.R. Forensic examination of synthetic media: problems of methodology//Bulletin of Criminalistics. 2024. № 4. S. 87-96.

[17] Passports of bills No. 718538-8, No. 885494-8, No. 1133088-8//SOZD GAS "Lawmaking." URL: https://sozd.duma.gov.ru (access date: 09.06.2026).