

УГОЛОВНО-ПРАВОВЫЕ НАУКИ/CRIMINAL LAW SCIENCES

DOI: https://doi.org/10.60797/IRJ.2026.164.34

ПРЕСТУПНЫЙ ПОТЕНЦИАЛ ДИПФЕЙКА В СОВРЕМЕННОМ МИРЕ

Научная статья

Гаранина Е.Д.[1, *]

[1] Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Российская Федерация

* Корреспондирующий автор (ekaterina.garanina05[at]mail.ru)

Аннотация

Статья посвящена уголовно-правовому анализу использования технологий дипфейков в преступной деятельности в условиях цифровизации общественных отношений. Рассматривается криминогенный потенциал технологий дипфейк, отмечается отсутствие сформировавшейся судебной практики, что обусловливает сложности квалификации. Анализируются основные направления преступного применения дипфейков, включая обход систем биометрической идентификации, использование методов социальной инженерии и создание компрометирующих материалов. Выявляются ключевые проблемы уголовно-правовой регламентации, связанные с квалификацией деяний и доказыванием, формулируются предложения по совершенствованию действующего законодательства.

Ключевые слова: дипфейк, киберпреступность, ст. 159 УК РФ, социальная инженерия, биометрическая идентификация, цифровая криминалистика, Liveness Detection.

THE CRIMINAL POTENTIAL OF DEEPFAKES IN THE MODERN WORLD

Research article

Garanina E.D.[1, *]

[1] Vladimir State University, Vladimir, Russian Federation

* Corresponding author (ekaterina.garanina05[at]mail.ru)

Abstract

The article is devoted to the criminal law analysis of the use of deepfake technologies in criminal activity in the context of the digitalisation of public relations. The criminogenic potential of deepfake technologies is reviewed, and the lack of established judicial practice is noted, which causes difficulties in classification. The main areas of criminal use of deepfakes are analysed, including the bypassing of biometric identification systems, the use of social engineering methods, and the creation of compromising materials. Key problems in criminal law regulation related to the classification of acts and evidence are identified, and proposals for improving the current legislation are formulated.

Keywords: deepfake, cybercrime, Article 159 of the Criminal Code of the Russian Federation, social engineering, biometric identification, digital forensics, Liveness Detection.

Введение

Стремительное развитие технологий искусственного интеллекта и их активное использование в преступной деятельности ставят перед современным уголовным правом принципиально новые вызовы, связанные с квалификацией деяний и доказыванием вины. Особую актуальность в этом контексте приобретает феномен дипфейка, подрывающий традиционные представления о доказательствах, средствах и способах совершения преступлений [1, С. 177].

Основные результаты

К 2026 году ландшафт угроз информационной безопасности претерпел фундаментальные изменения. Прогнозы аналитиков Gartner и Europol [8], [9] подтвердились: использование искусственного интеллекта (ИИ) в преступных целях перешло из фазы экспериментов в фазу индустриализации. Если в начале 2020-х годов создание качественного дипфейка требовало мощных видеокарт и дней рендеринга, то сегодня облачные сервисы Dark Web предлагают услуги *«Deepfake-as-a-Service»* в режиме реального времени.

Проблема перестала быть теоретической. Согласно ретроспективным данным отчета Sumsub Identity Fraud Report, еще в 2023 году количество дипфейков в сфере верификации личности выросло в 10 раз, а в 2026-м мы будем наблюдать полную автоматизацию атак на системы KYC (Know Your Customer) банков и государственных сервисов [10].

Это означает, что мошенничество будет осуществляться не через заранее записанные видео, а через *живое* общение в чатах и видеозвонках. Нейросети будут способны генерировать диалоги, адаптируясь к эмоциональным реакциям жертвы в реальном времени [3, С. 82].

Для понимания масштаба угрозы необходимо обратиться к ключевым прецедентам, которые формируют современную судебную практику, показывая уязвимость правовой системы.

Преступный потенциал технологии дипфейк реализуется в трех основных направлениях, которые требуют квалификации с точки зрения уголовного права [4, С. 108]:

1. Биометрический взлом и хищение: обход систем FaceID и VoiceID для доступа к банковским счетам.

2. Социальная инженерия нового уровня: звонки от «родственников» или «генеральных директоров» с полной имитацией голоса и мимики.

3. Дискредитация и шантаж: создание порнографических материалов или компрометирующих видео с участием жертвы.

Показательным примером криминальной инженерии нового типа стало ограбление транснациональной компании Arup (Гонконгский филиал). Сотрудник бухгалтерии перевел мошенникам 25,6 млн. долларов после видеоконференции, в которой участвовал финансовый директор и несколько коллег. Все участники звонка, кроме жертвы, были дипфейками, сгенерированными в реальном времени на основе публичных видеозаписей руководства [2]. Данный кейс в контексте правоприменения демонстрирует переход от статьи 159.3 УК РФ (мошенничество с использованием ЭСП) к более сложным составам, где орудием преступления выступает не просто код, а синтетическая личность.

Актуальным остается распространение сервисов типа «Nudify» (автоматическое удаление одежды на фото), что привело к всплеску вымогательств [7]. Преступники требуют выкуп за непубликацию сгенерированного порноконтента. По данным ФБР и Европола, количество обращений по поводу «сексторшн» с использованием ИИ выросло на 300% за последние два года.

Правоприменительная практика сталкивается с проблемой сбора доказательств. Обычный осмотр видеозаписи следователем больше не эффективен [5, С. 107]. На помощь приходят специализированные программные комплексы, которые должны стать обязательным инструментом экспертов-криминалистов:

1. Intel FakeCatcher: первая в мире система, работающая в реальном времени. Принцип действия основан на фотоплетизмографии (PPG) — программа анализирует микроизменения цвета кожи, вызванные кровотоком. На реальном видео «пульс» виден на пиксельном уровне, на дипфейке — отсутствует.

2. Microsoft Video Authenticator: анализирует границы смешения пикселей и артефакты сжатия, оценивая вероятность искусственного вмешательства («индекс достоверности»).

3. Reality Defender: мультимодальная платформа, используемая в банковском секторе для выявления синтетического голоса (audio deepfakes) при телефонном банкинге.

Однако злоумышленники в 2026 году используют методы «состязательного обучения» (adversarial attacks), специально добавляя шумы в видео, чтобы обмануть детекторы. Это создает бесконечную «гонку вооружений».

Несмотря на рост числа общественно опасных деяний, совершаемых с использованием дипфейков, единообразная судебная практика по данной категории дел в настоящее время не сформировалась. На законодательном уровне предпринимались попытки урегулировать указанную проблему. В Государственной Думе Российской Федерации высказывались предложения о введении уголовной ответственности за использование дипфейков, однако при обсуждении инициативы не был выработан однозначный подход к определению соответствующего состава преступления, не определена статья УК РФ для квалификации таких деяний. В результате правоприменитель вынужден прибегать к квалификации по уже существующим нормам уголовного закона, что обусловливает необходимость анализа их применимости к преступлениям, совершаемым с использованием технологий синтетического медиаконтента.

В российском правовом поле деяния с использованием дипфейков балансируют между статьями 128.1 (Клевета), 207.3 (Публичное распространение заведомо ложной информации) и 159 (Мошенничество), однако сложность технической атрибуции автора дипфейк-модели затрудняет привлечение к ответственности. Действующий Уголовный кодекс РФ требует адаптации к реалиям автоматизированной преступности [6, С. 322].

Анализ правоприменительной практики и действующего законодательства свидетельствует о том, что использование дипфейков в преступной деятельности порождает ряд взаимосвязанных уголовно-правовых и уголовно-процессуальных проблем, требующих нормативного разрешения.

Так, совершение мошеннических и иных преступлений с применением технологии дипфейк характеризуется повышенной степенью подготовки и причиняет значительный ущерб доверию к цифровой среде, однако в уголовном законе отсутствуют специальные квалифицирующие признаки, позволяющие учесть данный способ совершения преступления, в связи с чем обоснованным представляется дополнение статьи 63 УК РФ положением о совершении преступления с использованием технологий искусственного интеллекта для подделки биометрических данных или голоса.

Одновременно возникает проблема определения уголовно-правового статуса изображения лица и голоса, которые, являясь биометрическими персональными данными, могут незаконно использоваться для обучения нейросетей и создания синтетического контента, однако их копирование не образует состава хищения в силу нематериального характера таких данных, что обусловливает необходимость введения самостоятельной нормы, криминализирующую «Незаконное использование биометрических параметров лица для создания синтетического контента, порочащего честь и достоинство или используемого в целях хищения» и устанавливающую ответственность за незаконное использование биометрических параметров лица в целях хищения либо дискредитации личности.

Существенные затруднения возникают и на стадии доказывания, поскольку визуальный осмотр аудиовизуальных материалов следователем утрачивает эффективность в условиях нейросетевого синтеза, что требует нормативного закрепления обязанности проведения автоматизированной технической экспертизы цифровых доказательств, в том числе путем внесения соответствующих уточнений в статью 74 УПК РФ.

Заключение

Индустриализация киберпреступности в 2026 году ставит перед юристами ультиматум: либо правовая система интегрирует технические знания и инструменты (Liveness Detection, водяные знаки C2PA) в процесс квалификации преступлений, либо мы столкнемся с кризисом доверия к любым цифровым доказательствам. Борьба с дипфейками

лежит не только в плоскости IT, но и в плоскости модернизации уголовного закона, который должен четко сигнализировать: кража цифрового лица — это тяжкое преступление.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Архипцев И.Н. К вопросу о правовом обеспечении предупреждения преступлений, совершаемых с использованием искусственного интеллекта и технологий, созданных на его основе, в Российской Федерации / И.Н. Архипцев, А.В. Сарычев, А.В. Мотузов // Legal Concept. — 2022. — № 2. — С. 175–181.

2. В Гонконге с помощью дипфейка мошенники украли миллионы долларов у крупнейшей корпорации // Российская газета. — 2024. — URL: https://rg.ru/2024/02/04/v-gonkonge-s-pomoshchiu-dipfejka-moshenniki-ukrali-milliony-dollarov-u-krupnejshej-korporacii.html (дата обращения: 01.02.2026).

3. Демкин В. Дипфейки: поиск модели правового регулирования / В. Демкин // Правовые проблемы в эпоху цифровых технологий. — 2024. — Т. 5, № 4. — С. 73–91.

4. Долгиева М.М. Квалификация дипфейк-мошенничества и киберпохищения человека / М.М. Долгиева // Актуальные проблемы российского права. — 2024. — № 11(168). — С. 106–113.

5. Клишков В.Б. Киберпреступность: понятие, признаки, основные направления противодействия / В.Б. Клишков, Е.В. Стебенева, М.А. Яковлева // Вестник Нижегородского университета им. Н.И. Лобачевского. — 2022. — № 4. — С. 106–114.

6. Модонов Н.В. Распространение ложных сведений с использованием дипфейков: правовые аспекты и ответственность / Н.В. Модонов // Молодой ученый. — 2024. — № 50(549). — С. 321–323.

7. Что такое Nudify и почему это опасно: ИИ, дипфейки и сексуальная эксплуатация // Bitrue Blog. — 2024. — URL: https://www.bitrue.com/ru/blog/nudify-ban-nsfw-nft-ai-danger (дата обращения: 01.02.2026).

8. Facing Reality? Law Enforcement and the Challenge of Deepfakes // Europol. — The Hague : Europol Innovation Lab, 2022. — URL: https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes (accessed: 09.12.2025).

9. Emerging Risks of AI-Driven Social Engineering // Gartner. — 2021. — URL: https://www.gartner.com (accessed: 01.02.2026).

10. Identity Fraud Report 2023 // Sumsub. — URL: https://sumsub.com/identity-fraud-report/ (accessed: 30.01.2026).

Список литературы на английском языке / References in English

1. Arkhiptsev I.N. K voprosu o pravovom obespechenii preduprezhdeniya prestuplenij, sovershaemyh s ispol'zovaniem iskusstvennogo intellekta i tekhnologij, sozdannyh na ego osnove, v Rossijskoj Federacii [On the Legal Framework for Preventing Crimes Committed Using Artificial Intelligence and Related Technologies in the Russian Federation] / I.N. Arhipcev, A.V. Sarychev, A.V. Motuzov // Legal Concept. — 2022. — № 2. — P. 175–181. [in Russian]

2. V Gonkonge s pomoshch'yu dipfejka moshenniki ukrali milliony dollarov u krupnejshej korporacii [In Hong Kong, scammers used deepfake technology to steal millions of dollars from a major corporation] // Rossijskaya gazeta [Russian newspaper]. — 2024. — URL: https://rg.ru/2024/02/04/v-gonkonge-s-pomoshchiu-dipfejka-moshenniki-ukrali-milliony-dollarov-u-krupnejshej-korporacii.html (accessed: 01.02.2026). [in Russian]

3. Demkin V. Dipfejki: poisk modeli pravovogo regulirovaniya [Deepfakes: Searching for a Model of Legal Regulation] / V. Demkin // Pravovye problemy v epohu cifrovyh tekhnologij [Legal Issues in the Era of Digital Technologies]. — 2024. — Vol. 5, № 4. — P. 73–91. [in Russian]

4. Dolgieva M.M. Kvalifikaciya dipfejk-moshennichestva i kiberpohishcheniya cheloveka [Qualification of Deepfake Fraud and Cyber Kidnapping] / M.M. Dolgieva // Aktual'nye problemy rossijskogo prava [Current Problems of Russian Law]. — 2024. — № 11(168). — P. 106–113. [in Russian]

5. Klishkov V.B. Kiberprestupnost': ponyatie, priznaki, osnovnye napravleniya protivodejstviya [Cybercrime: Concept, Characteristics, and Main Directions of Counteraction] / V.B. Klishkov, E.V. Stebeneva, M.A. Yakovleva // Vestnik Nizhegorodskogo universiteta im. N.I. Lobachevskogo [Bulletin of Nizhny Novgorod University named after N. I. Lobachevsky]. — 2022. — № 4. — P. 106–114. [in Russian]

6. Modonov N.V. Rasprostranenie lozhnyh svedenij s ispol'zovaniem dipfejkov: pravovye aspekty i otvetstvennost' [Dissemination of False Information Using Deepfakes: Legal Aspects and Responsibility] / N.V. Modonov // Molodoj uchenyj [Young Scientist]. — 2024. — № 50(549). — P. 321–323. [in Russian]

7. Chto takoe Nudify i pochemu eto opasno: II, dipfejki i seksual'naya ekspluataciya [What is Nudify and why is it dangerous: AI, deepfakes, and sexual exploitation] // Bitrue Blog. — 2024. — URL: https://www.bitrue.com/ru/blog/nudify-ban-nsfw-nft-ai-danger (accessed: 01.02.2026). [in Russian]

8. Facing Reality? Law Enforcement and the Challenge of Deepfakes // Europol. — The Hague : Europol Innovation Lab, 2022. — URL: https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes (accessed: 09.12.2025).

9. Emerging Risks of AI-Driven Social Engineering // Gartner. — 2021. — URL: https://www.gartner.com (accessed: 01.02.2026).

10. Identity Fraud Report 2023 // Sumsub. — URL: https://sumsub.com/identity-fraud-report/ (accessed: 30.01.2026).