Дата поступления рукописи в редакцию: 10.07.2026 г. DOI: 10.24412/2224-9133-2026-8-242-250
Дата принятия рукописи в печать: 01.09.2026 г.

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

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ДИПФЕЙК-ТЕХНОЛОГИЙ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ КВАЛИФИКАЦИИ И НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА

Аннотация. *Статья посвящена уголовно-правовой оценке мошенничества, совершаемого с применением генеративного искусственного интеллекта, включая технологии синтеза голоса, изображения и видео конкретного лица. Цель исследования состоит в определении места дипфейка в механизме мошеннического обмана, разграничении составов, предусмотренных статьями 159, 159.3, 159.6 и 187 УК РФ, а также в разработке предложений по обеспечению единообразной квалификации. Методологическую основу составили формально-юридический, системно-структурный, сравнительно-правовой и моделирующий методы. Обосновано, что дипфейк не образует самостоятельного способа хищения, а выступает высокотехнологичной формой сообщения ложных сведений о личности, полномочиях, воле либо фактическом положении мнимого коммуникатора. Квалификация по статье 159.6 УК РФ допустима только при наличии предусмотренного ею воздействия на компьютерную информацию или функционирование средств ее обработки; одно лишь использование нейросети или мессенджера такого основания не создает. Рассмотрены критерии отграничения мошенничества от кражи с банковского счета и неправомерного оборота средств платежей. Предложено дополнить разъяснения Пленума Верховного Суда РФ положениями о синтетическом медиаконтенте, а после накопления репрезентативной практики — предусмотреть квалифицирующий признак использования искусственного интеллекта для достоверной имитации личности другого лица.*

Ключевые слова: *мошенничество; дипфейк; искусственный интеллект; обман; социальная инженерия; электронное средство платежа; дроппер; квалификация преступлений.*

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

FRAUD USING DEEPFAKE TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE: CRIMINAL-LAW CLASSIFICATION AND DIRECTIONS FOR LEGISLATIVE DEVELOPMENT

Annotation. *The article examines the criminal-law assessment of fraud committed through generative artificial intelligence, including technologies that synthesize the voice, image, and video of a particular person. The study aims to determine the role of deepfakes in fraudulent deception, distinguish the offences under Articles 159, 159.3, 159.6, and 187 of the Criminal Code of the Russian Federation, and formulate proposals for consistent legal classification. The research relies on formal legal, systemic, comparative, and legal modelling methods. It is argued that a deepfake does not constitute an autonomous method of theft; rather, it is*

a technologically enhanced form of communicating false information about the identity, authority, intention, or factual situation of an apparent communicator. Article 159.6 may be applied only where the conduct involves the legally specified manipulation of computer information or interference with information-processing systems; the mere use of a neural network, messenger, or digital platform is insufficient. The paper develops criteria for separating deepfake fraud from theft from a bank account and unlawful circulation of payment instruments. It proposes Supreme Court guidance on synthetic media and, after sufficient empirical practice has accumulated, a qualifying circumstance for the use of artificial intelligence to convincingly impersonate another person.

Key words: *fraud; deepfake; artificial intelligence; deception; social engineering; electronic payment instrument; money mule; criminal classification.*

Введение

Цифровая трансформация мошенничества выражается не только в переносе традиционных схем в дистанционную среду, но и в изменении качества самого обмана. Генеративные модели позволяют автоматизировать подготовку легенды, анализировать открытые данные о потерпевшем, воспроизводить голос близкого человека или руководителя, создавать реалистичное видеосообщение и поддерживать длительный персонализированный диалог. В результате ложная информация приобретает внешние признаки подлинной коммуникации, а классический психологический прием социальной инженерии соединяется с технологией синтетического воспроизведения личности.

Актуальность проблемы подтверждается устойчиво высоким уровнем финансовых хищений. По данным Банка России, в 2025 г. кредитные организации предотвратили 134,2 млн мошеннических операций, однако объем фактически похищенных средств достиг 29,3 млрд руб., а количество успешных операций увеличилось на 31,2 % [5]. Эти показатели не отражают исключительно дипфейк-мошенничество, но демонстрируют масштаб среды, в которой синтетический контент становится усилителем уже действующих преступных моделей. Одновременно законодатель сформировал комплекс превентивных механизмов: Федеральный закон от 1 апреля 2025 г. № 41-ФЗ предусмотрел государственную информационную систему противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий [3], а Федеральный закон от 24 июня 2025 г. № 176-ФЗ существенно расширил статью 187 УК РФ, установив специальные основания ответственности за дропперскую деятельность [4].

Научная дискуссия развивается по двум основным направлениям. Представители первого предлагают специальную криминализацию изготовления либо применения дипфейков в преступных целях [9; 10]. Сторонники второго рассматривают синтетический медиаконтент преимущественно как средство или способ совершения уже предусмотренных преступлений, полагая, что действующие составы способны охватить причиненный вред при условии корректного толкования [7; 13]. Обе позиции отражают реальные риски: чрезмерно ранняя криминализация может нарушить принципы правовой определенности и экономии уголовной репрессии, тогда как отказ от адаптации законодательства способен привести к недооценке повышенной опасности масштабируемого и персонализированного обмана.

Цель настоящей статьи — сформировать уголовно-правовую модель квалификации мошенничества, в котором генеративный искусственный интеллект используется для имитации личности и побуждения потерпевшего к имущественному распоряжению. Для достижения цели необходимо: определить юридическую природу дипфейка как элемента обмана; разграничить общую и специальные нормы о мошенничестве; установить пределы применения статьи 187 УК РФ к участникам платежной инфраструктуры; исследовать значение синтетического контента для стадий преступления и соучастия; предложить направления совершенствования судебного толкования и уголовного закона.

1. Дипфейк как форма мошеннического обмана

В соответствии с частью 1 статьи 159 УК РФ мошенничество представляет собой хищение чужого имущества или приобретение права на чужое имущество путем обмана либо злоупотребления доверием [1]. Пленум Верховного Суда РФ разъясняет, что ложные сведения могут относиться к любым обстоятельствам, в том числе к личности виновного, его полномочиям и намерениям; умолчание также способно образовывать обман [2, п. 2]. Следовательно, технологический способ формирования ложного сообщения сам по себе не меняет юридическую природу обмана. Дипфейк лишь повышает убедительность недостоверной информации и затрудняет ее критическую проверку.

Для целей уголовно-правового анализа под дипфейком целесообразно понимать синтетический аудио-, визуальный или аудиовизуальный материал, созданный либо существенно преобразованный с использованием алгоритмов искус-

ственного интеллекта и способный сформировать у воспринимающего лица ложное представление о том, что конкретный человек произнес определенные слова, совершил действия или участвовал в коммуникации. Подобное определение должно быть функциональным: решающее значение имеет не архитектура модели, а способность результата имитировать идентичность и участвовать в причинном механизме имущественного распоряжения. В научной литературе справедливо подчеркивается необходимость отделять вредоносный синтетический контент от правомерного художественного, образовательного и технического использования [14].

В механизме мошенничества дипфейк может выполнять по меньшей мере четыре функции. Во-первых, он подтверждает ложную личность коммуникатора: потерпевший видит или слышит родственника, руководителя, представителя банка либо государственного органа. Во-вторых, синтетический материал легитимирует фиктивное полномочие, например поручение о срочном переводе средств. В-третьих, он создает мнимое событие — похищение человека, задержание, аварию, необходимость медицинской помощи. В-четвертых, дипфейк поддерживает длительное заблуждение, последовательно отвечая на вопросы и нейтрализуя сомнения. Во всех вариантах юридически значим не файл как таковой, а ложное представление, которое он вызывает и которое становится причиной передачи имущества или права на него.

Ключевым критерием мошенничества остается добровольно-волевой внешний характер передачи. Потерпевший совершает платеж, сообщает код подтверждения, оформляет кредит, передает наличные курьеру либо подписывает документ, полагая распоряжение соответствующим своим интересам или обязанностям. Его воля сформирована дефектно, но не исключена. Если же обман используется только для получения доступа к счету, а последующее списание осуществляется тайно без нового волевого акта потерпевшего, содеянное может образовывать кражу, а не мошенничество. Пленум Верховного Суда РФ прямо указывает, что обман, не направленный непосредственно на завладение имуществом, а лишь облегчающий доступ к нему, квалифицируется с учетом фактического способа хищения [2, п. 2].

Поэтому типичная схема «видеозвонок руководителя — поручение бухгалтеру — добровольное перечисление» образует мошенничество: ложная имитация полномочий непосредственно обусловила платеж. Напротив, схема «дипфейк родственника — получение от потерпевшего данных карты — самостоятельное тайное списание» требует разграничения. Если потерпевший сам подтверждает конкретный перевод, сохраняется конструкция мошенничества. Если он лишь сообщает реквизиты, а виновный затем без его волевого участия извлекает деньги, более обоснованна квалификация как кражи с банковского счета при наличии предусмотренных законом признаков. Технологическая эффектность первоначального обмана не должна подменять анализ причинной связи между заблуждением и способом изъятия.

2. Основная квалификация и разграничение специальных составов

Базовой нормой для большинства случаев дипфейк-мошенничества является статья 159 УК РФ. Ее применение оправдано, когда синтетический образ воздействует на человека, уполномоченного распоряжаться имуществом, и побуждает его совершить имущественное действие. Предметом могут быть наличные и безналичные деньги, цифровые права, вещи, а также право на имущество. Мошенничество с безналичными денежными средствами признается оконченным с момента их изъятия со счета владельца, в результате которого причинен ущерб [2, п. 5]. Для дипфейк-схем это важно, поскольку последующее дробление, конвертация либо обналичивание средств относится уже к распоряжению похищенным и деятельности соучастников.

Статья 159.3 УК РФ предусматривает мошенничество с использованием электронных средств платежа. Сам факт перевода через банковское приложение не делает норму специальной по отношению к статье 159. Электронное средство платежа должно выступать юридически значимым инструментом совершения преступления, а обстоятельства должны соответствовать конструкции специального состава. Если дипфейк используется для того, чтобы владелец счета самостоятельно инициировал перевод по реквизитам злоумышленника, предметная сторона обмана обычно не сводится к использованию чужого электронного средства платежа виновным; в таких случаях статья 159 сохраняет приоритет. Иное возможно, когда виновный применяет полученное или поддельное средство платежа и вводит в заблуждение лицо, участвующее в расчетной операции.

Статья 159.6 УК РФ также не должна применяться лишь потому, что преступник воспользовался нейросетью, программным обеспечением или сетью Интернет. Объективная сторона компьютерного мошенничества связана с хищением имущества или приобретением права на него посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств ее хранения, обработки или передачи [1]. Создание синтетического голоса и его воспроизведение

потерпевшему не является вмешательством в компьютерную информацию потерпевшего или банка. Здесь программный инструмент производит содержание обмана, но само изъятие обусловлено решением человека. Следовательно, квалификация по статье 159.6 возможна только тогда, когда генеративная технология включена в непосредственный алгоритм воздействия на информационную систему: например, синтетические биометрические данные используются для обхода автоматической идентификации, изменения учетной записи или инициирования операции без волевого решения уполномоченного лица.

Разграничение статей 159 и 159.6 целесообразно проводить по адресату и механизму воздействия. Если ложная информация воспринимается человеком и вызывает имущественное распоряжение, имеет место классический обман. Если же технически сформированный сигнал воздействует на автоматизированную систему, изменяя состояние компьютерной информации либо порядок функционирования системы, речь может идти о компьютерном мошенничестве. Гибридная схема способна образовывать совокупность либо конкуренцию норм, но только при наличии самостоятельных действий и последствий. Нельзя считать любое прохождение цифровой идентификации вмешательством: необходимо доказать предусмотренный законом способ воздействия, а также причинную связь между ним и хищением.

Отдельную проблему представляет использование синтетической биометрии. Голосовая или видеоимитация может быть адресована оператору банка, сотруднику организации либо автоматической системе. В первом случае ложные сведения о личности охватываются общим понятием обмана. Во втором необходим анализ архитектуры идентификации: если система принимает синтетический шаблон как подлинный вследствие обычного выполнения заложенного алгоритма, доктринально возникает вопрос, является ли это «вводом компьютерной информации» или «иным вмешательством». Для соблюдения принципа nullum crimen sine lege расширительное толкование недопустимо. Более устойчивым решением станет специальное разъяснение Пленума Верховного Суда РФ, устанавливающее, при каких условиях представление искусственно сформированных биометрических данных образует способ статьи 159.6 УК РФ.

Необходимо учитывать и совокупность с преступлениями против личности, информационной безопасности и порядка управления. Получение исходных записей путем неправомерного доступа может образовывать самостоятельный состав; незаконное собирание и распространение сведений о частной жизни — статью 137 УК РФ; подделка официального электронного документа — соответствующие нормы о документах. Однако совокупность допустима лишь при наличии самостоятельного объекта и действия, не охватываемого мошенничеством. Само использование внешности или голоса другого лица в обмане, направленном на хищение, не требует автоматического вменения дополнительной нормы. Иначе одно средство преступления искусственно дробится на несколько составов.

3. Субъективная сторона, стадии и соучастие

Мошенничество совершается с прямым умыслом и корыстной целью. В делах о синтетическом контенте доказыванию подлежит осознание виновным ложности создаваемой идентичности, ее назначения для введения конкретного либо неопределенного круга лиц в заблуждение и направленность умысла на безвозмездное обращение имущества. Поскольку многие генеративные сервисы имеют правомерное назначение, факт создания аудио- или видеоматериала не доказывает преступного умысла. Необходима совокупность данных: содержание задания модели, подбор образца голоса, сценарий коммуникации, подготовка платежных реквизитов, распределение ролей, переписка, тестовые звонки и действия по сокрытию следов.

Изготовление дипфейка для последующего хищения может рассматриваться как приготовление, если лицо создает средство совершения преступления, подыскивает потерпевшего и организует инфраструктуру, но еще не приступило к непосредственному введению в заблуждение. Уголовная ответственность за приготовление ограничена тяжкими и особо тяжкими преступлениями, что требует учитывать планируемый размер ущерба и квалифицирующие признаки. Покушение начинается тогда, когда синтетическое сообщение направлено потерпевшему либо используется в коммуникации, непосредственно ориентированной на получение имущества, но передача не состоялась по независящим от виновного обстоятельствам. Массовая рассылка может образовывать множественность покушений, если умысел конкретизирован относительно каждого адресата, либо единое продолжаемое деяние при заранее сформированном общем замысле и однородном механизме.

Особенно сложна оценка разработчиков, операторов моделей, владельцев аккаунтов и лиц, предоставляющих исходные данные. Нейтральное создание программного продукта, предоставление облачной инфраструктуры либо технической консультации не образует соучастия без доказанного умысла на конкретное преступление. Интеллектуальное пособничество возможно, когда специалист осознает мошеннический план и дает советы по обходу проверки, повышению

реалистичности имитации или сокрытию происхождения контента. Физическое пособничество имеет место при предоставлении моделей, аккаунтов, вычислительных ресурсов, баз данных или средств связи, заранее предназначенных для реализации хищения.

Распределение ролей в современной мошеннической группе часто носит платформенный характер: один участник собирает данные, другой генерирует синтетический контент, третий ведет диалог, четвертый принимает денежные средства, пятый конвертирует их в цифровые активы. Для признания организованной группы недостаточно технологической связанности операций; требуется устойчивость, предварительное объединение и общая направленность на совершение преступлений. Вместе с тем цифровая специализация и наличие единой инфраструктуры могут выступать доказательствами устойчивости. Публичное предложение «услуг по озвучке» либо «аренды карты» само по себе не исключает соучастия, если фактический контекст показывает осознание преступного назначения.

При оценке исполнителя следует исходить из теории функционального выполнения объективной стороны. Лицо, которое непосредственно общается с потерпевшим, используя заранее созданный дипфейк, является исполнителем мошенничества. Создатель синтетического образа может быть соисполнителем, если в рамках общего плана его действия составляют необходимую часть единого обмана и охватываются совместным умыслом; в иных случаях — пособником. Автоматизация не превращает модель искусственного интеллекта в субъекта преступления: юридически значимые решения о цели, настройке, запуске и использовании результата принимаются физическими лицами. Ошибка модели может влиять на доказанность умысла и причинной связи, но не порождает самостоятельной «ответственности алгоритма».

4. Дропперы и статья 187 УК РФ в инфраструктуре дипфейк-мошенничества

Федеральный закон от 24 июня 2025 г. № 176-ФЗ дополнил статью 187 УК РФ частями 3–6, установив ответственность за передачу, приобретение и использование электронных средств платежа и доступа к ним для неправомерных операций [4]. Эти изменения принципиально важны для дистанционного мошенничества, поскольку вывод похищенных средств нередко обеспечивается сетью дропперов. Специальная норма позволяет оценивать действия посредника даже тогда, когда доказательств его осведомленности о конкретном эпизоде мошенничества недостаточно, но установлено понимание неправомерного характера платежных операций.

Однако статья 187 УК РФ не должна поглощать соучастие в мошенничестве. Если владелец карты заранее знает о готовящемся хищении, предоставляет реквизиты именно для приема денег потерпевшего, согласует лимиты, порядок обналичивания и размер вознаграждения, его действия охватываются общим умыслом и подлежат квалификации как пособничество либо соисполнительство в мошенничестве — в зависимости от фактической роли. Статья 187 может применяться по совокупности лишь при наличии самостоятельного деяния, выходящего за пределы участия в конкретном хищении. Напротив, когда лицо не осведомлено о способе получения средств и конкретных потерпевших, но сознательно передает доступ для проведения незаконных операций, специальный состав статьи 187 становится основной формой ответственности.

Новая конструкция требует осторожного разграничения умысла и неосторожного вовлечения. Молодой человек, который передает карту под видом легальной работы и не осознает неправомерность операций, не отвечает по уголовному закону при отсутствии доказанного умысла. Формальные предупреждения банка, необычный размер вознаграждения, инструкции скрывать назначение платежей, использование множества карт, быстрое снятие наличных и передача их неизвестным лицам могут подтверждать осознание. Но ни один из этих признаков не должен автоматически заменять доказывание субъективной стороны. Доктрина уже отмечает, что специальные части статьи 187 устранили часть прежней неопределенности, однако нуждаются в единых правоприменительных ориентирах [12].

Для дипфейк-мошенничества типична многоэпизодность: один и тот же счет используется для поступлений от нескольких потерпевших. Вопрос о единичном или множественном преступлении должен решаться с учетом единства умысла, источника средств и характера операций. Если дроппер последовательно обслуживает неопределенное число хищений в рамках постоянной договоренности, возможна оценка совокупности его самостоятельного преступления по статье 187 и соучастия в тех эпизодах мошенничества, осведомленность о которых доказана. Механическое вменение участия во всех переводах только на основании принадлежности счета нарушало бы принцип личной виновной ответственности.

5. Доказывание синтетического характера контента и причинной связи

Квалификация невозможна без надежного установления того, что спорный материал является синтетическим или существенно модифицированным. При этом экспертный вывод должен отвечать не на правовой вопрос о наличии мошенничества, а на технические вопросы: имеются ли признаки генерации, монтажа, клонирования

голоса, подмены лица; каким программным способом создан файл; сохранены ли метаданные; соответствует ли запись исходным образцам. Значение имеют оригинальные файлы, журналы платформ, сведения о времени и устройствах, данные облачных сервисов, история запросов к модели, платежи за вычислительные ресурсы и криптографические контрольные суммы.

Особая проблема — утрата исходного файла при пересылке через мессенджер. Компрессия и повторное кодирование могут уничтожать технические маркеры, поэтому отрицательный вывод эксперта не всегда означает подлинность. Следствию необходимо обеспечивать раннее изъятие устройств, получать серверные данные, фиксировать цепочку хранения и исследовать коммуникацию в совокупности. Авторство дипфейка нельзя выводить исключительно из факта владения компьютером: требуется связь между аккаунтом, заданием модели, исходными материалами и последующим использованием результата.

Причинная связь также имеет самостоятельное значение. Не каждый дипфейк, предъявленный потерпевшему, обусловливает передачу имущества. Потерпевший мог действовать из-за последующего телефонного давления, подложного документа либо угрозы, а синтетическое видео имело лишь фоновую роль. Для состава мошенничества достаточно, чтобы обман был существенным фактором имущественного решения, но суд должен установить, какие именно ложные сведения сформировали заблуждение. Это влияет и на квалификацию соучастников: создатель контента отвечает за хищение лишь тогда, когда его вклад включен в общий умысел и причинный механизм преступления.

Синтетический контент одновременно способен быть доказательством и объектом манипуляции доказательствами. Поэтому процессуальная проверка должна включать не только экспертизу содержания, но и оценку происхождения, целостности, способа получения и воспроизводимости исследования. В научной литературе справедливо предлагается формировать междисциплинарные методики, объединяющие компьютерно-технический, фоноскопический, портретный и лингвистический анализ [8; 13]. Для уголовного права это означает, что новые технологии требуют прежде всего повышения качества доказывания, а не автоматического расширения диспозиций.

6. Направления совершенствования законодательства и судебного толкования

Первым и наиболее оперативным направлением должно стать дополнение постановления Пленума Верховного Суда РФ № 48. В нем целесообразно прямо указать, что обман при мошенничестве может осуществляться посредством искусственно созданного или измененного аудио-, визуального либо аудиовизуального материала, имитирующего личность, голос, изображение, действия или волеизъявление другого лица. Такое разъяснение не создает новый состав, но снимает сомнения относительно охвата технологически сложной формы ложных сведений действующим понятием обмана.

Второе разъяснение должно касаться разграничения статей 159 и 159.6 УК РФ. Предлагается закрепить, что использование программ искусственного интеллекта для подготовки сообщения, воспринимаемого человеком, само по себе не является вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации. Статья 159.6 применяется, когда синтетические данные непосредственно воздействуют на автоматизированную систему в предусмотренной диспозицией форме и это воздействие причинно связано с изъятием имущества. Данный критерий «человек — система» не решает всех пограничных случаев, но обеспечивает понятную исходную модель.

Третье направление связано с оценкой повышенной общественной опасности. Дипфейк способен резко повысить достоверность обмана, масштабировать атаки и использовать биометрическую идентичность потерпевших или третьих лиц. В литературе предложено учитывать его применение в качестве квалифицирующего признака [9], тогда как более осторожная позиция предостерегает от криминализации любого использования информационных технологий [15]. Представляется, что общий признак «с использованием информационно-телекоммуникационных технологий» действительно чрезмерно широк: почти любое современное мошенничество совершается с помощью телефона или сети. Квалифицирующее значение должно иметь не цифровая среда как таковая, а достоверная имитация конкретного человека, существенно снижающая способность адресата распознать ложь.

После накопления репрезентативной судебной практики часть 2 статьи 159 УК РФ может быть дополнена признаком: «с использованием технологии искусственного интеллекта для создания синтетического аудио-, визуального или аудиовизуального образа другого лица в целях достоверной имитации его личности или волеизъявления». Для правовой определенности в примечании либо межотраслевом законодательстве потребуется понятие синтетического медиаконтента. Вместе с тем вводить отдельную статью «дипфейк-мошенничество» нецелесообразно: она дублировала бы общий состав, быстро устаревала технологически и провоцировала конкуренцию норм в зависимости от разновидности модели.

Четвертое направление — согласование уголовно-правовых и превентивных механизмов. Федеральный закон № 41-ФЗ создает инфраструктуру межведомственного обмена данными и блокирования мошеннических коммуникаций [3]. Уголовно-правовая политика должна учитывать результаты этой системы: типовые сценарии, признаки синтетического голоса, цепочки дропперских счетов, повторное использование идентификаторов. Однако автоматизированный риск-профиль не может выступать достаточным доказательством виновности; он служит ориентиром для проверки. Баланс эффективности и презумпции невиновности требует прозрачности происхождения аналитических данных и возможности их процессуального оспаривания.

Пятое направление — развитие правил ответственности профессиональных участников. Провайдер генеративной модели не должен отвечать за каждое противоправное применение универсального инструмента. Уголовная ответственность возможна при намеренном содействии конкретному преступлению, а гражданско-правовые и административные обязанности могут включать маркировку синтетического контента, ведение журналов высокорисковых операций, реагирование на обоснованные запросы и защиту биометрических образцов. Такой многоуровневый подход соответствует выводу о том, что противодействие дипфейкам не сводится к расширению уголовной репрессии и требует технологических, организационных и образовательных мер [11; 14].

Шестое направление касается статьи 187 УК РФ. Пленуму Верховного Суда РФ целесообразно разъяснить соотношение новых частей этой статьи с соучастием в хищениях: осведомленность о конкретном мошенническом эпизоде и заранее обещанное содействие приему либо обналичиванию средств должны оцениваться по правилам соучастия; осознание лишь неправомерного характера операций без знания способа завладения средствами — по статье 187. Необходимо также раскрыть критерии добровольного сообщения и активного способствования, предусмотренные примечанием к статье, чтобы стимулировать выход вовлеченных лиц из преступной инфраструктуры.

Проведенное исследование позволяет сформулировать следующие выводы.

Дипфейк в мошенничестве является не самостоятельным предметом посягательства и не новой формой хищения, а технологически усиленной разновидностью обмана — сообщения ложных сведений о личности, полномочиях, намерениях или фактических обстоятельствах.

Основной нормой для случаев, когда синтетический контент воздействует на человека и побуждает его к имущественному распоряжению, выступает статья 159 УК РФ. Технология создания ложного сообщения не меняет конструкции состава.

Статья 159.6 УК РФ применима не по факту использования нейросети, а только при доказанном вводе, удалении, блокировании, модификации компьютерной информации либо ином вмешательстве в функционирование соответствующих средств, непосредственно обусловившем хищение.

Разграничение мошенничества и кражи с банковского счета зависит от роли заблуждения в изъятии: добровольное подтверждение конкретной операции под влиянием дипфейка указывает на мошенничество; тайное списание после получения данных доступа — на иной способ хищения.

Список литературы:

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. по состоянию на 31 июля 2026 г.) // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

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

[3] О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 1 апреля 2025 г. № 41-ФЗ // Собрание законодательства Российской Федерации. 2025.

[4] О внесении изменений в статью 187 Уголовного кодекса Российской Федерации: Федеральный закон от 24 июня 2025 г. № 176-ФЗ // Официальный интернет-портал правовой информации. URL: https://publication.pravo.gov.ru/document/0001202506240043 (дата обращения: 31.07.2026).

[5] Противодействие кибермошенничеству: статистика хищений и обзор атак на финансовые организации // Банк России: официальный сайт. 13 февраля 2026 г. URL: https://www.cbr.ru/press/event/?id=28300 (дата обращения: 31.07.2026).

[6] Годовой отчет Банка России за 2025 год. М.: Банк России, 2026. URL: https://www.cbr.ru/Collection/Collection/File/59752/ar_2025.pdf (дата обращения: 31.07.2026).

[7] 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..

[8] Палий Е. С. Криминологические и уго-

ловно-правовые аспекты дистанционного мошенничества с применением deepfake-технологий и социальной инженерии // Вестник Санкт-Петербургского университета МВД России. 2025. № 4 (108). С. 149–157.

[9] Ситник В. Н. Перспективы установления уголовной ответственности за преступления, совершенные с использованием технологии дипфейк // Уральский журнал правовых исследований. 2022. № 3. С. 76–83. DOI: 10.34076/2658_512X_2022_3_76..

[10] Белых Е. С., Грабчев М. А. К вопросу о введении уголовной ответственности за изготовление дипфейков в преступных целях // Право и государство: теория и практика. 2024. № 5. С. 372–377. DOI: 10.24412/2224-9133-2024-5-372-377..

[11] Малышева Ю. Ю. Мошеннические проявления фейков и дипфейков: проблемы противодействия // Российско-азиатский правовой журнал. 2025. № 1. DOI: 10.14258/ralj(2025)1.16.

[12] Петрикова С. В., Подтергера Н. С. Уголовно-правовое регулирование ответственности за преступления, совершенные дропперами (посредниками в сфере незаконных финансовых операций) // Проблемы экономики и юридической практики. 2026. № 1. С. 119–126. DOI: 10.33693/2541-8025-2026-22-1-119-126..

[13] Асадов Р. Б. Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий // Полицейская и следственная деятельность. 2025.

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

[15] Зотина Е. В. Уголовно-правовой аспект предупреждения мошенничества с использованием информационно-телекоммуникационных технологий и приемов социальной инженерии // Вестник Казанского юридического института МВД России. 2024. Т. 15. № 3 (57). С. 72–82. DOI: 10.37973/VESTNIKKUI-2024-57-8..

[16] Бодров Н. Ф., Лебедева А. К. Понятие дипфейка в российском праве, классификация дипфейков и вопросы их правового регулирования // Юридические исследования. 2023. № 11.

[17] Зямилева Р. Р., Мартынова А. О., Ситдикова Г. З. Мошенничество с использованием дипфейков: проблемы квалификации по ст. 159 УК РФ и перспективы законодательного регулирования // Экономика и социум. 2026. № 5-2. С. 203–207. DOI: 10.24412/2500-1000-2026-5-2-203-207..

References:

[1] Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (as amended on July 31, 2026) // Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

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

[3] On the creation of a state information system for countering offenses committed using information and communication technologies, and on amending certain legislative acts of the Russian Federation: Federal Law of April 1, 2025 No. 41-FZ // Collection of Legislation of the Russian Federation. 2025.

[4] On Amendments to Article 187 of the Criminal Code of the Russian Federation: Federal Law of June 24, 2025 No. 176-FZ // Official Internet Portal of Legal Information. URL: https://publication.pravo.gov.ru/document/0001202506240043 (access date: 31.07.2026).

[5] Countering cyber fraud: theft statistics and an overview of attacks on financial institutions // Bank of Russia: official website. February 13, 2026 URL: https://www.cbr.ru/press/event/?id=28300 (Accessed 31.07.2026).

[6] Bank of Russia Annual Report 2025. M.: Bank of Russia, 2026. URL: https://www.cbr.ru/Collection/Collection/File/59752/ar_2025.pdf (access date: 31.07.2026).

[7] Dolgieva M. M. Qualification of deepfake fraud and human cyber theft // Actual problems of Russian law. 2024. VOL. 19. № 11. S. 106-113. DOI: 10.17803/1994-1471.2024.168.11.106-113..

[8] Paliy E. S. Criminological and criminal legal aspects of remote fraud using deepfake technologies and social engineering // Bulletin of St. Petersburg University of the Ministry of Internal Affairs of Russia. 2025. № 4 (108). S. 149-157.

[9] Sitnik V.N. Prospects for criminalizing crimes committed using deepfake technology // Ural Journal of Legal Research. 2022. № 3. S. 76-83. DOI: 10.34076/2658_512X_2022_3_76..

[10] Belykh E. S., Grabchev M. A. On the issue of introducing criminal liability for the manufacture of deepfakes for criminal purposes // Law and state: theory and practice. 2024. № 5. PP. 372-377. DOI: 10.24412/2224-9133-2024-5-372-377..

[11] Malysheva Yu. Yu. Fraudulent manifestations of fakes and deepfakes: problems of counteraction // Russian-Asian legal journal. 2025. № 1. DOI: 10.14258/ralj(2025)1.16.

[12] Petrikova S.V., Podtergera N.S. Criminal law regulation of liability for crimes committed by droppers (intermediaries in the field of illegal financial transactions) // Problems of economics and legal practice. 2026. № 1. S. 119-126. DOI: 10.33693/2541-8025-2026-22-1-119-126..

[13] Asadov R. B. Digital mimicry: protection

of individual rights from illegal use of deepfake technologies // Police and investigative activities. 2025.

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

[15] Zotina E. V. Criminal law aspect of fraud prevention using information and telecommunication technologies and social engineering techniques // Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2024. VOL. 15. № 3 (57). S. 72-82. DOI: 10.37973/VESTNIKKUI-2024-57-8..

[16] Bodrov N.F., Lebedeva A.K. The concept of deepfake in Russian law, classification of deepfakes and issues of their legal regulation // Legal research. 2023. № 11.

[17] Zyamileva R.R., Martynova A.O., Sitdikova G.Z. Fraud using deepfakes: qualification problems under Art. 159 of the Criminal Code of the Russian Federation and prospects for legislative regulation // Economy and Society. 2026. № 5-2. S. 203-207. DOI: 10.24412/2500-1000-2026-5-2-203-207..