Полицейская и следственная деятельность
Правильная ссылка на статью:
Асадов Р.Б. Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий // Полицейская и следственная деятельность. 2025. № 4. DOI: 10.25136/2409-7810.2025.4.75462 EDN: MFCNUV URL: https://nbpublish.com/library_read_article.php?id=75462

Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий

Асадов Раму Бекханович

старший преподаватель; Юридический институт; Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых
главный редактор; Диалог (www.npzhdialog.ru)

600026, Россия, Владимирская обл., г. Владимир, ул. Горького, д. 87

asadov@npzhdialog.ru

Статья из рубрики "Полиция и защита прав человека"

DOI:

10.25136/2409-7810.2025.4.75462

EDN:

MFCNUV

Дата направления статьи в редакцию:

08-08-2025

Дата публикации:

15-08-2025

Аннотация: Настоящее исследование посвящено комплексному анализу феномена «цифровой мимикрии» – неправомерного использования технологий глубокого синтеза (deepfake) в контексте защиты прав личности. Предмет охватывает как уголовно-правовые, так и криминалистические аспекты применения синтетических аудио- и видеоматериалов, воспроизводящих биометрические характеристики человека (внешность, голос, мимику) без его согласия. Особое внимание уделяется квалификации противоправных деяний, связанных с дипфейками, в действующем российском законодательстве, выявлению пробелов в правовом регулировании и их соотношению с международными подходами. Анализируются типовые модели преступных схем, включая дипфейк-мошенничество и «виртуальное похищение», а также вопросы допустимости использования синтетических медиа в культурных, образовательных и

правоохранительных целях. Исследование базируется на изучении судебной практики, доктринальных источников, сравнительно-правовых данных и технологических характеристик современных алгоритмов глубокого синтеза. Исследование выполнено с использованием формально-юридического, сравнительно-правового, криминалистического и системно-структурного методов в сочетании с анализом судебной практики и нормативных актов. Научная новизна исследования заключается в комплексном междисциплинарном рассмотрении феномена дипфейка с позиций уголовного права, криминалистики и сравнительного правоведения, а также в формулировании предложений по совершенствованию российского законодательства в сфере защиты биометрических данных. Впервые систематизированы и классифицированы основные модели противоправного применения технологий глубокого синтеза, выявлены пробелы в квалификации деяний, связанных с подделкой изображения или голоса, и обоснована необходимость введения в Уголовный кодекс РФ самостоятельного состава преступления, предусматривающего ответственность за незаконное использование синтетических биометрических образов. Дополнительно обоснована значимость внедрения процедурных гарантий, обеспечивающих допустимость цифровых доказательств, полученных с использованием специализированных алгоритмов выявления дипфейков. Сделан вывод о целесообразности разработки унифицированной методики доказывания факта применения дипфейка, интеграции автоматизированных систем его выявления и гармонизации национальных норм с международными стандартами.

Ключевые слова:

дипфейк, технологии глубокого синтеза, биометрические данные, уголовное право, криминалистика, цифровая мимикрия, фальсификация доказательств, киберпреступления, защита прав личности, международное сотрудничество

Настоящее исследование посвящено комплексному анализу феномена «цифровой мимикрии» — неправомерного использования технологий глубокого синтеза (*deepfake*) в контексте защиты прав личности. Предмет охватывает как уголовно-правовые, так и криминалистические аспекты применения синтетических аудио- и видеоматериалов, воспроизводящих биометрические характеристики человека (внешность, голос, мимику) без его согласия. Особое внимание уделяется квалификации противоправных деяний, связанных с дипфейками, в действующем российском законодательстве, выявлению пробелов в правовом регулировании и их соотношению с международными подходами. Анализируются типовые модели преступных схем, включая дипфейк-мошенничество и «виртуальное похищение», а также вопросы допустимости использования синтетических медиа в культурных, образовательных и правоохранительных целях.

Методологическая основа исследования состоит из общенаучных, частнонаучных и специальных юридических методов. К числу общенаучных относятся системно-структурный метод, а также методы анализа и синтеза, обеспечившие целостное восприятие объекта исследования и установление взаимосвязей между уголовно-правовыми, административно-правовыми и гражданско-правовыми механизмами защиты. Среди частнонаучных методов — сравнительно-правовой, предназначенный для сопоставления подходов разных стран к квалификации деяний, совершенных с использованием технологий глубокого синтеза, и криминалистический — для анализа особенностей обнаружения, фиксации и исследования цифровых доказательств. Из

специальных юридических методов — формально-юридический — для выявления, систематизации и толкования норм российского и зарубежного законодательства о синтетических медиа.

Термин «дипфейк» был введен в 2017 г. на платформе *Reddit* и первоначально обозначал подмену изображения лица с применением алгоритмов искусственного интеллекта (ИИ) для генерации новых, реалистично выглядящих изображений [1]. Развитие технологий привело к выходу за рамки статичных визуальных манипуляций: современные алгоритмы синтезируют не только изображение, но и голос, создавая аудио- и видеоконтент с использованием внешности или тембра иного лица. Для этого не требуется глубоких технических знаний или дорогостоящего оборудования: ряд мобильных приложений позволяет сформировать дипфейк-ролик за считанные минуты.

Потенциально допустимое использование таких технологий охватывает широкий спектр — от кинопроизводства (омоложение актеров, языковая адаптация фильмов, безопасная постановка сложных трюков) до образования и медицины. Так, технологии глубокого синтеза применялись для воссоздания экранных образов умерших артистов и реализации коммерческих проектов при согласии правообладателей, в том числе для использования образа Леонида Куравлева в рекламной кампании Сбербанка (*Сбербанк воссоздал образ Жоржа Милославского и сделал его своим новогодним амбассадором. URL: https://tass.ru/obschestvo/10145879 (дата обращения: 09.08.2025)*).

Широкое распространение технологий цифрового синтеза обусловливает существенные риски их противоправного использования, что предопределяет необходимость их анализа в контексте уголовно-правового регулирования. В 2023 г. количество видеоматериалов, созданных с применением технологий глубокого синтеза, утроилось, а объем поддельных голосовых записей увеличился в восемь раз по сравнению с 2022 г., по данным *DeepMedia*, что свидетельствует о стремительном распространении соответствующих технологий и усилении угроз для информационной безопасности и охраны прав граждан (*Deepfaking it: America's 2024 election collides with AI boom. URL: https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30 (дата обращения: 09.08.2025)*).

В юридической и криминалистической плоскостях важно разграничивать два близких, но юридически различающихся явления [2]:

а) «дипфейк-мошенничество» — хищение, совершаемое посредством синтезированного изображения или голоса, вводящего потерпевшего в заблуждение относительно личности либо обстоятельств события;

б) «киберпохищение» («виртуальное похищение») — комплекс действий, направленных на получение выкупа без фактического захвата и удержания потерпевшего, нередко с побуждением его к самовольному перемещению и сокрытию от близких. Разграничение данных форм необходимо для правильной квалификации, поскольку преступления против собственности и преступления против свободы личности имеют различную объективную сторону и структуру умысла. В литературе выделяются две основные модели реализации таких схем:

1. Модель А предполагает дистанционное общение с жертвой (часто с использованием дипфейка голоса родственника) и требование выкупа без побуждения потерпевшего к перемещению. Такая схема, как правило, подпадает под квалификацию мошенничества.

2. Модель В включает комбинированный сценарий: под воздействием обмана и угроз

потерпевший самостоятельно покидает место проживания, укрывается и прекращает связь с семьей, а параллельно злоумышленники выдвигают требования выкупа. В этой модели возникает конкуренция между составами, охраняющими свободу личности, и составами против собственности. Однако чаще всего применяется совокупность норм (незаконное лишение свободы и вымогательство), но подобная квалификация во многом является «вынужденной» вследствие пробелов в описании объективной стороны.

Отдельного анализа требует связь технологий глубокого синтеза с фальсификацией биометрических данных — индивидуально-определяющих физиологических и поведенческих характеристик человека (изображение лица, тембр голоса, мимика, жесты, манера речи). Дипфейк способен воспроизводить эти параметры с такой степенью достоверности, что под угрозу ставится не только доверие к аудио- и видеоматериалам, но и надежность автоматизированных систем аутентификации, основанных на биометрии. В результате проблема выходит за пределы информационной безопасности, переходя в сферу защиты персональных данных и цифровой идентичности [3].

В этой связи актуализируется необходимость выработки комплексных мер, включающих как правовые, так и технологические решения. Их цель — обеспечить баланс между законным использованием технологий глубокого синтеза и защитой от их вредоносного применения, включая неправомерный доступ к биометрическим данным и их подделку.

Современная юридическая наука, реагируя на вызовы, связанные с дипфейками, должна решать ряд ключевых задач:

1) оценка применимости действующих уголовно-правовых конструкций к зафиксированным и потенциальным случаям противоправного использования технологии;

2) установление социально-правовых оснований для запрета отдельных форм применения дипфейков, в том числе с использованием мер уголовно-правового воздействия;

3) определение пределов и форм криминализации, исключающих чрезмерное ограничение свободы выражения и творчества.

Дальнейший анализ в рамках данного исследования предполагает комплексное рассмотрение феномена дипфейка, включающее криминалистические, уголовно-правовые и компаративистские аспекты, а также изучение зарубежного опыта регулирования и применения технологий глубокого синтеза.

Проблематика дипфейков исследуется преимущественно в междисциплинарной плоскости, что обусловлено многоаспектностью их влияния. Приоритетной задачей остается разработка алгоритмов автоматизированного выявления и оперативного удаления синтетического контента из цифровой среды. Подобные решения направлены на сокращение времени реагирования и предотвращение повторного распространения модифицированных материалов, а также на повышение точности их идентификации при судебно-экспертных исследованиях.

Социально-гуманитарный аспект отражен в социологических работах, анализирующих воздействие дипфейков на массовое сознание и общественные коммуникации [4; 5], а также в политологических исследованиях, изучающих их роль как инструмента информационной войны [6].

В области журналистики и медиаисследований рассматриваются трансформации форм массовой коммуникации и снижение доверия к медиапродукции в условиях роста технологических возможностей фальсификации [7; 8]. Отмечается, что подрыв доверия к визуальной информации способен иметь долговременные последствия для институтов массовой информации и демократии.

В отечественной юридической науке внимание исследователей сконцентрировано как на частноправовых, так и на публично-правовых аспектах регулирования. Анализируются в том числе гражданско-правовые механизмы защиты нематериальных благ при посмертном использовании голоса или изображения [9].

Значительное внимание уделяется рискам, которые технологии глубокого синтеза создают для медиабезопасности и репутации организаций. Исследования фиксируют угрозу подрыва доверия к брендам и деловой репутации в условиях целенаправленного распространения синтетического контента [10].

В научных публикациях также рассматриваются меры гражданско-правового и административного реагирования на создание и распространение дипфейков [11; 12]. Отдельное направление составляют работы, посвященные достоверности цифровых доказательств и адаптации судебного процесса к вызовам цифровизации [13; 14].

В юридической литературе находит отражение и возможность правомерного использования дипфейков в деятельности правоохранительных органов, включая оперативно-розыскную работу, что предполагает баланс между эффективностью выявления правонарушений и защитой прав личности [15].

Таким образом, обзор литературы демонстрирует, что проблема дипфейков затрагивает широкий круг дисциплин — от инженерных и медийных до правовых. Для выработки адекватных мер противодействия необходимо междисциплинарное взаимодействие, объединяющее технологические разработки, социально-гуманитарные исследования и юридический анализ.

Проведенный анализ подтверждает, что технология дипфейк используется в различных сферах — от культурных и образовательных до криминальных. В искусстве и рекламе синтезированные образы знаменитостей применялись с согласия правообладателей, в том числе в случае с Брюсом Ли в рекламе виски *Johnnie Walker* (*The Emergence of Deepfake Technology: A Review. URL: https://www.timreview.ca/article/1282 (дата обращения: 09.08.2025)*).

В образовательной деятельности глубокий синтез может повышать наглядность и вовлеченность аудитории, например, через создание учебных видеороликов, где исторические деятели или ученые «рассказывают» о событиях или научных концепциях. При наличии согласия правообладателей и соблюдении авторских прав такие проекты имеют значительный просветительский потенциал.

Растет число случаев неправомерного применения технологий глубокого синтеза. К наиболее распространенным видам относятся:

— изготовление и распространение порнографических материалов — объект охраны: общественная нравственность (ст. 242 Уголовного кодекса Российской Федерации); типичные доказательства: цифровые файлы, метаданные, заключения компьютерно-технической и искусствоведческой экспертиз;

— нарушение неприкосновенности частной жизни — конституционное право на тайну личной жизни (ст. 137 УК РФ); доказательства: синтетические фото- и видеоматериалы, подтверждение отсутствия согласия субъекта, показания потерпевшего;

— вмешательство в избирательные процессы — конституционные права граждан избирать и быть избранными (ст. 141 УК РФ); доказательства: дипфейк-ролики с дискредитирующим содержанием, анализ цифровых следов публикации и распространения;

— мошенничество — имущественные права (ст. 159 или 159.6 УК РФ); доказательства: аудио- или видеозаписи, созданные для введения в заблуждение, а также цифровые транзакционные следы;

— дискредитация государственных органов — авторитет власти и общественное доверие (возможна квалификация по ряду составов в зависимости от способа и последствий); доказательства: синтетические материалы, установление факта их распространения и умысла.

Использование дипфейка как средства обмана охватывается положениями о мошенничестве: при вмешательстве в компьютерную информацию — ст. 159.6 УК РФ, при его отсутствии — ст. 159 УК РФ. В доктрине отмечается, что форма обмана не изменяет юридическую природу преступления: способ совершения не подменяет состав, что обуславливает осторожность в признании использования ИИ самостоятельным отягчающим обстоятельством. Приоритет в таких случаях следует отдавать точной квалификации и доказательству самого факта применения синтетического изображения или голоса.

В судебной практике уже зафиксированы споры, связанные с использованием внешности известных лиц в синтетическом контенте без их согласия. Так, Арбитражный суд города Москвы рассматривал дело о неправомерном применении образа актера Киану Ривза в рекламном ролике, созданном с использованием технологий глубокого синтеза. Суд установил, что отсутствие согласия правообладателя и искажение образа в коммерческих целях нарушают исключительные права на изображение, что послужило основанием для привлечения ответчика к гражданско-правовой ответственности. Этот прецедент иллюстрирует, что дипфейки становятся объектом не только уголовно-правовой, но и активной гражданско-правовой защиты *(Суд в РФ впервые взыскал компенсацию за использование дипфейк-видео без разрешения. URL: https://tass.ru/obschestvo/19463433 (дата обращения: 09.08.2025)*).

Выявление факта использования технологий глубокого синтеза в рамках расследования преступлений требует проведения специальных процессуальных действий. Наиболее эффективным инструментом является назначение комплексной компьютерно-технической и лингвистической экспертизы, целью которой выступает выявление признаков синтетической генерации изображения или голоса. Экспертный анализ включает выявление артефактов в видеопотоке, установление несоответствия мимических движений и речевого сопровождения, а также фиксацию цифровых шумов, характерных для работы алгоритмов генеративных нейросетей. При необходимости используются эталонные базы биометрических данных и методы спектрографического анализа голоса для сопоставления с оригиналом.

Судебная практика подчеркивает необходимость полной процессуальной фиксации всего цикла получения, передачи и исследования цифрового доказательства. Это обеспечивает проверяемость и исключает сомнения в его достоверности. Нарушение

таких требований может повлечь признание доказательств недопустимыми.

В ряде государств правоохранительные органы уже применяют алгоритмы автоматического выявления синтетических медиа, интегрированные в системы мониторинга цифрового пространства. Эти системы способны анализировать миллионы изображений и видеозаписей в реальном времени, определяя характерные для дипфейков искажения (например, индийская облачная система *Vastav.AI*).

В России аналогичные решения тестируются в подразделениях МВД и Роскомнадзора, включая алгоритмы поиска контента в социальных сетях и мессенджерах. Несмотря на высокую точность обнаружения и значительное сокращение времени реагирования, такие технологии пока функционируют в пилотном режиме и не закреплены нормативно, что ограничивает их использование в качестве источника процессуально значимой информации.

Практика последних лет демонстрирует, что технологии глубокого синтеза становятся инструментом сложных и высокотехнологичных преступных схем.

Пожилая женщина, став жертвой телефонных мошенников, была обманом выведена из места жительства и лишена возможности общения с родственниками; действия квалифицированы по п. «а» ч. 2 ст. 127 УК РФ и п. «б» ч. 3 ст. 163 УК РФ (*СК возбудил уголовное дело после исчезновения матери советника сенатора. URL: https://ria.ru/20230420/delo-1866606667.html (дата обращения: 09.08.2025)*).

В Гонконге в 2023г. злоумышленники, используя глубокий синтез образа финансового директора и коллег посредством дипфейк-видео, убедили сотрудника компании провести перевод более 25млн долл. (*Real insurance coverage for increasing AI deepfake risks. URL: https://www.reuters.com/legal/legalindustry/real-insurance-coverage-increasing-ai-deepfake-risks-2024-04-11 (дата обращения: 09.08.2025)*).

В Великобритании в 2019 г. была зафиксирована афера, при которой мошенники сымитировали голос руководителя и убедили сотрудника перевести 220 тыс. евро на счета, находящиеся под их контролем (*How to guard against voice cloning and deepfake scams. URL: https://www.icaew.com/insights/viewpoints-on-the-news/2025/jan-2025/how-to-guard-against-voice-cloning-and-deepfake-scams (дата обращения: 09.08.2025)*).

В 2024г. Центральный банк России предупредил, что мошенники все чаще имитируют голоса родственников или знакомых потенциальных жертв, используя дипфейк-технологии для обмана и хищения денежных средств (*ЦБ: мошенники стали имитировать голоса родных потенциальной жертвы. URL: https://www.mk.ru/social/2024/01/17/cb-moshenniki-stali-imitirovat-golosa-rodnykh-potencialnoy-zhertvy.html (дата обращения: 09.08.2025)*).

Эти примеры подтверждают, что дипфейки способны не только обходить традиционные технологические и процедурные механизмы аутентификации, но и существенно осложнять расследование. Сравнительно-правовой анализ показывает, что ряд зарубежных государств уже выработал специализированные меры противодействия вредоносному применению дипфейков.

В рамках *National Defense Authorization Act for Fiscal Year2020* (NDAA-2020) на федеральном уровне США было предусмотрено финансирование исследований, направленных на минимизацию влияния синтетических медиа (*deepfakes*) на

политические процессы, включая выборы (*First Federal Legislation on Deepfakes Signed Into Law. URL: https://www.wilmerhale.com/en/insights/client-alerts/20191223-first-federal-legislation-on-deepfakes-signed-into-law (дата обращения: 09.08.2025)*):

— в Техасе установлена ответственность за создание поддельных видеозаписей с целью вмешательства в выборы (штраф до 4 тыс. долл. и лишение свободы до одного года);

— в Вирджинии — за изготовление и распространение порнографических материалов с применением технологий глубокого синтеза.

Аналогичные инициативы реализуются в Великобритании, Австралии и Южной Корее, где вводятся ограничения на распространение и коммерческое использование поддельных аудио- и видеозаписей без согласия субъектов.

В уголовном законодательстве Китая отсутствует специальная норма, направленная исключительно на биометрическую информацию; однако незаконное приобретение, продажа или фальсификация персональных данных — включая биометрию — при наличии особо серьезных последствий подпадают под действие ст. 253 УК КНР («нарушение гражданской личной информации»), что подтверждается судебной практикой о взыскании лишь при получении незаконного дохода, превышающего значимую сумму. Закон КНР «О защите личной информации» (PIPL, 2021) относит биометрические данные (лицо, голос) к категории «чувствительной персональной информации», обработка которой требует отдельного, информированного согласия и строгих защитных мер.

Для повышения эффективности расследования преступлений, совершаемых с использованием дипфейков, требуется разработка и внедрение унифицированной методики доказывания, обязательной для применения на всей территории Российской Федерации. Такая методика должна включать:

— назначение комплексной экспертизы (компьютерно-технической, фоноскопической, лингвистической), направленной на достоверное установление факта синтетической генерации изображения или голоса;

— установление единых стандартов отбора, хранения и передачи цифровых доказательств, исключающих их модификацию или подмену;

— сертификацию специализированного программного обеспечения, используемого для распознавания дипфейков, с целью повышения доверия судов к его результатам;

— формирование национальной базы эталонных биометрических данных с защищенным доступом для экспертов, что позволит ускорить процесс идентификации и верификации. В 2024 г. в России анонсировано создание базы биометрических данных мошенников, включая голосовые образцы, для оперативного выявления и пресечения противоправных действий (*Узнать по голосу: в России появится база биометрических данных мошенников. URL: https://iz.ru/1913710/maria-frolova/uznat-po-golosu-v-rossii-poavitsa-baza-biometriceskih-dannyh-mosennikov (дата обращения: 09.08.2025)*);

— подготовку судебных экспертов, обладающих одновременно навыками цифровой криминалистики и знанием правовых требований к допустимости доказательств.

Введение такой методики обеспечит единообразие правоприменительной практики, повысит предсказуемость квалификации деяний и сократит число судебных ошибок,

связанных с оценкой цифровых доказательств. Реальные случаи многомиллионных хищений, совершенных с использованием технологий глубокого синтеза, подтверждают необходимость их приоритетного учета в национальной стратегии кибербезопасности. Для минимизации финансовых и корпоративных рисков целесообразно:

— внедрить обязательные механизмы многофакторной аутентификации при дистанционных финансовых операциях, исключающие возможность одобрения транзакций исключительно на основе голосовой или видеосвязи;

— разработать отраслевые рекомендации для корпоративного сектора по проверке подлинности участников цифровых коммуникаций, включая верификацию через независимые каналы связи;

— закрепить в уголовном законодательстве квалифицирующие признаки для мошенничества и иных имущественных преступлений, совершенных с использованием синтетических медиа, с учетом размера причиненного ущерба;

— сформировать межведомственные группы быстрого реагирования для расследования высокотехнологичных преступлений с применением дипфейков, в состав которых должны входить специалисты в области искусственного интеллекта, цифровой криминалистики и киберразведки.

Реализация данных мер позволит существенно повысить защищенность финансовых операций, сократить вероятность успешного совершения мошеннических действий и укрепить навыки выявления и предотвращения угроз как в корпоративном секторе, так и на уровне частных пользователей.

Высокая точность воспроизведения дипфейком индивидуальных биометрических характеристик требует включения в российскую систему правовой защиты комплекса специальных мер. Предлагается:

— закрепить в федеральных законах «О персональных данных» и «Об информации, информационных технологиях и о защите информации» легальное определение «синтетический биометрический образ», под которым понимать искусственно сгенерированные с использованием технологий глубокого синтеза изображения лица, голоса или иных биометрических параметров;

— установить запрет на их использование без предварительного согласия субъекта данных, за исключением прямо предусмотренных законом случаев;

— ввести обязательную технологическую маркировку цифрового контента, содержащего синтетические биометрические данные, с сохранением метаданных, позволяющих идентифицировать факт применения технологий глубокого синтеза;

— усилить системы аутентификации за счет методов, устойчивых к подделке с помощью дипфейка, включая поведенческую биометрию и анализ микродвижений лица;

— разработать для правоохранительных органов методические рекомендации по выявлению и фиксации фактов использования синтетических биометрических данных в противоправных целях.

Такая модель позволит повысить устойчивость систем идентификации к вмешательству, упростить процесс доказывания в суде и гармонизировать российское законодательство с международными стандартами защиты биометрической информации.

С учетом международного опыта и нарастающих угроз целесообразно рассмотреть возможность включения в Уголовный кодекс РФ самостоятельного состава преступления, предусматривающего ответственность за незаконное использование, фальсификацию и оборот биометрических данных, полученных как традиционными способами, так и с применением технологий глубокого синтеза.

Предлагаемая конструкция может включать:

— основной состав, охватывающий неправомерное извлечение, хранение, передачу или модификацию биометрических данных без согласия субъекта;

— квалифицированные виды — с использованием технологий глубокого синтеза, с причинением значительного имущественного или нематериального ущерба, а также в целях совершения тяжких или особо тяжких преступлений;

— отягчающие признаки — совершение деяния в отношении несовершеннолетнего, в крупном размере либо с использованием служебного положения;

— процессуальные гарантии — обязательное проведение судебной экспертизы для установления факта применения технологий глубокого синтеза.

Введение такого состава обеспечит:

— правовую определенность и единообразие квалификации деяний, связанных с подделкой биометрии;

— упрощение процесса доказывания, выделив сам факт неправомерного обращения с биометрическими данными как самостоятельный объект уголовно-правовой охраны;

— гармонизацию национального законодательства с международными тенденциями, в которых защита биометрии рассматривается как ключевой элемент цифрового суверенитета.

Важным шагом в институционализации борьбы с вредоносным применением технологий глубокого синтеза стало включение в утвержденные формы статистической отчетности Генеральной прокуратуры РФ отдельного показателя «с использованием технологии дипфейк» (п. 049 Приказа от 9 декабря 2022 г. № 746).

Однако, по состоянию на 2024 г., данный учет находился в стадии становления и не обеспечивал полноты охвата всех релевантных случаев. Отсутствие стандартизированных методик фиксации и кодирования таких преступлений затрудняет проведение комплексного анализа, выявление динамики и выработку адресных мер противодействия.

Для устранения этих проблем представляется целесообразным:

— разработать единые критерии отнесения преступлений к категории «с использованием технологии дипфейк»;

— обеспечить согласованность статистических данных Генеральной прокуратуры, МВД и Роскомнадзора;

— синхронизировать российскую систему учета с международными классификаторами киберпреступлений, что упростит обмен информацией в рамках трансграничного сотрудничества;

— внедрить автоматизированные системы анализа и сопоставления данных, позволяющие выявлять скрытые тенденции и межрегиональные различия.

Совершенствование методики статистического учета позволит не только повысить качество аналитики, но и сделает государственную политику в сфере противодействия дипфейкам более доказательной и результативной.

Судебная практика, включая дело Арбитражного суда города Москвы об использовании образа актера Киану Ривза, демонстрирует необходимость комплексной правовой защиты от неправомерной коммерческой эксплуатации синтетических изображений. Такая защита должна строиться по многоуровневой модели:

1. Уголовно-правовой компонент — применение норм, предусматривающих ответственность за деяния, посягающие на собственность, честь, достоинство или неприкосновенность частной жизни, в случаях, когда использование образа сопровождается иными противоправными действиями.

2. Гражданско-правовой компонент — защита исключительных прав на изображение, включая возможность требования удаления незаконно созданного или распространенного контента и компенсации причиненного ущерба.

3. Административно-правовой компонент — пресечение нарушений правил рекламной деятельности и норм, регулирующих оборот персональных данных.

Реализация такой комплексной модели позволит правоприменителю гибко реагировать на различные формы неправомерного использования дипфейков, обеспечивая баланс между защитой прав личности и допустимым оборотом синтетического контента в культурных, образовательных и коммерческих целях.

При разработке правовых механизмов противодействия вредоносным дипфейкам важно избежать чрезмерного регулирования, способного ограничить свободу выражения мнения, закрепленную ст. 29 Конституции РФ и международными договорами. Для сохранения баланса между защитой прав личности и поддержанием творческой свободы целесообразно закрепить в законодательстве следующие положения:

1. Законодательные исключения — разрешение создания и распространения синтетических медиа в целях сатиры, пародии, образовательных и научных исследований, при условии отсутствия умысла на причинение вреда личности или ее репутации.

2. Критерии общественного интереса — формализация признаков, позволяющих правоприменителю различать допустимый и вредоносный контент.

3. Процедуры оценки соразмерности мер — обязательная проверка необходимости и пропорциональности удаления или блокировки материалов, включая судебный контроль в спорных случаях.

4. Применение теста «наименее ограничительного вмешательства» — приоритет тем мерам, которые минимально затрагивают свободу выражения, но обеспечивают эффективную защиту прав и интересов.

Такой подход позволит сохранить пространство для законного применения технологий глубокого синтеза в искусстве, науке и журналистике, одновременно выстраивая надежные механизмы защиты от их противоправного использования.

Ввиду отсутствия надлежащего правового регулирования в доктрине обосновывается необходимость включения в Уголовный кодекс РФ самостоятельного состава преступления, предусматривающего ответственность за незаконное использование, подделку и оборот биометрических данных, включая синтетические образы, созданные с применением технологий глубокого синтеза. Целесообразно также дополнить ряд составов квалифицирующим признаком «совершение преступления с использованием технологии дипфейк». Закрепление таких положений позволит учесть специфическую опасность визуально-аудиального обмана, унифицировать судебную практику и упростить доказывание. Вместе с тем введение квалифицирующего признака должно сопровождаться разъяснениями Верховного Суда РФ о пределах его применения, в том числе о допустимости использования технологий глубокого синтеза в сатирических, образовательных и иных общественно значимых целях при отсутствии умысла на причинение вреда личности или ее репутации.

В целях обеспечения оперативности и эффективности расследования преступлений с использованием дипфейков целесообразно внедрить в деятельность правоохранительных органов системы автоматического выявления синтетических медиа. Предлагается:

— создать централизованную платформу мониторинга, интегрированную с базами данных МВД, Роскомнадзора и Генеральной прокуратуры, предназначенную для обнаружения и фиксации потенциально вредоносного контента в режиме реального времени;

— разработать алгоритмы на основе машинного обучения, способные адаптироваться к новым методам генерации дипфейков и минимизировать количество ложноположительных срабатываний;

— нормативно закрепить порядок использования таких технологий, включая требования к защите персональных данных и процессуальной допустимости полученных результатов;

— включить обучение работе с системами автоматического выявления в программы подготовки следователей, прокуроров и оперативных сотрудников.

Интеграция подобных технологий в правоприменительную деятельность позволит существенно сократить время обнаружения и блокировки вредоносных материалов, повысить качество доказательной базы и снизить нагрузку на экспертов.

Системный анализ российской и зарубежной практики обосновывает целесообразность включения в Уголовный кодекс РФ квалифицирующего признака «совершение преступления с использованием технологии дипфейк». Такая норма позволит:

— учитывать повышенную общественную опасность деяний, при которых визуально-аудиальная форма обмана усиливает психологическое воздействие на потерпевшего;

— унифицировать квалификацию преступлений в различных сферах (против собственности, свободы личности, конституционных прав и свобод);

— снизить количество случаев применения «вынужденных» совокупностей составов, вызванных пробелами в описании объективной стороны деяния;

— обеспечить правоприменителю предсказуемый инструмент реагирования на высокотехнологичные преступления.

Введение данной нормы должно сопровождаться развитием технических и организационных механизмов фильтрации и пресечения вредоносного контента. Без

комплексного подхода изолированная репрессивная мера окажется малоэффективной. Оптимальной представляется комбинация законодательных нововведений с внедрением технологий автоматического выявления дипфейков, совершенствованием судебной экспертизы и формированием профессиональных компетенций в правоохранительных органах.

Библиография

1. 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. EDN: LXAWLM.
2. Долгиева М. М. Квалификация дипфейк-мошенничества и киберпохищения человека // Актуальные проблемы российского права. 2024. Т. 19. № 11. С. 106-113. DOI: 10.17803/1994–1471.2024.168.11.106-113. EDN: GDLNXP.
3. Мосечкин И. Н. Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования // Вестник Санкт-Петербургского университета. Право. 2025. Т. 16. № 1. С. 95-110. DOI: 10.21638/spbu14.2025.107. EDN: QGPADN.
4. Уртаева Э. Б. Возможности и угрозы применения искусственного интеллекта (ИИ) в политических коммуникациях // Общество: политика, экономика, право. 2024. № 2. С. 44-51. DOI: 10.24158/pep.2024.2.3. EDN: UALQLW.
5. Иванов В. Г., Игнатовский Я. Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник РУДН. Серия: Государственное и муниципальное управление. 2020. Т. 7. № 4. С. 379-386. DOI: 10.22363/2312–8313-2020-7-4-379-386. EDN: YJJUWH.
6. Красовская Н. Р., Гуляев А. А. Технологии манипуляции сознанием при использовании дипфейков // Власть. 2020. Т. 28. № 4. С. 93-98. DOI: 10.31171/vlast.v28i4.7439. EDN: GQJJQY.
7. Васильева И. А., Халина Н. В. Дипфейк как технология призрачных коммуникаций // PR и реклама в изменяющемся мире: региональный аспект. 2021. № 25. С. 111-116. EDN: DDCSUY.
8. Купка И. П., Щербаков С. С. Дипфейк как информационное оружие современности // Динамика медиасистем. 2023. Т. 3. № 1. С. 375-381. EDN: IAHENL.
9. Яценко Т. С. Проблемы гражданско-правового регулирования посмертного использования нематериальных благ // Журнал российского права. 2023. Т. 27. № 7. С. 35-46. DOI: 10.12737/jrp.2023.077. EDN: DMSJHN.
10. Никишин В. Д. Репутационная безопасность и медиабезопасность компаний и проектов в контексте целей устойчивого развития и ESG-принципов // Актуальные проблемы российского права. 2022. Т. 17. № 9. С. 73-82. DOI: 10.17803/1994–1471.2022.142.9.073-082. EDN: MKOIFG.
11. Калятин В. О. Дипфейк как правовая проблема: новые угрозы или новые возможности? // Закон. 2022. № 7. С. 87-103. DOI: 10.37239/0869–4400-2022-19-7-87-103. EDN: FENGGS.
12. Минбалеев А. В. Проблемы гражданско-правовой защиты личных неимущественных прав в процессе цифрового профилирования граждан // Гражданское право. 2022. № 2. С. 9-11. DOI: 10.18572/2070–2140-2022-2-9-11. EDN: TQOLTI.
13. Апостолова Н. Н. Достоверность доказательств и технологии дипфейка // Российский судья. 2023. № 11. С. 7-11. DOI: 10.18572/1812–3791-2023-11-7-11. EDN: OUSXSG.
14. Лаптев В. А. Deepfake и иные продукты искусственного интеллекта на пути развития онлайн-правосудия // Актуальные проблемы российского права. 2021. Т. 16. № 11. С. 180-186. DOI: 10.17803/1994–1471.2021.132.11.180-186. EDN: HOMQCG.
15. Батоев В. Б. Об использовании технологии "Deepfake" в оперативно-розыскной

деятельности // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2023. № 1. С. 70-76. DOI: 10.36511/2078–5356-2023-1-70-76. EDN: MKPHSD.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом исследования в представленной на рецензирование статье является, как это следует из ее наименования, цифровая мимикрия. Автор сосредоточил внимание на анализе защиты прав личности от противоправного применения дипфейк-технологий. Заявленные границы исследования соблюдены ученым.
Методология исследования в тексте статьи не раскрывается.
Актуальность избранной автором темы исследования несомненна и обосновывается им следующим образом: "Термин «дипфейк» был введен в 2017 г. на платформе Reddit и первоначально обозначал подмену изображения лица с применением алгоритмов искусственного интеллекта (ИИ) для генерации новых, реалистично выглядящих изображений [1]. Развитие технологий привело к выходу за рамки статичных визуальных манипуляций: современные алгоритмы синтезируют не только изображение, но и голос, создавая аудио- и видеоконтент с использованием внешности или тембра иного лица. Для этого не требуется глубоких технических знаний или дорогостоящего оборудования: ряд мобильных приложений позволяет сформировать дипфейк-ролик за считанные минуты. Потенциально допустимое использование таких технологий охватывает широкий спектр — от кинопроизводства (омоложение актеров, языковая адаптация фильмов, безопасная постановка сложных трюков) до образования и медицины. Так, технологии глубокого синтеза применялись для воссоздания экранных образов умерших артистов и реализации коммерческих проектов при согласии правообладателей, в том числе для использования образа Леонида Куравлева в рекламной кампании Сбербанка (Сбербанк воссоздал образ Жоржа Милославского и сделал его своим новогодним амбассадором. URL: https://tass.ru/obschestvo/10145879 (дата обращения: 09.08.2025)). Широкое распространение технологий цифрового синтеза обусловливает существенные риски их противоправного использования, что предопределяет необходимость их анализа в контексте уголовно-правового регулирования. В 2023 г. количество видеоматериалов, созданных с применением технологий глубокого синтеза, утроилось, а объем поддельных голосовых записей увеличился в восемь раз по сравнению с 2022 г., по данным DeepMedia, что свидетельствует о стремительном распространении соответствующих технологий и усилении угроз для информационной безопасности и охраны прав граждан (Deepfaking it: America’s 2024 election collides with AI boom. URL: https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30 (дата обращения: 09.08.2025))" и др. Ученый подробно раскрывает степень изученности рассматриваемых в статье проблем: "Социально-гуманитарный аспект отражен в социологических работах, анализирующих воздействие дипфейков на массовое сознание и общественные коммуникации [4; 5], а также в политологических исследованиях, изучающих их роль как инструмента информационной войны [6]. В области журналистики и медиаисследований рассматриваются трансформации форм массовой коммуникации и снижение доверия к медиапродукции в условиях роста технологических возможностей фальсификации [7; 8]. Отмечается, что подрыв доверия к визуальной информации способен иметь долговременные последствия для институтов массовой информации и демократии. В отечественной юридической науке внимание исследователей сконцентрировано как на частноправовых, так и на публично-правовых

аспектах регулирования. Анализируются в том числе гражданско-правовые механизмы защиты нематериальных благ при посмертном использовании голоса или изображения [9]. Значительное внимание уделяется рискам, которые технологии глубокого синтеза создают для медиабезопасности и репутации организаций. Исследования фиксируют угрозу подрыва доверия к брендам и деловой репутации в условиях целенаправленного распространения синтетического контента [10].

В научных публикациях также рассматриваются меры гражданско-правового и административного реагирования на создание и распространение дипфейков [11; 12]. Отдельное направление составляют работы, посвященные достоверности цифровых доказательств и адаптации судебного процесса к вызовам цифровизации [13; 14].

В юридической литературе находит отражение и возможность правомерного использования дипфейков в деятельности правоохранительных органов, включая оперативно-розыскную работу, что предполагает баланс между эффективностью выявления правонарушений и защитой прав личности [15]".

Научная новизна работы проявляется в ряде заключений автора: "Выявление факта использования технологий глубокого синтеза в рамках расследования преступлений требует проведения специальных процессуальных действий. Наиболее эффективным инструментом является назначение комплексной компьютерно-технической и лингвистической экспертизы, целью которой выступает выявление признаков синтетической генерации изображения или голоса. Экспертный анализ включает выявление артефактов в видеопотоке, установление несоответствия мимических движений и речевого сопровождения, а также фиксацию цифровых шумов, характерных для работы алгоритмов генеративных нейросетей. При необходимости используются эталонные базы биометрических данных и методы спектрографического анализа голоса для сопоставления с оригиналом. Судебная практика подчеркивает необходимость полной процессуальной фиксации всего цикла получения, передачи и исследования цифрового доказательства. Это обеспечивает проверяемость и исключает сомнения в его достоверности. Нарушение таких требований может повлечь признание доказательств недопустимыми. В ряде государств правоохранительные органы уже применяют алгоритмы автоматического выявления синтетических медиа, интегрированные в системы мониторинга цифрового пространства. Эти системы способны анализировать миллионы изображений и видеозаписей в реальном времени, определяя характерные для дипфейков искажения (например, индийская облачная система Vastav.AI). В России аналогичные решения тестируются в подразделениях МВД и Роскомнадзора, включая алгоритмы поиска контента в социальных сетях и мессенджерах. Несмотря на высокую точность обнаружения и значительное сокращение времени реагирования, такие технологии пока функционируют в пилотном режиме и не закреплены нормативно, что ограничивает их использование в качестве источника процессуально значимой информации"; "Для повышения эффективности расследования преступлений, совершаемых с использованием дипфейков, требуется разработка и внедрение унифицированной методики доказывания, обязательной для применения на всей территории Российской Федерации. Такая методика должна включать:

— назначение комплексной экспертизы (компьютерно-технической, фоноскопической, лингвистической), направленной на достоверное установление факта синтетической генерации изображения или голоса; — установление единых стандартов отбора, хранения и передачи цифровых доказательств, исключающих их модификацию или подмену; — сертификацию специализированного программного обеспечения, используемого для распознавания дипфейков, с целью повышения доверия судов к его результатам;

— формирование национальной базы эталонных биометрических данных с защищенным

доступом для экспертов, что позволит ускорить процесс идентификации и верификации. В 2024 г. в России анонсировано создание базы биометрических данных мошенников, включая голосовые образцы, для оперативного выявления и пресечения противоправных действий (Узнать по голосу: в России появится база биометрических данных мошенников. URL: https://iz.ru/1913710/maria-frolova/uznat-po-golosu-v-rossii-poavitsa-baza-biometriceskih-dannyh-mosennikov (дата обращения: 09.08.2025)).; — подготовку судебных экспертов, обладающих одновременно навыками цифровой криминалистики и знанием правовых требований к допустимости доказательств. Введение такой методики обеспечит единообразие правоприменительной практики, повысит предсказуемость квалификации деяний и сократит число судебных ошибок, связанных с оценкой цифровых доказательств. Это особенно важно в условиях трансграничного характера преступлений с применением технологий глубокого синтеза, когда необходима совместимость процедур с международными стандартами"; "Для минимизации финансовых и корпоративных рисков целесообразно:

— внедрить обязательные механизмы многофакторной аутентификации при дистанционных финансовых операциях, исключающие возможность одобрения транзакций исключительно на основе голосовой или видеосвязи; — разработать отраслевые рекомендации для корпоративного сектора по проверке подлинности участников цифровых коммуникаций, включая верификацию через независимые каналы связи; — закрепить в уголовном законодательстве квалифицирующие признаки для мошенничества и иных имущественных преступлений, совершенных с использованием синтетических медиа, с учетом размера причиненного ущерба; — сформировать межведомственные группы быстрого реагирования для расследования высокотехнологичных преступлений с применением дипфейков, в состав которых должны входить специалисты в области искусственного интеллекта, цифровой криминалистики и киберразведки. Реализация данных мер позволит существенно повысить защищенность финансовых операций, сократить вероятность успешного совершения мошеннических действий и укрепить навыки выявления и предотвращения угроз как в корпоративном секторе, так и на уровне частных пользователей" и др. Таким образом, статья вносит определенный вклад в развитие отечественной правовой науки и, безусловно, заслуживает внимания потенциальных читателей.

Научный стиль исследования выдержан автором в полной мере.

Структура работы логична. Во вводной части статьи ученый обосновывает актуальность избранной им темы исследования. В основной части работы автор анализирует современное состояние защиты прав личности от противоправного применения дипфейк-технологий, выявляет соответствующие проблемы и предлагает пути их решения. В заключительной части работы содержатся выводы по результатам проведенного исследования.

Содержание статьи соответствует ее наименованию, но не лишено недостатков формального характера.

Так, автор пишет: "Российская правоприменительная практика квалифицирует такие действия по существующим нормам Уголовного кодекса Российской Федерации: ст. 242 (порнографические материалы), ст. 137 (нарушение неприкосновенности частной жизни), ст. 141 (воспрепятствование осуществлению избирательных права)" - "прав" (опечатка).

Таким образом, статья нуждается в дополнительном вычитывании - в ней встречаются опечатки.

Библиография исследования представлена 15 источниками (научными статьями). С формальной точки зрения этого достаточно.

Апелляция к оппонентам имеется, но носит общий характер. В научную дискуссию с

конкретными учеными автор не вступает, ссылаясь на ряд теоретических источников исключительно в обоснование своих суждений либо для иллюстрирования отдельных положений работы.

Выводы по результатам проведенного исследования имеются ("Судебная практика, включая дело Арбитражного суда города Москвы об использовании образа актера Киану Ривза, демонстрирует необходимость комплексной правовой защиты от неправомерной коммерческой эксплуатации синтетических изображений. Такая защита должна строиться по многоуровневой модели: 1. Уголовно-правовой компонент — применение норм, предусматривающих ответственность за деяния, посягающие на собственность, честь, достоинство или неприкосновенность частной жизни, в случаях, когда использование образа сопровождается иными противоправными действиями. 2. Гражданско-правовой компонент — защита исключительных прав на изображение, включая возможность требования удаления незаконно созданного или распространенного контента и компенсации причиненного ущерба. 3. Административно-правовой компонент — пресечение нарушений правил рекламной деятельности и норм, регулирующих оборот персональных данных.

Реализация такой комплексной модели позволит правоприменителю гибко реагировать на различные формы неправомерного использования дипфейков, обеспечивая баланс между защитой прав личности и допустимым оборотом синтетического контента в культурных, образовательных и коммерческих целях. При разработке правовых механизмов противодействия вредоносным дипфейкам важно избежать чрезмерного регулирования, способного ограничить свободу выражения мнения, закрепленную ст. 29 Конституции РФ и международными договорами. Для сохранения баланса между защитой прав личности и поддержанием творческой свободы целесообразно закрепить в законодательстве следующие положения: 1. Законодательные исключения — разрешение создания и распространения синтетических медиа в целях сатиры, пародии, образовательных и научных исследований, при условии отсутствия умысла на причинение вреда личности или ее репутации.

2. Критерии общественного интереса — формализация признаков, позволяющих правоприменителю различать допустимый и вредоносный контент. 3. Процедуры оценки соразмерности мер — обязательная проверка необходимости и пропорциональности удаления или блокировки материалов, включая судебный контроль в спорных случаях. 4. Применение теста «наименее ограничительного вмешательства» — приоритет тем мерам, которые минимально затрагивают свободу выражения, но обеспечивают эффективную защиту прав и интересов. Такой подход позволит сохранить пространство для законного применения технологий глубокого синтеза в искусстве, науке и журналистике, одновременно выстраивая надежные механизмы защиты от их противоправного использования" и др.), обладают свойствами достоверности, обоснованности и, несомненно, заслуживают внимания научного сообщества.

Интерес читательской аудитории к представленной на рецензирование статье может быть проявлен прежде всего со стороны специалистов в сфере административного права, информационного права, гражданского права, уголовного права, уголовного процесса и криминалистики при условии ее доработки: раскрытии методологии исследования, введении дополнительных элементов дискуссионности, устранении небольших нарушений в оформлении статьи.

Результаты процедуры повторного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

Рецензия на статью
«Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий»
Объектом исследования выступает совокупность правоотношений, возникающих в ходе защиты прав личности от противоправного применения дипфейк-технологий. Предметом представленного на рецензирование исследования являются теоретические воззрения по тематике статьи, правовая регламентация защиты прав личности от противоправного применения дипфейк-технологий, а также правоприменительная практика в изучаемой сфере.
Среди методологического арсенала автора особенно полезными, исходя из целей и задач, следует признать методы сравнительно-правового анализа в плане сопоставления средств и методов защиты прав личности от противоправного применения дипфейк-технологий в разных государствах; системно-структурный, примененный «для установления взаимосвязей между уголовно-правовыми, административно-правовыми и гражданско-правовыми механизмами защиты», формально-юридический, с помощью которого автор выявлял и системного толковал нормы российского и зарубежного законодательства, регулирующих обращение с синтетическими медиа. Вместе с тем автор не проводит должную классификацию использованных методов, обозначив их в обобщенную группу: «Методологическая основа исследования строится на сочетании общенаучных и частнонаучных методов». Однако формально-юридический метод, обозначенный с самого начала, ни к тем, ни к другим не относится: это специальный юридический метод.
Актуальность разработки заявленной темы не вызывает сомнений в свете широкого распространения киберпреступности в целом и противоправного применения дипфейк-технологий в частности. Автор справедливо отмечает на этот счет: «В 2023 г. количество видеоматериалов, созданных с применением технологий глубокого синтеза, утроилось, а объем поддельных голосовых записей увеличился в восемь раз по сравнению с 2022 г., по данным DeepMedia, что свидетельствует о стремительном распространении соответствующих технологий и усилении угроз для информационной безопасности и охраны прав граждан».
Статья обладает, на наш взгляд, достаточным уровнем научной новизны, поскольку является одним из первых исследований, в котором исследуется защита прав личности от противоправного применения дипфейк-технологий с учетом необходимости определения баланса мер правового реагирования со свободой творчества и самовыражения. Кроме того, заслуживают внимания предложенные изменения действующего законодательства и унифицированной методики доказывания.
Статья характеризуется в целом научным стилем изложения.
Логика изложения при этом не всегда безупречна. Так, автор приводит пример правомерного использования образа покойного киноактёра: «Так, технологии глубокого синтеза применялись для воссоздания экранных образов умерших артистов и реализации коммерческих проектов при согласии правообладателей, в том числе для использования образа Леонида Куравлева в рекламной кампании Сбербанка». Через несколько абзацев подобный пример в почти тех же формулировках приводится снова в сочетании с аналогичной ситуацией с образом Брюса Ли.
Выявленные автором модели киберпохищения было бы логичнее переместить выше, в ту часть статьи, где это явление впервые характеризуется читатели. В противном случае модели выглядят, как «остров» в окружении не связанной с ними информации.
Автор отмечает, что «практика последних лет демонстрирует, что технологии глубокого синтеза становятся инструментом сложных и высокотехнологичных преступных схем, в

том числе с трансграничным характером». Далее даются два отечественных и два зарубежных примера, трансграничный характер которых неочевиден.

Автором дважды в разных частях статьи, но в очень схожих формулировках даются предложения включить в УК РФ самостоятельный состав преступления, предусматривающий ответственность за незаконное использование, подделку и оборот биометрических данных, а также дополнить УК РФ квалифицирующим признаком «совершение преступления с использованием технологии дипфейк». Рекомендуется компактно разместить предложения в качестве одного из финальных выводов в заключительной части статьи.

Библиография как по своему наполнению, так и по оформлению представляется вполне соответствующей работам соответствующего рода.

Апелляция к оппонентам достаточна по своему объему и вполне информативна.

В целом следует заключить, что представленная на рецензирование статья вызовет определенный интерес у читательской аудитории, заинтересованной в уголовно-правовых исследованиях. При условии определенной доработки она может быть рекомендована к публикации.

Результаты процедуры окончательного рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

На рецензирование представлена статья на тему «Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий» для опубликования в журнале «Полицейская и следственная деятельность». Статья посвящена комплексному анализу уголовно-правовых и криминалистических аспектов противоправного использования технологий глубокого синтеза (дипфейков) в контексте защиты прав личности. Предмет охватывает квалификацию деяний, пробелы в законодательстве (российском и международном), преступные схемы, допустимое использование, проблемы доказательств и предложения по совершенствованию правового регулирования и практики противодействия. Автор обоснованно применяет комплекс методов: системно-структурный, анализ и синтез, сравнительно-правовой, криминалистический, формально-юридический. Такой подход обеспечивает всестороннее рассмотрение объекта. Методология адекватна поставленным исследовательским задачам. Однако эмпирическая часть (анализ конкретных дел, статистики МВД/СК РФ по дипфейк-преступлениям) представлена фрагментарно, преимущественно примерами из СМИ. Использование конкретных данных судебной статистики Генпрокуратуры РФ (указанной в п.049 Приказа № 746) усилило бы аргументацию. Тема обладает высокой степенью актуальности. Экспоненциальный рост возможностей и доступности дипфейк-технологий (подтверждаемый данными DeepMedia и предупреждениями ЦБ РФ) создает серьезные вызовы для правопорядка, информационной безопасности и защиты фундаментальных прав (неприкосновенность частной жизни, достоинство, имущественные права, избирательные права). Рост числа инцидентов, как в России, так и за рубежом (примеры с финансовыми директорами, имитацией голоса родственников), и пробелы в правовом регулировании делают исследование своевременным и востребованным. Данные МВД РФ и аналитических центров (например, РАНХиГС) фиксируют устойчивый рост киберпреступлений с использованием ИИ, включая дипфейки. Научная новизна проявляется в нескольких аспектах. Автором представлена концептуальная модель и проведена теоретическая классификация. Наиболее удачным видится авторское разграничение «дипфейк-

мошенничества» и «виртуального похищения» (Модели А и Б), анализ их квалификационных сложностей и конкуренции составов. В статье сделан фокус на биометрию. Представлен глубокий анализ связи дипфейков с фальсификацией биометрических данных и угрозами системам аутентификации, что выводит проблему за рамки чисто информационной безопасности в сферу защиты персональных данных и цифровой идентичности. Сформулированы комплексные предложения, а именно: предложена разработка многоуровневой модели правовой защиты (уголовно-правовой, гражданско-правовой, административно-правовой) и конкретных предложений по совершенствованию законодательства (введение спецсостава/квалифицирующего признака, регулирование «синтетического биометрического образа»), методики доказывания, статистического учета и технологических мер (маркировка, устойчивая аутентификация). При формулировании предложений автором соблюден баланс интересов. Указанное проявилось в рассмотрении проблемы допустимого использования (культура, образование, правоохранительная деятельность) и предложениях по сохранению баланса со свободой выражения мнения (исключения для сатиры, пародии, науки).

Стиль, структура, содержание соответствуют предъявляемым требованиям. Стиль в целом соответствует научному. Текст информативен, насыщен терминологией. Однако встречаются отдельные стилистические шероховатости и канцеляризмы (например, «имеет место быть», «предопределяет необходимость их анализа», некоторые громоздкие предложения). Требуется внимательная редакторская правка для большей ясности и лаконичности. Структура работы логична и обоснована. Последовательно раскрыты постановка проблемы, методология, технологическая основа, риски, классификация преступлений, анализ правового регулирования и практики, зарубежный опыт, предложения. Отсутствие явного введения и заключения (с четко сформулированными выводами) несколько снижает удобство читательского восприятия. Содержание глубокое и всестороннее. Автор демонстрирует хорошее знание предмета, привлекает актуальные примеры и источники. Сильной стороной является междисциплинарный охват (право, криминалистика, ИТ). Содержание теста полностью соответствует заявленному названию статьи. Список литературы обширный (15 источников) и в основном релевантен теме исследования. Преобладают современные публикации (2022-2025 гг.), что соответствует требованию. Указаны ведущие российские юридические журналы («Журнал российского права», «Закон», «Актуальные проблемы российского права», Вестники университетов). Приведенные DOI и EDN позволяют проверить наличие публикаций в научных базах (eLibrary, КиберЛенинка). В списке преобладают российские источники. Включение большего числа актуальных зарубежных исследований (особенно по регулированию и технологиям обнаружения) усилило бы сравнительно-правовую часть. Апелляция к оппонентам присутствует, но косвенно. Автор неявно полемизирует с возможными возражениями. Относительно возможного возражения о достаточности существующих норм автором указываются в статье квалификационные сложности, «вынужденность» совокупности составов, пробелы в описании ОСО (особенно для Модели Б), необходимость спецсостава/квалифицирующего признака для учета специфической опасности. Относительно риска чрезмерного регулирования предлагаются меры для баланса – законодательные исключения (сатира, пародия, образование, наука), критерии общественного интереса, тест «наименее ограничительного вмешательства», судебный контроль. Это коррелируется с позициями, высказываемыми, например, Калятиным В.О. в его работах о цифровых правах. В части технологической детерминированности автор избегает технологического алармизма, фокусируясь на правовых и криминалистических механизмах реагирования, подчеркивая, что способ совершения (ИИ) не должен автоматически менять

юридическую природу преступления или быть само по себе отягчающим обстоятельством без учета иных факторов.

В целом, статья содержит ценные выводы о необходимости комплексного подхода к регулированию дипфейков, включая совершенствование УК РФ (спецсостав/квалифицирующий признак), законодательства о персональных и биометрических данных, методик доказывания, статистического учета и внедрения технологий обнаружения. Ключевой вывод – важность баланса между защитой прав и свободным развитием технологий. Статья представляет интерес для широкой юридической аудитории: ученых (уголовное право, криминология, криминалистика, информационное право), практиков (следователи, дознаватели, прокуроры, судьи, адвокаты), законодательных органов власти, специалистов по информационной безопасности и защите персональных данных. Публикация в журнале «Полицейская и следственная деятельность» является целесообразной, так как тема напрямую касается практики правоохранительных органов. Таким образом, статья «Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий» представляет собой серьезное, актуальное и научно ценное исследование, вносящее существенный вклад в изучение сложной и динамично развивающейся проблемы. Автор демонстрирует глубокое понимание предмета, применяет адекватную методологию и предлагает комплекс обоснованных мер по совершенствованию законодательства и правоприменительной практики. Междисциплинарный подход и привлечение актуальных источников усиливают работу. Статья рекомендуется к опубликованию в журнале «Полицейская и следственная деятельность».