

Научная статья

УДК 343.721:004.8(470+571)

<https://doi.org/10.35266/2949-3455-2026-3-11>



Уголовно-правовая оценка использования deepfake-технологий при совершении мошенничества

Кристина Александровна Зарубина

Юго-Западный государственный университет, Курск, Россия

Аннотация. Объектом исследования выступают общественные отношения, возникающие в сфере уголовно-правового противодействия мошенничеству, совершаемому с использованием deepfake-технологий.

Целью настоящего исследования является разработка на основе комплексного анализа уголовно-правовой природы мошенничества с использованием deepfake-технологий системы мер противодействия данному виду преступной деятельности.

Задачи исследования: раскрыть сущность deepfake-технологий и определить их уголовно-правовую природу как средства совершения мошенничества; рассмотреть зарубежные модели правового регулирования в указанной сфере и оценить их значимость для российской правовой системы; проанализировать доктринальные подходы к уголовно-правовой оценке использования технологий искусственного интеллекта при совершении мошенничества; сформулировать предложения по модернизации системы мер противодействия мошенничествам, совершаемым с использованием синтетического медиаконтента.

Методология исследования включает совокупность общенаучных и частнонаучных методов познания, в том числе диалектический, формально-юридический методы, методы анализа, обобщения.

Установлено, что использование deepfake-технологий существенно трансформирует способ совершения мошенничества, придавая обману высокую степень визуально-аудиальной достоверности и одновременно повышая латентность таких деяний. Вместе с этим определено, что действующее уголовное законодательство как в России, так и в мире не содержит специальных норм и критериев для их самостоятельной квалификации. В доктринальной науке выявлено наличие разнонаправленных подходов к уголовно-правовой оценке указанного явления при общем преобладании позиции, согласно которой использование синтетического медиаконтента охватывается традиционной конструкцией мошенничества как способа обмана без изменения его юридической природы, но нуждается в квалификационной доработке.

Обоснована необходимость комплексного совершенствования мер противодействия данной разновидности преступной деятельности, включая нормативную конкретизацию признаков использования искусственного интеллекта при мошенничестве, уточнение соответствующих разъяснений Верховного Суда Российской Федерации, внедрение специализированной экспертизы синтетического медиаконтента и усиление профилактических мер.

Ключевые слова: deepfake-технологии, искусственный интеллект, мошенничество, уголовное право, цифровая преступность, синтетический медиаконтент, квалификация преступлений

Финансирование: статья подготовлена в рамках государственного задания на 2026 год № 075-03-2026-489.

Для цитирования: Зарубина К. А. Уголовно-правовая оценка использования deepfake-технологий при совершении мошенничества // Вестник Сургутского государственного университета. 2026. Т. 14, № 3. С. 127–138. <https://doi.org/10.35266/2949-3455-2026-3-11>.

Original article

Criminal evaluation of deepfake technologies use in fraud

Kristina A. Zarubina

Southwest State University, Kursk, Russia

Abstract. The article is devoted to the public relations in criminal law prevention of fraud committed using deepfake technologies.

Comprehensively analyzing the criminal nature of deepfake fraud, the work aims to develop a system of preventive measures against this type of crime.

To achieve the goal, the research addresses the essence of deepfake technology and defines its criminal nature as a tool of fraud. The author investigates foreign models of legal regulation in this field and assesses their applicability to the Russian legal system. The additional study objectives are to analyze doctrinal approaches to the criminal assessment of the artificial intelligence (AI) use in fraud and to propose methods to modernize the system of measures to counter fraud committed using synthetic media content.

The research utilizes general and specific scientific methods of cognition, including dialectical, formal legal approaches as well as analysis and generalization.

It is revealed that the use of deepfake technologies significantly transforms fraud methods, as it simultaneously boosts the audiovisual reliability of the deceptive materials and the dark figure of such crimes. Moreover, the work identifies no special norms and criteria for independent qualification of the subject in the current Russian and global criminal legislation. Predominantly, legislators articulate the use of synthetic media content as a means of deception, i.e. traditional fraud, without changes to its legal nature. Nevertheless, there are multidirectional doctrinal approaches to the criminal legal assessment of this phenomenon, which dictate its required refinement.

The conclusion substantiates the necessity to comprehensively improve the preventive measures against the aforementioned type of crime. This includes legally clarifying the signs of AI use in fraud and the corresponding guidance notes of the Supreme Court of the Russian Federation, while also introducing specialized expertise in synthetic media content and strengthening preventive measures.

Keywords: deepfake technologies, artificial intelligence (AI), fraud, criminal law, digital crime, synthetic media content, qualification of crimes

Funding: the work is prepared within the framework of the State Assignment for 2026 No. 075-03-2026-489.

For citation: Zarubina K. A. Criminal evaluation of deepfake technologies use in fraud. *Surgut State University Journal*. 2026;14(3):127–138. <https://doi.org/10.35266/2949-3455-2026-3-11>.

ВВЕДЕНИЕ

В настоящее время наблюдается повсеместное внедрение технологий искусственного интеллекта в различные сферы общественной жизни, сопровождающееся их интенсивным развитием и усложнением функциональных возможностей. Особое место в данном процессе занимают генеративные технологии, в том числе deepfake-системы, основанные на архитектурах глубокого машинного обучения, обеспечивающие создание синтетического аудио- и видеоконтента, воспроизводящего индивидуальные характеристики конкретных лиц с высокой степенью достоверности.

Между тем указанные технологические решения, изначально ориентированные на легитимные цели, в условиях цифровизации общественных отношений начинают активно использоваться и в противоправной деятельности. Особенно отчетливо данная тенденция проявляется в сфере мошенничества, где в последние годы фиксируется устойчивый рост дистанционных форм хищения, реализуемых посредством телефонных и интернет-коммуникаций. В этих условиях deepfake-технологии становятся эффективным инструментом преступного воздействия, позволяющим имитировать личность другого человека и использовать

сформированный образ в процессе взаимодействия с потерпевшими для достижения корыстных целей, особенно при совершении действий мошеннического характера.

Опасность использования deepfake-технологий в механизме мошенничества обусловлена рядом обстоятельств. Прежде всего они радикально трансформируют саму природу обмана, переводя его на уровень комплексной аудиовизуальной симуляции, воспринимаемой потерпевшим как объективная реальность, что существенно повышает результативность преступного воздействия. Кроме того, применение подобных технологий приводит к размыванию традиционных критериев идентификации личности в цифровой среде, вследствие чего визуальные и аудиальные признаки, ранее служившие основой доверия, утрачивают свою верификационную значимость. Существенным фактором выступает и возможность масштабирования мошеннических посягательств, обусловленная автоматизацией создания синтетического контента и его широким распространением через цифровые каналы связи. И, наконец, данные деяния характеризуются повышенной латентностью и сложностью выявления, что связано как с технологической природой используемых средств, так и с необходимостью применения специальных знаний для их распознавания и доказывания. В совокупности указанные обстоятельства свидетельствуют о формировании качественно новых угроз в сфере уголовно-правовой охраны общественных отношений, что предопределяет необходимость их научного осмысления и обуславливает актуальность настоящего исследования.

МАТЕРИАЛЫ И МЕТОДЫ

Объектом исследования выступают общественные отношения, возникающие в сфере уголовно-правового противодействия мошенничеству, совершаемому с использованием deepfake-технологий.

Целью настоящего исследования является разработка на основе комплексного анализа уголовно-правовой природы мошенничества с использованием deepfake-технологий

системы мер противодействия данному виду преступной деятельности.

Для достижения поставленной цели в работе формулируются и последовательно решаются следующие задачи:

- раскрыть сущность deepfake-технологий и определить их уголовно-правовую природу как средства совершения мошенничества;
- рассмотреть зарубежные модели правового регулирования в указанной сфере и оценить их значимость для российской правовой системы;
- проанализировать доктринальные подходы к уголовно-правовой оценке использования технологий искусственного интеллекта при совершении мошенничества;
- сформулировать предложения по модернизации системы мер противодействия мошенничествам, совершаемым с использованием синтетического медиаконтента.

Методологическую основу исследования составляет совокупность общенаучных и частнонаучных методов познания, обеспечивающих комплексный анализ уголовно-правовой природы использования deepfake-технологий при совершении мошенничества. В качестве базового использован диалектический метод, позволивший рассмотреть исследуемое явление в комплексной взаимосвязи и обусловленности современными процессами цифровизации общественных отношений. Формально-юридический метод использовался при анализе действующего уголовного законодательства Российской Федерации, в частности положений, регламентирующих ответственность за мошенничество, а также при выявлении пробелов и коллизий в правовом регулировании рассматриваемой сферы. Также в работе применялись методы анализа и обобщения, направленные на разработку предложений по совершенствованию уголовно-правовой квалификации деяний, совершаемых с использованием deepfake-технологий. Использование указанных методов в совокупности позволило обеспечить всесторонность, обоснованность и научную достоверность полученных результатов.

РЕЗУЛЬТАТЫ И ИХ ОБСУЖДЕНИЕ

В технологическом аспекте *deepfake* (от англ. *deep learning* «глубинное обучение» и *fake* «подделка») представляет собой совокупность методов синтеза цифрового контента, основанных на алгоритмах машинного обучения, прежде всего генеративно-сопоставительных нейросетевых моделях. Указанные алгоритмы, активно используемые мировым сообществом с 2017 г., позволяют создавать изображения, аудио- и видеозаписи, воспроизводящие индивидуализирующие признаки конкретного лица (внешность, мимику, голосовые характеристики и поведенческие паттерны) с высокой степенью достоверности. В результате формируется синтетический медиаконтент, воспринимаемый адресатом как аутентичное отражение действительности [1]. Как справедливо отмечают R. Chesney и D. Citron, *deepfake* формирует качественно новый тип информационного воздействия, при котором граница между реальным и искусственно сконструированным контентом становится трудноразличимой [2].

В зависимости от формы реализации данных технологий принято выделять несколько разновидностей *deepfake*-контента, различающихся по каналу воздействия на воспринимающее лицо. Наиболее распространенными являются видеодипфейки, основанные на подмене визуального образа человека в видеоматериале, а также аудиодипфейки, позволяющие синтезировать голос конкретного лица с учетом его индивидуальных характеристик. Особую опасность представляют комбинированные формы, интегрирующие аудио- и видеосинтез, что обеспечивает многоканальное воздействие на восприятие и усиливает эффект достоверности. Такие технологические особенности предопределяют высокий криминогенный потенциал *deepfake*, который находит свое проявление в различных формах противоправной деятельности. Причем наиболее активно данные технологии используются в сфере мошенничества, где они выполняют функцию средства имитации личности, позволяя злоумышленнику выстраивать коммуникацию с потерпевшим от имени другого лица. В этой связи *deepfake* следует рассма-

тривать как высокотехнологичное средство совершения мошенничества, обладающее повышенной степенью убедительности и способное усиливать общественную опасность деяния, ввиду чего особую значимость приобретает уголовно-правовая оценка такого рода общественно опасной деятельности.

В зарубежных правовых системах регулирование использования *deepfake*-технологий формируется фрагментарно и носит разнородный характер, что обусловлено как различиями в самих правовых системах, так и темпами развития цифровых технологий, опережающими законодательную реакцию. Вместе с тем уже сформировались отдельные модели правового воздействия, реализуемые в США, Европейском союзе и Китайской Народной Республике.

Так, в Соединенных Штатах Америки регулирование *deepfake*-технологий характеризуется отсутствием единого федерального закона, устанавливающего комплексный правовой режим синтетического медиаконтента. Вместе с тем предпринимаются попытки точечного нормативного вмешательства, направленного на пресечение наиболее общественно опасных форм использования *deepfake*. Например, *Take It Down Act* от 19 мая 2025 г. устанавливает уголовную ответственность за недобровольное распространение интимных изображений, включая созданные с использованием искусственного интеллекта, а также вводит обязательства для онлайн-платформ по оперативному удалению такого контента [3]. На уровне штатов также были приняты соответствующие нормативные правовые акты. В частности, законодательство отдельных штатов предусматривает как гражданско-правовые, так и уголовно-правовые меры ответственности за создание и распространение синтетического контента без согласия лица, чьи признаки используются [4]. В результате американская модель характеризуется децентрализованным и казуистическим подходом, ориентированным на защиту конкретных охраняемых интересов, но не формирующим единой уголовно-правовой конструкции противодействия *deepfake*-мошенничеству.

В праве Европейского союза, напротив, наблюдается стремление к формированию системного регулирования, основанного на сочетании нескольких нормативных инструментов. Ключевую роль играет Регламент Европейского союза об искусственном интеллекте (Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations), который вводит требования прозрачности в отношении систем, генерирующих или модифицирующих контент, включая обязательства по маркировке deepfake-материалов и информированию пользователей об их искусственном происхождении [5]. Параллельно действует Общий регламент защиты персональных данных Европейского союза от 25 мая 2018 г., предусматривающий возможность привлечения к ответственности за обработку персональных данных, включая создание синтетического контента, нарушающего права субъектов данных. В частности, ст. 82 данного акта закрепляет право на компенсацию материального и нематериального вреда, включая ущерб, причиненный мошенничеством или злоупотреблением идентичностью [6]. Также важное значение имеет Закон о цифровых услугах Европейского союза (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)), устанавливающий обязанности онлайн-платформ по выявлению и удалению незаконного контента, к которому могут относиться и deepfake-материалы, используемые в мошеннических схемах [7].

Как видим, европейская правовая модель характеризуется комплексным и риск-ориентированным подходом к регулированию использования deepfake-технологий, в рамках которого акцент смещается с последующего уголовно-правового реагирования на превентивное воздействие, обеспечиваемое через механизмы прозрачности, подотчетности и контроля за оборотом синтетического контента. Вместе с тем указанные нормативные

инструменты носят преимущественно рамочный и регулятивный характер, также не формируя самостоятельной уголовно-правовой конструкции оценки использования deepfake-технологий в мошеннических целях.

Китайская Народная Республика, в свою очередь, демонстрирует наиболее жесткий и централизованный подход к регулированию использования deepfake-технологий, основанный на административно-правовом контроле и превентивных мерах. Так, в 2023 г. в Китайской Народной Республике вступили в силу Положения об управлении технологиями глубокой синтетики (Administrative Provisions on Deep Synthesis), устанавливающие обязательства для разработчиков и пользователей технологий по идентификации, регистрации и маркировке синтетического контента, а также запрет на его использование в целях, нарушающих общественные интересы [8]. Дальнейшее развитие нормативный массив получил в виде Директивы о маркировке материалов, созданных или составленных с помощью искусственного интеллекта (ИИ) (2025 г.), предусматривающих обязательное наличие обозначений искусственного происхождения медиаматериалов [9]. Указанные меры направлены на отслеживание цифрового контента и снижение рисков его противоправного использования. Вследствие этого, как справедливо отмечается в научной литературе, китайская правовая модель отличается высокой степенью институционализации и ориентацией на превентивный контроль за оборотом синтетического медиаконтента, что позволяет рассматривать ее как элемент общей стратегии цифрового суверенитета и технологического надзора. При этом акцент делается на предупреждении рисков на стадии создания и распространения цифрового контента, а не на последующем реагировании на уже совершенные правонарушения [10]. В результате опыт китайского правового регулирования демонстрирует сочетание обязательной маркировки подобного контента, административный контроль и его отслеживаемость. И в контексте противодействия мошенничеству данный опыт представляет

особый интерес, поскольку позволяет минимизировать возможность использования синтетических материалов для имитации личности и введения потерпевших в заблуждение уже на ранних стадиях их оборота.

В целом проведенный сравнительно-правовой анализ позволяет констатировать следующее. В американской системе преобладает фрагментарное и казуистическое нормотворчество, ориентированное преимущественно на защиту отдельных охраняемых интересов и последующее реагирование на уже совершенные нарушения. Европейский союз, напротив, формирует риск-ориентированную регулятивную модель, в рамках которой акцент смещается на превентивные механизмы контроля, прозрачность и подотчетность оборота синтетического медиаконтента. Китайская Народная Республика реализует наиболее жесткий административно-контрольный подход, основанный на обязательной идентификации, маркировке цифрового контента на всех стадиях его «жизненного цикла». При этом, несмотря на различия в степени нормативной регламентации, общей чертой рассматриваемых правовых порядков является признание повышенной общественной опасности использования синтетического медиаконтента в противоправных целях, включая мошенничество, основанное на имитации личности и введении потерпевшего в заблуждение посредством цифровых технологий. Вместе с тем ни одна из рассмотренных моделей не формирует целостной уголовно-правовой конструкции квалификации мошеннических посягательств с использованием deepfake-технологий, что обуславливает сохранение значительного пробела. Аналогичная ситуация наблюдается и в российском уголовном законодательстве, где действующий Уголовный кодекс Российской Федерации (УК РФ) не содержит специальных норм, прямо регламентирующих ответственность за использование deepfake-технологий при совершении мошенничества, вследствие чего соответствующие деяния квалифицируются в рамках общей конструкции обмана. Указанное обстоятельство предопределяет необходимость

обращения к научной доктрине с целью выявления и систематизации существующих подходов к уголовно-правовой оценке данного феномена, а также определения возможных направлений его нормативного и правоприменительного осмысления.

В свою очередь, в современной отечественной научной литературе формируются несколько устойчивых доктринальных подходов к оценке использования deepfake-технологий при совершении действий мошеннического характера. Первый подход можно обозначить как уголовно-охранительный (традиционалистский), в рамках которого deepfake рассматривается исключительно как новое техническое средство совершения уже известных преступлений. Представители данного направления исходят из того, что использование синтетического медиаконтента не требует конструирования новых составов преступлений, поскольку существующие нормы уголовного закона, включая ст. 159 УК РФ, в полной мере охватывают случаи цифрового обмана при условии правильной квалификации способа совершения преступления [11]. Иной подход в доктрине может быть обозначен как технологически-детерминированный. Его сторонники указывают на то, что развитие генеративных нейросетевых технологий приводит к качественному изменению природы обмана, поскольку воздействие на потерпевшего осуществляется уже не через сообщение ложных сведений, а через создание полной аудиовизуальной симуляции личности. В рамках данного подхода подчеркивается, что deepfake формирует новый тип общественно опасного поведения, который потенциально требует либо модификации существующих составов преступлений, либо введения специальных квалифицирующих признаков, учитывающих цифровую природу обмана [12, 13].

Вместе с тем решение проблемы квалификации данных деяний видится в разных направлениях. Так, например, некоторые исследователи полагают, что необходимо введение в уголовное законодательство новых составов преступлений (например, «Создание вредоносной системы ИИ» [14] или «Незаконное

создание и (или) распространение синтетических аудиовизуальных материалов, способных вводить в заблуждение и причинять вред охраняемым законом интересам» [15]). Другие указывают на необходимость введения не новых составов преступлений, а уточнения квалифицирующих признаков в рамках действующих норм уголовного закона (например, введение данного квалифицирующего признака в ст. 159, 159.3, 159.6 УК РФ с дополнением перечня отягчающих обстоятельств в ст. 63 УК РФ признаком – «совершение преступления с использованием технологий искусственного интеллекта») [16]. И, наконец, отдельные исследователи полагают, что наиболее действенным способом является не нормативная переработка норм уголовного законодательства, а дача соответствующих разъяснений высшей судебной инстанцией (Пленумом Верховного Суда Российской Федерации), например в постановлении от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [17]. При этом отдельно укажем, что в отечественной правоприменительной практике приоритетным остается первый, традиционалистский подход, где мошенничество с использованием deepfake-технологий охватывается ст. 159 УК РФ, поскольку синтетический контент квалифицируется как способ обмана, не изменяющий конструкцию состава преступления [18]. При этом обращает на себя внимание, что в сложившейся правоприменительной практике использование deepfake-технологий, как справедливо отмечают некоторые современные исследователи, фактически не получает самостоятельной уголовно-правовой квалификации и, как правило, не находит прямого отражения в формулировках судебных актов. В результате суды и следственные органы, сталкиваясь с подобными способами совершения преступления, описывают их через традиционные категории: «введение в заблуждение», «представление иным лицом», «использование средств связи» и т. п., не прибегая к фиксации самого феномена синтетической генерации контента. Тем самым технологическая специфика

деяния оказывается нивелированной на уровне юридической оценки, а deepfake, по сути, «растворяется» в классической конструкции обмана [19]. В результате правоприменитель фактически фиксирует последствия и внешние проявления обмана, не отражая в достаточной мере его технологическую природу, что затрудняет формирование единообразной практики и адекватную оценку повышенной общественной опасности таких деяний. Считаем, что подобная ситуация обусловлена, с одной стороны, отсутствием легального определения и закреплённого понятийного аппарата, позволяющего однозначно идентифицировать и описывать использование синтетического медиаконтента, а с другой – некоторой инерционностью правоприменительной практики, ориентированной на уже устоявшиеся квалификационные модели.

В связи с этим в качестве конкретных мер противодействия мошенничеству с использованием deepfake-технологий, с учетом проведенного анализа научной литературы и зарубежного опыта правового регулирования, предлагаем следующее.

Прежде всего, соглашаясь с мнением ряда исследователей о необходимости модернизации отечественного уголовного законодательства в заданном направлении [12, 16, 17], укажем на целесообразность внесения изменения в ст. 159 УК РФ, дополнив ее квалифицирующей частью следующего содержания: «Мошенничество, совершенное с использованием искусственно созданных или модифицированных с применением технологий искусственного интеллекта аудиовизуальных либо аудиолингвистических образов личности». Представленное дополнение обусловлено тем, что использование deepfake-технологий принципиально изменяет способ обмана, где воздействие на потерпевшего осуществляется не через традиционное сообщение ложных сведений, а через создание высокореалистичной цифровой симуляции личности, обладающей эффектом «псевдореального присутствия».

Одновременно представляется необходимым закрепить в примечании к ст. 159 УК РФ легальное определение deepfake-технологий

в следующей формулировке: «Под использованием искусственно созданных или модифицированных аудиовизуальных либо аудиолингвистических образов личности понимается создание либо модификация с применением технологий искусственного интеллекта цифрового контента, имитирующего внешность, голос или поведение конкретного лица без его согласия, используемого для введения в заблуждение и хищения имущества». Представленное определение необходимо для устранения правовой неопределенности, поскольку в настоящее время отсутствуют единые критерии разграничения между допустимым использованием генеративных технологий (например, в медиа- или творческой сфере) и их уголовно наказуемым применением. Считаем, что подобное законодательное закрепление понятия позволит правоприменителю однозначно идентифицировать случаи использования *deepfake*-технологий именно как способа обмана в структуре мошенничества.

Кроме того, для повышения эффективности противодействия уголовно-правовыми мерами такого рода преступной деятельности существенное значение имеет развитие судебного толкования. В этой связи предлагается внесение соответствующих изменений в Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (с изм. и доп.) «О судебной практике по делам о мошенничестве, присвоении и растрате» [20]. В частности, считаем необходимым дополнить его разъяснением о том, что использование *deepfake*-технологий признается формой обмана независимо от канала коммуникации (мессенджеры, социальные сети, телефонная связь и иные цифровые платформы). Это обеспечит единообразие квалификации независимо от формы цифрового взаимодействия между виновным и потерпевшим. Отдельно необходимо закрепить положение о том, что момент окончания преступления определяется фактом завладения имуществом или приобретения права на него, а не моментом создания или использования синтетического контента. Это позволит устранить ошибки квалификации, когда действия на стадии генерации

соответствующего контента ошибочно рассматриваются как оконченное преступление. Также находим важным указать критерии разграничения ст. 159 УК РФ и смежных составов преступлений, что позволит устранить конкуренцию норм, возникающую в случаях, когда использование *deepfake*-технологий одновременно затрагивает сферу персональных данных и информационной безопасности. Указание на приоритет ст. 159 УК РФ при наличии цели хищения имущества обеспечит единообразное понимание квалификации, тогда как ст. 137, 272 и 273 УК РФ будут применяться только при наличии самостоятельного объекта посяательства, не поглощаемого мошенничеством. С позиции теории квалификации преступлений ст. 137, 272 и 273 УК РФ могут «поглощаться» ст. 159 УК РФ в случаях, когда нарушение неприкосновенности частной жизни, неправомерный доступ к компьютерной информации или использование вредоносных программ выступают лишь способом совершения мошенничества и полностью охватываются единым умыслом на хищение имущества. В такой ситуации имеет место конкуренция части и целого, при которой дополнительная квалификация не требуется. Однако самостоятельное применение указанных норм необходимо, если соответствующие действия причиняют дополнительный вред самостоятельному объекту уголовно-правовой охраны либо преследуют отдельную преступную цель.

В свою очередь, в целях повышения эффективности расследования преступлений, совершаемых с использованием технологий цифровой симуляции личности, представляется целесообразным нормативное закрепление самостоятельного вида судебной экспертизы – экспертизы синтетического медиаконтента. В частности, соответствующие изменения могут быть внесены в Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» (с изм. и доп.) [21] посредством дополнения положений о видах судебных экспертиз указанием на экспертизу синтетического медиаконтента как

на самостоятельный род экспертного исследования. Одновременно требуется внесение изменений в ведомственные нормативные акты Министерства юстиции Российской Федерации, в том числе в приказы, регламентирующие номенклатуру родов и видов судебных экспертиз, с целью включения данного направления в систему государственных экспертных учреждений, например в приказ Минюста России от 20.04.2023 № 72 (ред. от 31.01.2024) «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России» [22]. Необходимость такого нормативного закрепления обусловлена тем, что традиционные виды компьютерно-технических и фонографических экспертиз не в полной мере учитывают специфику объектов, создаваемых с применением технологий искусственного интеллекта, и, как следствие, не всегда позволяют достоверно установить факт их нейросетевой генерации или модификации. Введение специализированного экспертного исследования, в свою очередь, позволит выработать унифицированные методики выявления признаков синтетического происхождения аудиовизуальных материалов, включая анализ характерных фактов генерации, несоответствий поведенческих и мимических параметров, а также особенностей акустической структуры речи. Кроме того, такая экспертиза может быть направлена на установление используемых технологических решений и инструментов создания контента, что имеет существенное значение для определения способа совершения преступления, реконструкции механизма противоправного деяния и установления круга причастных лиц.

Наконец, в профилактическом аспекте представляется целесообразным развитие системной превентивной работы среди населения, направленной на формирование устойчивых

навыков распознавания мошеннических посягательств, совершаемых с использованием технологий искусственного интеллекта, в том числе deepfake. Особое внимание при этом должно уделяться социально уязвимым категориям граждан (лицам пожилого возраста, несовершеннолетним, а также лицам с низким уровнем цифровой грамотности), которые в наибольшей степени подвержены воздействию подобных преступных схем. В этой связи обоснованным является внедрение практико-ориентированных форм профилактики, включающих проведение обучающих семинаров, интерактивных тренингов и моделируемых ситуаций («практикумов»), в рамках которых участникам демонстрируются типичные сценарии мошенничества с использованием синтетического аудио- и видеоконтента, а также вырабатываются алгоритмы безопасного поведения при получении подозрительных сообщений или звонков. Организационно указанная деятельность может быть реализована посредством взаимодействия правоохранительных органов, образовательных учреждений, кредитных организаций и операторов цифровых платформ, с последующей разработкой методических рекомендаций и информационных материалов. Такая форма профилактического воздействия позволяет не только повысить уровень осведомленности населения о новых способах совершения мошенничества, но и сформировать практические навыки критической оценки цифровой информации, что в условиях распространения deepfake-технологий приобретает особое значение для снижения виктимности и предупреждения преступлений.

ЗАКЛЮЧЕНИЕ

Таким образом, следует констатировать, что использование deepfake-технологий при совершении мошенничества отражает качественно новый этап трансформации такого рода преступной деятельности, обусловленный цифровизацией общественных отношений и активным развитием генеративных систем искусственного интеллекта. Синтетическая симуляция личности не только

интенсифицирует традиционные механизмы обмана, но и модифицирует их сущностную природу, переводя преступное воздействие в плоскость комплексной аудиовизуальной перцепции, воспринимаемой как достоверная реальность. Указанные обстоятельства свидетельствуют о формировании принципиально новых криминологических и уголовно-правовых вызовов, связанных с эрозией традиционных механизмов идентификации личности и трансформацией структуры обманного воздействия, что, в свою очередь, обуславливает необходимость адекватного переосмысления существующих подходов к квалификации и противодействию подобного рода деяниям. В связи с этим представляется важным совершенствование системы противодействия такого рода преступной активности, в том

числе посредством нормативной конкретизации признаков использования технологий искусственного интеллекта при совершении мошенничества, развития судебного толкования в заданном направлении, институционализации специализированных механизмов доказывания (включая внедрение экспертизы синтетического медиаконтента), а также модернизации соответствующих превентивных мер. При этом следует подчеркнуть, что обозначенные предложения носят дискуссионный характер и представляют собой авторскую модель решения выявленных проблем, что предопределяет возможность их дальнейшей научной корректировки, переосмысления и адаптации в рамках последующего развития уголовно-правовой доктрины и правоприменительной практики.

Список источников

1. Цыбулевский А. В. Технология *deepfake* как угроза национальной безопасности // *Epomen.Global*. 2024. № 52. С. 121–128.
2. Chesney R., Citron D. K. Deep fakes: A looming challenge for privacy, democracy, and national security. URL: https://scholarship.law.bu.edu/faculty_scholarship/640 (дата обращения: 24.04.2026).
3. S. 146 – Take It Down Act. URL: <https://www.congress.gov/bill/119th-congress/senate-bill/146/text> (дата обращения: 17.04.2026).
4. Deepfake laws: Global regulations in the digital age against sexually explicit and criminal use of deepfakes. URL: <https://www.yoti.com/blog/deepfake-laws/> (дата обращения: 17.04.2026).
5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (дата обращения: 17.04.2026).
6. Общий регламент защиты персональных данных (GDPR) Европейского союза. URL: <https://gdpr-text.com/ru/> (дата обращения 17.04.2026).
7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (дата обращения: 17.04.2026).

References

1. Tsybulevskiy A. V. Deepfake technology as a threat to national security. *Epomen.Global*. 2024;(52):121–128. (In Russ.).
2. Chesney R., Citron D. K. Deep fakes: A looming challenge for privacy, democracy, and national security. URL: https://scholarship.law.bu.edu/faculty_scholarship/640 (accessed: 24.04.2026).
3. S. 146 – Take It Down Act. URL: <https://www.congress.gov/bill/119th-congress/senate-bill/146/text> (accessed: 17.04.2026).
4. Deepfake laws: Global regulations in the digital age against sexually explicit and criminal use of deepfakes. URL: <https://www.yoti.com/blog/deepfake-laws/> (accessed: 17.04.2026).
5. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> (accessed: 17.04.2026).
6. General Data Protection Regulation (EU GDPR). URL: <https://gdpr-text.com/ru/> (accessed: 17.04.2026). (In Russ.).
7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng> (accessed: 17.04.2026).

8. Provisions on the Administration of Deep Synthesis Internet Information Services. URL: <https://www.chinalawtranslate.com/en/deep-synthesis/> (дата обращения: 17.04.2026).
9. Власти Китая выпустили директиву по маркировке созданного искусственным интеллектом онлайн-контента. URL: <https://russian.news.cn/20250315/eb4a7f669a42476f9462e7ed3f5c8042/c.html> (дата обращения: 17.04.2026).
10. Афанасьева Е. Н., Коротнев Р. И., Сунь Ю. Правовое регулирование технологии глубокого синтеза в контексте искусственных интеллектуальных систем: на примере Китая и России // *Baikal Research Journal*. 2023. Т. 14, № 3. С. 1266–1280.
11. Асатов Р. Б. Цифровая мимикрия: защита прав личности от противоправного применения дипфейк-технологий // *Полицейская и следственная деятельность*. 2025. № 4. С. 16–36. <https://doi.org/10.25136/2409-7810.2025.4.75462>.
12. Ситник В. Н. Перспективы установления уголовной ответственности за преступления, совершенные с использованием технологии дипфейк // *Уральский журнал правовых исследований*. 2022. № 3. С. 76–83. https://doi.org/10.34076/2658_512X_2022_3_76.
13. Мочалкина И. С. Криминологическое противодействие экономическим преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий // *Вестник Университета имени О. Е. Кутафина (МГЮА)*. 2025. № 5. С. 189–196. <https://doi.org/10.17803/2311-5998.2025.129.5.189-196>.
14. Яковлева Е. О. ИИ как криминогенный фактор: проблемы квалификации и тактики расследования // *Полицейская и следственная деятельность*. 2025. № 4. С. 268–283. <https://doi.org/10.25136/2409-7810.2025.4.77391>.
15. Пучнин А. В., Миненко П. В. Технологии синтетической дезинформации (deepfake) как один из видов цифрового оружия XXI века // *Вестник Краснодарского университета МВД России*. 2025. № 2. С. 16–22.
16. 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. С. 73–82. <https://doi.org/10.37973/VESTNIKKUI-2024-57-8>.
17. Долгиева М. М. Квалификация дипфейк-мошенничества и киберпохищения человека // *Актуальные проблемы российского права*. 2024. Т. 19, № 11. С. 106–113. <https://doi.org/10.17803/1994-1471.2024.168.11.106-113>.
18. В Приамурье мошенники начали применять технологии Deepfake. URL: <https://portamur.ru/news/detail/v-priamure-moshenniki-nachali-primenyat-tehnologii-deepfake/> (дата обращения: 21.04.2026).
8. Provisions on the Administration of Deep Synthesis Internet Information Services. URL: <https://www.chinalawtranslate.com/en/deep-synthesis/> (accessed: 17.04.2026).
9. Vlasti Kitaya vypustili direktivu po markirovke sozdannogo iskusstvennym intellektom onlayn-kontenta. URL: <https://russian.news.cn/20250315/eb4a7f669a42476f9462e7ed3f5c8042/c.html> (accessed: 17.04.2026). (In Russ.).
10. Afanasyeva E. N., Kortnev R. I., Sun Y. Legal regulation of deep synthesis technology in the context of artificial intelligent systems: The case of China and Russia. *Baikal Research Journal*. 2023;14(3):1266–1280. (In Russ.).
11. Asadov R. B. Digital mimicry: Protecting personal rights from the illegal use of deepfake technologies. *Police and Investigative Activity*. 2025;(4):16–36. <https://doi.org/10.25136/2409-7810.2025.4.75462>. (In Russ.).
12. Sitnik V. N. Prospects for establishing criminal liability for crimes committed using deepfake technology. *Ural Journal of Legal Research*. 2022;(3):76–83. https://doi.org/10.34076/2658_512X_2022_3_76. (In Russ.).
13. Mochalkina I. S. Criminological counteraction to economic crimes committed using information and telecommunication technologies. *Courier of the Kutafin Moscow State Law University (MSAL)*. 2025;(5):189–196. <https://doi.org/10.17803/2311-5998.2025.129.5.189-196>. (In Russ.).
14. Yakovleva E. O. AI as a criminogenic factor: Issues of qualification and investigation tactics. *Police and Investigative Activity*. 2025;(4):268–283. <https://doi.org/10.25136/2409-7810.2025.4.77391>. (In Russ.).
15. Puchnin A. V., Minenko P. V. Synthetic disinformation technologies (deepfake) as one of the types of digital weapons of the 21st century. *Vestnik Krasnodarskogo universiteta MVD Rossii*. 2025;(2):16–22. (In Russ.).
16. Zotina E. V. Criminal aspect of public telecommunications networks crime and social engineering prevention. *Bulletin of the Kazan Law Institute of MIA of Russia*. 2024;15(3):73–82. <https://doi.org/10.37973/VESTNIKKUI-2024-57-8>. (In Russ.).
17. Dolgieva M. M. Classification of deepfake fraud and cyber kidnapping. *Aktual'nye problemy rossijskogo prava*. 2024;19(11):106–113. <https://doi.org/10.17803/1994-1471.2024.168.11.106-113>. (In Russ.).
18. V Priamure moshenniki nachali primenyat tekhnologii Deepfake. URL: <https://portamur.ru/news/detail/v-priamure-moshenniki-nachali-primenyat-tehnologii-deepfake/> (accessed: 21.04.2026). (In Russ.).
19. Mosechkin I. N. Deepfake technologies and biometric data: Directions of criminal legal regulation. *Vestnik of Saint Petersburg University. Law*. 2025;16(1):95–110. <https://doi.org/10.21638/spbu14.2025.107>. (In Russ.).
20. On judicial practice in cases of fraud, misappropriation and misapplication: Resolution of the Plenum

19. Мосечкин И. Н. Дипфейк-технологии и биометрические данные: направления уголовно-правового регулирования // Вестник Санкт-Петербургского университета. Право. 2025. Т. 16, № 1. С. 95–110. <https://doi.org/10.21638/spbu14.2025.107>.
20. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022). Доступ из СПС «КонсультантПлюс».
21. О государственной судебно-экспертной деятельности в Российской Федерации : федеральный закон от 31.05.2001 № 73-ФЗ. Доступ из СПС «КонсультантПлюс».
22. Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым предоставляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России : приказ Минюста России от 20.04.2023 № 72. Доступ из СПС «Гарант».
- of the Supreme Court of the Russian Federation No. 48 of November 30, 2017 (as amended on December 15, 2022). Accessed through Law assistance system “Consultant Plus”. (In Russ.).
21. On State forensic expertise in the Russian Federation: Federal Law No. 73-FZ of May 31, 2001. Accessed through Law assistance system “Consultant Plus”. (In Russ.).
22. On approval of the List of kinds (types) of forensic examinations performed in Federal Budgetary Forensic Expert Institutions of the Ministry of Justice of the Russian Federation and the List of expert specialties for which the right to independently conduct forensic examinations in Federal Budgetary Forensic Expert Institutions of the Ministry of Justice of the Russian Federation is granted: Order of the Ministry of Justice of the Russian Federation No. 72 of April 20, 2023. Accessed through Law assistance system “Garant”. (In Russ.).

Информация об авторе

К. А. Зарубина – кандидат исторических наук, кандидат юридических наук, доцент;
<https://orcid.org/0000-0003-2725-6906>,
kris1996z@mail.ru

About the author

K. A. Zarubina – Candidate of Sciences (History), Candidate of Sciences (Law), Docent;
<https://orcid.org/0000-0003-2725-6906>,
kris1996z@mail.ru