

DOI: 10.17803/1729-5920.2026.237.8.085-095

В. В. Поляков

Алтайский государственный университет
г. Барнаул, Российская Федерация

Применение дипфейк-технологий при совершении высокотехнологичных преступлений

Резюме. Рассмотрен термин «дипфейк», употребляемый в двух смыслах — как дипфейк-технологии и как контент, являющийся результатом применения этих технологий. С криминалистических позиций предложено определение этого понятия. Показано, что дипфейки могут рассматриваться как поддельные характеристики цифрового двойника личности, а используемые для их создания дипфейк-технологии выступают в качестве противоправной подмены характеристик цифрового двойника на искусственно сгенерированный подложный аналог. Недостаточность правового регулирования дипфейк-технологий приводит к широким возможностям для их внедрения в преступную деятельность, особенно при совершении высокотехнологичных преступлений. В связи с этим проанализированы основные тенденции криминального применения дипфейков. Установлено, что дипфейки являются инновационным средством совершения преступлений, архитектура которых представлена комбинацией программной и аппаратной составляющих. Отмечено, что дипфейки применяются не только для непосредственного совершения преступлений, но и для их сокрытия, при этом по своему криминалистическому смыслу они являются инсценировками. С позиций следообразования выделена специфика следов противоправного применения дипфейков: эти следы не отражают реальных событий. В криминалистическом следоведении дипфейки должны рассматриваться как специфический вид подложных электронно-цифровых следов, образуемых при совершении преступлений и противодействии расследованию. Отмечены сложности в уголовном судопроизводстве вследствие применения дипфейков при фальсификации доказательств. Сделан вывод о необходимости разработки практических рекомендаций и технико-криминалистических методов, направленных на обеспечение надежного выявления и исследования дипфейков.

Ключевые слова: информационные технологии; высокотехнологичные преступления; компьютерные преступления; дипфейк; искусственный интеллект; цифровизация; электронно-цифровые следы

Для цитирования: Поляков В. В. Применение дипфейк-технологий при совершении высокотехнологичных преступлений. *Lex russica*. 2026. Т. 79. № 8. С. 85–95. DOI: 10.17803/1729-5920.2026.237.8.085-095

The Use of Deepfake Technologies in High Tech Crimes

Vitaliy V. Polyakov

Altai State University

Barnaul, Russian Federation

Abstract. The concept of «deepfake» is examined in two senses: as deepfake technologies themselves, and as content produced through the application of these technologies. A definition of this concept is proposed from a forensic science perspective. It is shown that deepfake can be considered as falsified characteristics of a person's digital twin, while the deepfake technologies used to create them constitute an illegal substitution of the digital twin's characteristics with an artificially generated fake analogue. The insufficiency of legal regulation of deepfake technologies leads to wide opportunities for their introduction into criminal activities, especially in the commission of high-tech crimes. In this regard, the main trends in the criminal use of deepfake are analyzed. It is concluded that deepfake are an innovative means of committing crimes, the architecture of which is represented

© Поляков В. В., 2026

by a combination of software and hardware components. It is noted that deepfakes are used not only for the direct commission of crimes, but also for their concealment, while in terms of the forensic significance, they amount to staged scenarios. From the standpoint of trace formation, the specific nature of traces resulting from the illegal use of deepfake is highlighted, determined by the fact that these traces do not reflect real events. In forensic investigative science, deepfake should be regarded as a specific type of fake electronic digital traces formed during the commission of crimes and obstruction of investigation. Difficulties in criminal proceedings arising from the use of deepfake in the falsification of evidence are noted. It is concluded that it is necessary to develop practical recommendations and technical and forensic methods aimed at ensuring reliable detection and investigation of deepfake.

Keywords: information technology; high-tech crimes; computer crimes; deepfake; artificial intelligence; digitalization; electronic digital traces

Cite as: Polyakov VV. The Use of Deepfake Technologies in High Tech Crimes. *Lex russica*. 2026;79(8):85-95. (In Russ.). DOI: 10.17803/1729-5920.2026.237.8.085-095

Введение

В настоящее время происходит быстрое развитие информационных технологий, приводящее к цифровизации всех общественных отношений. Негативной стороной этого явления выступает то, что инновационные достижения в области цифровых технологий активно применяются в современной преступной деятельности. К цифровым инновациям в наибольшей степени восприимчивы организованные преступные группы, обладающие необходимыми для этого материально-техническими, финансовыми и кадровыми ресурсами. В первую очередь внедрение цифровых технологий в преступную деятельность наблюдается для динамично развивающейся криминалистической группы высокотехнологичных преступлений. Эта группа преступных деяний характеризуется совершением в групповой форме, с участием специалистов в области информационных технологий, путем применения специально созданных или модифицированных в преступных целях компьютерных средств и удаленного доступа к объектам преступных посягательств по информационно-телекоммуникационным сетям. Одной из последних инноваций, взятых на вооружение организованными преступными группами, являются дипфейк-технологии. Использование дипфейков в преступной деятельности — новая угроза, требующая безотлагательного исследования и практического разрешения.

1. Понятие дипфейк-технологий

Эволюция преступной деятельности в новых условиях цифровой реальности приводит к появлению и быстрому распространению, по выражению А. Н. Савенкова и Е. Р. Россинской, «новых цифровых сущностей»¹. Дипфейки могут рассматриваться как один из примеров этого явления. Понятие «дипфейк» быстро стало предметом исследования различных юридических наук в связи с увеличивающейся потребностью правового противодействия стремительной фейковизации информационной сферы и использованию дипфейков в преступных целях².

Термин «дипфейк» (англ. deepfake, от deep learning — «глубокое обучение» и fake — «подделка») применяется в двух различных смыслах. Во-первых, это дипфейк-технологии, т. е. методы синтеза правдоподобных изображений, видео-, аудиозаписей путем замены исходных данных на поддельные с помощью методов машинного обучения. Можно сказать, что дипфейк-технологии — это математические модели, реализуемые с помощью компьютерных программ и позволяющие массивы данных с реальными голосовыми записями и/или видеоизображениями изменять так, что отличить сгенерированный результат от исходного реального объекта при непосредственном восприятии практически невозможно. Для машинного обучения используются так называемые генеративно-состязательные нейронные

¹ Савенков А. Н., Россинская Е. Р. Вектор развития криминалистической науки в условиях глобальной цифровизации // Государство и право. 2023. № 5. С. 103.

² Правовое противодействие фейковизации информационного пространства : коллективная монография / под ред. Е. С. Аничкина, В. В. Сорокина. Барнаул : Изд-во Алт. ун-та, 2025.

сети³, алгоритмы действия которых позволяют путем обучения на больших наборах данных с исходными изображениями и голосовыми записями генерировать правдоподобный аудио-визуальный контент. Во-вторых, дипфейками называют сам контент, созданный с помощью дипфейк-технологий, т.е. измененные видео-изображения и голосовые записи, причем они представляются совершенно реальными. Сразу отметим, что выявить искусственно сгенерированный дипфейк вполне возможно с помощью специальных компьютерных программ.

Использование дипфейк-технологий само по себе не является преступной деятельностью. Для создания дипфейков существует множество программ, находящихся в свободном доступе, в частности бесплатные DeepFaceLab для операционных систем Windows и Linux, Doublicat для мобильных операционных систем Android и iOS. Исходная информация может быть получена, например, из открытых баз данных в сети Интернет. Широкая доступность соответствующего программного обеспечения с открытым кодом позволяет злоумышленникам свободно создавать и распространять дипфейки в преступных целях⁴.

На сегодняшний день в российском законодательстве понятие и специальное регулирование дипфейк-технологий отсутствуют. Использование дипфейков не запрещено и быстро распространяется в различных сферах общественной жизни. В то же время серьезной проблемой является то, что дипфейки предоставляют широкие возможности для внедрения в преступную деятельность. Например, к сотруднику организации по видеосвязи может обратиться злоумышленник, который благодаря использованию специальной программы выглядит и говорит практически неотличимо от руководителя этой организации. Подобные действия будут получать всё большее распространение, поскольку для их совершения требуется только достаточное количество и качество

записей голоса, фотографий или видеозаписей. Таким образом, применение в преступных целях дипфейк-технологий становится опасным инновационным видом криминальных угроз.

2. Дипфейки с позиций криминалистики

С наиболее общих позиций само возникновение дипфейков явилось одним из следствий цифровизации общественных отношений. С этим процессом Т. Я. Хабриева и Н. Н. Черногор связали формирование в виртуальном пространстве виртуальных личностей, важнейшей характеристикой которых выступают «цифровые данные о реальном человеке, его виртуальном или “цифровом” образе»⁵. Полагаем, что с такой точки зрения созданные в криминальных целях дипфейки могут рассматриваться как подложный аналог виртуальной личности, а использованная для его создания дипфейк-технология — как противоправный, без ведома реальной личности, способ создания такого аналога.

Применение дипфейк-технологий в преступных целях — это сложное и многоаспектное явление. Прежде всего дипфейк, используемый при совершении преступления, выступает как инновационное *средство преступления*. Исходя из классификации средств высокотехнологичных преступлений дипфейк относится к комбинированным средствам⁶, представленным программной и аппаратной архитектурой, а именно сочетанием специализированной компьютерной программы и аппаратного устройства записи и воспроизведения видео- и/или аудиоконтента.

Кроме того, дипфейк может применяться не только для непосредственного совершения преступления, но и для его сокрытия, и прежде всего для сокрытия идентифицирующих признаков преступника⁷. Подобно тому, как в реальном пространстве преступник надевает парик и т.п., чтобы выглядеть как другой человек,

³ Энциклопедия «Касперского» // URL: <https://encyclopedia.kaspersky.ru/glossary/deepfake/> (дата обращения: 20.01.2025).

⁴ Bendiab G., Haïouni H., Moulas I., Shiaele S. Deepfakes in digital media forensics: Generation, AI-based detection and challenges // Journal of Information Security and Applications. 2025. Vol. 88. Art. 103935.

⁵ Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 94.

⁶ Поляков В. В. Криминалистическая классификация средств высокотехнологичных преступлений // Вестник Санкт-Петербургского университета. Право. 2024. Т. 15. Вып. 2. С. 423.

⁷ Белкин Р. С. Курс криминалистики : в 3 т. М. : Юрист, 1997. Т. 3 : Криминалистические средства. Приемы и рекомендации. С. 364.

т.е. осуществляет маскировку, в приведенном примере тот, кто по видеосвязи выдает себя за руководителя, маскирует свои внешность и голос. Другими словами, происходит сокрытие преступника в виртуальном пространстве.

Криминалистическая многоаспектность понятия «дипфейк» означает, что оно может быть исследовано и с иной позиции — следообразования. Дипфейки (записи поддельного голоса, изображения и т.д.), использованные при совершении преступления, будучи зафиксированными, выступают в качестве следов преступления. В отличие от традиционных эти следы представляют собой результат воздействия на исходную компьютерную информацию и, как и сама эта информация, могут быть восприняты человеком только с помощью компьютерных систем. Такие следы, существующие в специфической цифровой форме, являются электронно-цифровыми (в различных работах применяются разные термины: «виртуальные», «цифровые», «информационные» и т.д., что не меняет сути)⁸.

Следы, оставляемые дипфейками, обладают принципиальной спецификой. Во-первых, это весьма «узкий» вид электронно-цифровых следов, отражающий компьютерное представление видеоизображения человека и/или его голоса. Во-вторых, и это главное, если обычные электронно-цифровые следы с записью голоса и видео отражают реальное событие (выступление конкретного человека, факт его нахождения в конкретном месте и т.д.), то дипфейки, рассматриваемые в качестве следов преступления, реальных событий не отражают. Искусственно сгенерированные события существуют только

в виртуальном пространстве (в действительности этот человек такую речь не произносил, в данном месте не находился и т.п.). Использование таких следов с целью искажения реальных обстоятельств и их замены на специально созданные вымышленные, выглядящие как совершенно достоверные, по своему криминалистическому смыслу является инсценировкой⁹. Таким образом, с позиций следообразования дипфейки представляют собой инсценированные электронно-цифровые следы. Их создание и использование выступают способом сокрытия преступников путем инсценировки с целью противодействия расследованию.

Отметим, что стремительное развитие технологий искусственного интеллекта¹⁰ вызвало появление самообучающихся компьютерных программ, в настоящее время еще несовершенных. Однако быстрый прогресс в области создания так называемого сильного искусственного интеллекта, на наш взгляд, может привести к возникновению принципиально нового вида электронно-цифровых следов, сгенерированных самообучающейся компьютерной программой вообще без намерения человека и его участия. Они принципиально отличаются от других видов следов отсутствием какой-либо связи с событиями в окружающей действительности. Нужно признать, что для их исследования, в отличие от поддельных следов, искажающих реальные события, в настоящее время еще не разработана криминалистическая теория, отсутствуют практические методики и сертифицированная криминалистическая техника, которые могли бы использоваться правоохранительными органами.

⁸ См.: Мещеряков В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. 2013. № 5 (10). С. 265–270 ; Вехов В. Б. Понятие и механизм образования электронно-цифровых следов // Использование современных информационных технологий и проблемы информационной безопасности в деятельности правоохранительных органов : межвузовский тематический сборник научных трудов. Калининград : Изд-во Калинингр. ЮИ МВД России, 2009. С. 62–72 ; Осипенко А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс // Научный вестник Омской академии МВД России. 2009. № 4 (35). С. 31–34 ; Семикаленова А. И. Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 5. С. 115–120.

⁹ Поляков В. В. Криминалистическая классификация способов противодействия расследованию высокотехнологичных преступлений // Юридическая наука и правоохранительная практика. 2023. № 1 (63). С. 74.

¹⁰ См.: Бахтеев Д. В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 2 (28). С. 35 ; Поляков В. В. К проблеме использования понятия «искусственный интеллект» в криминалистике // Юрислингвистика. 2022. № 25 (36).

3. Основные тенденции криминального применения дипфейк-технологий

На сегодняшний день с помощью дипфейк-технологий может реализовываться довольно большой круг преступных задач. Прежде всего следует выделить криминальные возможности, возникающие при использовании дипфейков для обхода видео- или голосовой идентификации и аутентификации пользователей посредством информационно-телекоммуникационной сети на различных онлайн-сервисах, т.е. при удаленной проверке подлинности физического лица по его изображению или голосу. Преступники могут копировать и затем нужным образом видоизменять изображения пользователя и записи его голоса, создавая на этой основе подложный контент, и с его помощью осуществлять незаконное воздействие на финансово-хозяйственную деятельность организаций, например по передаче материальных ценностей и проведению финансовых операций. Так, Ю. А. Даниленко описывает пример использования с подобными преступными целями методов машинного обучения, обеспечивающих имитацию голоса¹¹. Предоставление фейковых изображений и голосовых данных может быть направлено на получение неправомерного доступа к конфиденциальной информации физических и юридических лиц, к защищаемым персональным данным, к реквизитам банковских счетов и т.д. При совершении преступлений в сфере компьютерной информации дипфейки могут, в частности, способствовать нарушению правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования информационно-телекоммуникационной сетей, установке вредоносного программного обеспечения, а также неправомерному

сбору компьютерной информации, содержащей персональные данные. При мошенничестве дипфейки позволяют обмануть граждан или злоупотребить их доверием посредством имитации общения с реальными банковскими служащими, сотрудниками правоохранительных органов, руководителями организаций и иными доверенными лицами.

По мнению Е. И. Галяшиной и В. Д. Никишина, наибольшую общественную опасность среди различных видов дипфейков представляют на сегодняшний день голосовые дипфейки, сгенерированные нейронными сетями на основе подлинных аудиозаписей речи конкретных людей¹². При этом получаемый дипфейк на слух обычного человека оказывается неотличимым от реального голоса по тембру, эмоциональной окраске и иным особенностям.

Криминальные возможности, предоставляемые таким инновационным средством совершения преступлений, как дипфейк, были быстро оценены организованными группами и преступными сообществами, специализирующимися на совершении высокотехнологичных преступлений. На угрозы правам человека при использовании дипфейк-технологий преступными организациями обратила внимание М. Б. Добробаба¹³. Широкий спектр угроз национальной безопасности, возникающих при овладении дипфейк-технологиями организованными преступными группами, был описан В. Г. Ивановым и Я. Р. Игнатовским¹⁴. Ряд авторов полагает, что применение дипфейков ведет к росту организованной преступности¹⁵.

Привлечение дипфейк-технологий обеспечило быстрое распространение высокотехнологичных преступлений, получивших название «спуфинг-атаки», или «спуфинг» (от англ. spoofing — «подмена»). Под спуфингом понимается незаконная деятельность в информаци-

¹¹ Даниленко Ю. А. Проблемы расследования отдельных видов киберпреступлений, совершенных с использованием искусственного интеллекта // Проблемы получения и использования доказательственной и криминалистически значимой информации : материалы Международной научно-практической конференции, Мисхор (Большая Ялта), 26–27 сентября 2019 г. Симферополь : Ариал, 2019. С. 38.

¹² Galyashina E. I., Nikishin V. D. The protection of megascience projects from deepfake technologies threats: information law aspect // Journal of Physics : Conference Series. 2022. Vol. 2210. P. 012007.

¹³ Добробаба М. Б. Дипфейки как угроза правам человека // Lex russica. 2022. Т. 75. № 11. С. 114.

¹⁴ Иванов В. Г., Игнатовский Я. Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Серия «Государственное и муниципальное управление». 2020. № 4. С. 381.

¹⁵ Ali A., Khushboo K. F., Naseem H., et al. Battle of Deep Fakes: Artificial Intelligence Set to Become a Major Threat to the Individual and National Security // International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 6–7 October 2022. Institute of Electrical and Electronics Engineers (IEEE), 2022. P. 1–5.

онно-телекоммуникационной сети, при которой преступник выдает себя за конкретное лицо или надежный источник информации. Обычно спуфинг применяется для получения конфиденциальных сведений с целью дистанционного хищения денежных средств, внедрения вредоносных компьютерных программ и т.п. Думается, что особую опасность представляет объединение технологий спуфинга и методов социальной инженерии¹⁶, негативно воздействующих на когнитивные способности потерпевших и провоцирующих на осуществление определенных действий, нужных преступникам. Такое объединение за счет возникающего синергетического взаимодействия обеспечивает дополнительные криминальные преимущества и высокую эффективность преступных посягательств.

Особое внимание следует обратить на угрозы уголовному судопроизводству, возникающие при использовании в качестве электронных доказательств цифровых видеоизображений и голосовых записей. По мнению ряда авторов, эти риски являются наиболее значимыми, поскольку они снижают доверие к таким доказательствам и требуют переоценки их применения¹⁷. Ранее подобные доказательства, полученные процессуально допустимым образом, не вызывали особых сомнений. Полагаем, что на сегодняшний день распространение дипфейк-технологий уже требует дополнительной проверки привлекаемых для доказывания цифровых аудио- и видео-записей на предмет отсутствия искусственно сгенерированного контента. Кроме того, представляется справедливым мнение, что дипфейк-технологии могут существенно затруднить внедрение системы электронного правосудия¹⁸.

Применение дипфейков в качестве криминальных инсценировок может повлечь такое тяжелое последствие, как обвинение невиновных лиц. Используемые для противодействия

расследованию инсценировки, по мнению Е. А. Мироновой и В. А. Образцова, являются крайне сложной для разоблачения формой «криминальных фикций»¹⁹. Тяжело также выявить и доказать основанную на применении дипфейков фальсификацию доказательств, ложные показания свидетелей, заключения экспертов и специалистов. Искусственно сгенерированные данные могут долгое время фигурировать в уголовном деле в качестве доказательств, существенно искажая реальные обстоятельства расследуемого дела, затрудняя выдвижение и проверку криминалистических версий. Специфика и опасность инсценировок с применением дипфейк-технологий и сложность их изобличения традиционными методами, на наш взгляд, требуют отдельного исследования.

4. Противодействие применению дипфейков в преступных целях

Криминалистическое противодействие использованию дипфейков в преступной деятельности требует разработки новых практических рекомендаций, предназначенных для правоохранительных органов. Полагаем, что криминалистические основы расследования преступных деяний, в которых в качестве инновационных средств преступления используются дипфейки, были заложены в работах отечественных криминалистов. Так, В. Я. Колдин писал, что при установлении подлинности информации выделяются случаи, в которых «форма выражения информации в исходном и опосредствованном источниках различается», и на примере фонографических записей отмечал, что их подлинность «может быть установлена только техническим путем (исследованием механизма записи и воспроизведения)»²⁰.

¹⁶ См.: Головин А. Ю., Головина Е. В. Социальная инженерия в механизме преступной деятельности в сфере информационно-телекоммуникационных технологий // Известия Тульского государственного университета. Экономические и юридические науки. 2021. № 2. С. 3–13 ; Поляков В. В. Применение методов социальной инженерии при совершении высокотехнологичных преступлений // Криминалистика: вчера, сегодня, завтра. 2023. № 3 (27).

¹⁷ Sandoval M. P., Almeida Vau M. de, Solaas J., Rodrigues L. Threat of deepfakes to the criminal justice system: a systematic review // Crime Science. 2024. Vol. 13. Art. 41.

¹⁸ Лаптев В. А. Deepfake и иные продукты искусственного интеллекта на пути развития онлайн-правосудия // Актуальные проблемы российского права. 2021. Т. 16. № 11. С. 180.

¹⁹ Миронова Е. А., Образцов В. А. Криминальная инсценировка как система фикций // Образование и право. 2019. № 2. С. 182.

²⁰ Колдин В. Я. Электронная информация в праве // Вестник Московского университета. Серия 11, Право. 2016. № 2. С. 104.

Дипфейк-технологии эволюционируют крайне быстро даже на фоне ускоренного развития других технологий искусственного интеллекта. Как следствие, отличить искусственно сгенерированные речь или видеоизображение от оригинала при непосредственном восприятии уже сейчас очень сложно, а в ближайшем будущем станет возможным только при использовании методик, основанных на применении специализированных программных средств. На сегодняшний день находятся в свободном обращении компьютерные программы, в определенной степени способные решать эту задачу, например бесплатные сервисы Forensically, Image Edited, DeepFaceLab, Deepware Scanner. Алгоритмы работы подобных программ обычно основаны на использовании сверточных нейронных сетей, которые позволяют за счет учета пространственных и временных аномалий в распределениях пикселей на изображении или амплитудно-частотных характеристик аудиосигнала выявлять дипфейки²¹ (например, по движению зрачков, отсутствию тени, неестественной изогнутости линий, несоответствию акустики месту съемки при анализе фоновых шумов в аудиофайле и т.д.). В то же время исследователи справедливо указывают на недостаточную готовность методического обеспечения судебной экспертизы к выявлению дипфейков²² и отмечают потребность в специализированном криминалистическом инструментарии, который бы обеспечивал надежное выявление искусственно сгенерированного контента²³. Это свидетельствует о возрастающей роли и важности дальнейшего развития судебных компьютерно-технических экспертиз²⁴,

ориентированных на такие новые задачи, как выделение дипфейковых видеоизображений и аудиоданных в доказательственных материалах, используемых в процессе расследования, и разделение в этих материалах дипфейкового контента и оригинала. Проведение таких экспертиз потребует высокой квалификации в сфере компьютерной обработки изображений и акустических сигналов, а также привлечения экспертов с другими специализациями для проведения комплексных экспертиз²⁵.

Значительно затрудняет противодействие высокотехнологичным преступлениям, в которых используются дипфейки, неразработанность уголовно-правовой квалификации таких деяний. В связи с этим заслуживает внимания мнение о введении уголовной ответственности за использование и распространение дипфейков в преступных целях²⁶. Совершенно обоснованно предложение ввести в качестве нового квалифицирующего признака совершение преступлений с применением дипфейков²⁷. Полагаем также, что мошенничество в сфере компьютерной информации, совершенное с привлечением дипфейк-технологий, с позиций действующего уголовного законодательства может квалифицироваться по совокупности преступлений, подпадающих под действие ст. 159.6 и новой статьи 272.1 УК РФ (введенной Федеральным законом от 30.11.2024 № 421-ФЗ).

В 2010–2020-е гг. активно велась разработка информационных систем, предназначенных для широкого использования биометрических данных. Ведущие коммерческие банки, прежде всего крупнейшее в Российской Федерации ПАО «Сбербанк», государственные органы,

²¹ Amerini I., Barni M., Battiato S., et al. Deepfake Media Forensics: Status and Future Challenges // *Journal of Imaging*. 2025. Vol. 11 (3). P. 1–42.

²² Бодров Н. Ф., Лебедева А. К. Уголовно-правовые и криминалистические аспекты противодействия распространению и использованию дипфейков в Российской Федерации // *Криминалистика: вчера, сегодня, завтра*. 2023. Т. 28. № 4. С. 47.

²³ Исакова А. Г., Осин А. В. Применение искусственного интеллекта в расследовании преступлений с использованием технологии «дипфейк» // *Вестник науки*. 2024. Т. 3. № 1 (70). С. 237.

²⁴ Россинская Е. Р. Генезис и проблемы развития новых родов и видов судебных экспертиз // *Вестник Университета имени О.Е. Кутафина (МГЮА)*. 2014. № 3. С. 114–121; Галяшина Е. И. Диагностика аутентичности цифровых фонограмм в фоноскопической экспертизе: возможности и пределы исследования // *Вестник экономической безопасности*. 2018. № 1. С. 34–41.

²⁵ Galyashina E. I., Nikishin V. D. Op. cit. P. 012007.

²⁶ Киселев А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // *Вестник Московского государственного областного университета. Серия «Юриспруденция»*. 2021. № 3. С. 62.

²⁷ Ефремова М. А., Русскиевич Е. А. Дипфейк (deepfake) и уголовный закон // *Вестник Казанского юридического института МВД России*. 2024. Т. 15. № 2 (56). С. 103.

отвечающие за функционирование государственных (федеральных и региональных) информационных систем, обоснованно планировали внедрение удобных удаленных систем идентификации и аутентификации с помощью информационно-телекоммуникационных сетей на основе записей голоса пользователей и их изображений при обращении граждан за получением услуг. По-видимому, распространение дипфейк-технологий и негативные последствия их криминального применения не вполне учитывались при определении перспективных направлений цифровизации. Представляется, что быстрое развитие этих технологий ставит под сомнение возможность надежной удаленной идентификации и аутентификации личности по биометрическим параметрам, таким как видеоизображение лица и голосовые данные. В этой связи нужно поддержать мнение М. А. Желудкова²⁸ о недооценке той опасности, которую несет расширяющееся применение в преступных

целях технологий искусственного интеллекта, обеспечивающих создание дипфейков.

Заключение

Полагаем, что в ближайшее десятилетие можно уверенно прогнозировать значительный рост высокотехнологичных преступлений с использованием дипфейк-технологий. Разработки в сфере искусственного интеллекта с неизбежностью будут приводить к созданию новых и изменению существующих способов совершения преступлений, в которых могут быть задействованы дипфейки. В связи с этим важны дальнейшее изучение правовой сущности дипфейк-технологий и способов использования дипфейков в преступной деятельности, а также выработка криминалистических приемов, средств и методов для их эффективного выявления, фиксации, исследования и оценки.

СПИСОК ЛИТЕРАТУРЫ

- Бахтеев Д. В. Частные криминалистические теории как источник для разработки прикладных систем искусственного интеллекта в следственной деятельности // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 2 (28). С. 32–43.
- Белкин Р. С. Курс криминалистики : в 3 т. Т. 3 : Криминалистические средства. Приемы и рекомендации. М. : Юристъ, 1997. 480 с.
- Бодров Н. Ф., Лебедева А. К. Уголовно-правовые и криминалистические аспекты противодействия распространению и использованию дипфейков в Российской Федерации // Криминалистика: вчера, сегодня, завтра. 2023. Т. 28. № 4. С. 42–55.
- Вехов В. Б. Понятие и механизм образования электронно-цифровых следов // Использование современных информационных технологий и проблемы информационной безопасности в деятельности правоохранительных органов : межвузовский тематический сборник научных трудов. Калининград : Изд-во Калинингр. ЮИ МВД России, 2009. С. 62–72.
- Галяшина Е. И. Диагностика аутентичности цифровых фонограмм в фоноскопической экспертизе: возможности и пределы исследования // Вестник экономической безопасности. 2018. № 1. С. 34–41.
- Головин А. Ю., Головина Е. В. Социальная инженерия в механизме преступной деятельности в сфере информационно-телекоммуникационных технологий // Известия Тульского государственного университета. Экономические и юридические науки. 2021. № 2. С. 3–13.
- Даниленко Ю. А. Проблемы расследования отдельных видов киберпреступлений, совершенных с использованием искусственного интеллекта // Проблемы получения и использования доказательственной и криминалистически значимой информации : материалы Международной научно-практической конференции, Мисхор (Большая Ялта), 26–27 сентября 2019 г. Симферополь : Ариал, 2019. С. 37–39.
- Добробаба М. Б. Дипфейки как угроза правам человека // Lex russica. 2022. Т. 75. № 11. С. 112–119.
- 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.
- Желудков М. А. Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды // Lex russica. 2021. Т. 74. № 4. С. 63–70.

²⁸ Желудков М. А. Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды // Lex russica. 2021. Т. 74. № 4. С. 68.

Иванов В. Г., Игнатовский Я. Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Серия «Государственное и муниципальное управление». 2020. № 4. С. 379–386.

Исакова А. Г., Осин А. В. Применение искусственного интеллекта в расследовании преступлений с использованием технологии «дипфейк» // Вестник науки. 2024. Т. 3. № 1 (70). С. 235–242.

Киселев А. С. О необходимости правового регулирования в сфере искусственного интеллекта: дипфейк как угроза национальной безопасности // Вестник Московского государственного областного университета. Серия «Юриспруденция». 2021. № 3. С. 54–64.

Колдин В. Я. Электронная информация в праве // Вестник Московского университета. Серия 11, Право. 2016. № 2. С. 96–110.

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.

Мещеряков В. А. Следы преступлений в сфере высоких технологий // Библиотека криминалиста. 2013. № 5 (10). С. 265–270.

Миронова Е. А., Образцов В. А. Криминальная инсценировка как система фикций // Образование и право. 2019. № 2. С. 182–196.

Осипенко А. Л. Проблемы вовлечения электронно-цифровых следов в уголовный процесс // Научный вестник Омской академии МВД России. 2009. № 4 (35). С. 31–34.

Поляков В. В. К проблеме использования понятия «искусственный интеллект» в криминалистике // Юрислингвистика. 2022. № 25 (36). С. 21–28.

Поляков В. В. Криминалистическая классификация способов противодействия расследованию высокотехнологичных преступлений // Юридическая наука и правоохранительная практика. 2023. № 1 (63). С. 69–79.

Поляков В. В. Криминалистическая классификация средств высокотехнологичных преступлений // Вестник Санкт-Петербургского университета. Право. 2024. Т. 15. Вып. 2. С. 421–439.

Поляков В. В. Применение методов социальной инженерии при совершении высокотехнологичных преступлений // Криминалистика: вчера, сегодня, завтра. 2023. № 3 (27). С. 175–188.

Правовое противодействие фейковизации информационного пространства : коллективная монография / под ред. Е. С. Аничкина, В. В. Сорокина. Барнаул : Изд-во Алт. ун-та, 2025. 454 с.

Россинская Е. Р. Генезис и проблемы развития новых родов и видов судебных экспертиз // Вестник Университета имени О.Е. Кутафина (МГЮА). 2014. № 3. С. 114–121.

Савенков А. Н., Россинская Е. Р. Вектор развития криминалистической науки в условиях глобальной цифровизации // Государство и право. 2023. № 5. С. 100–110.

Семикаленова А. И. Цифровые следы: назначение и производство экспертиз // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 5. С. 115–120.

Хабриева Т. Я., Черногор Н. Н. Право в условиях цифровой реальности // Журнал российского права. 2018. № 1. С. 85–102.

Ali A., Khushboo K. F., Naseem H., et al. Battle of Deep Fakes: Artificial Intelligence Set to Become a Major Threat to the Individual and National Security // International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 6–7 October 2022. Institute of Electrical and Electronics Engineers (IEEE), 2022. P. 1–5.

Amerini I., Barni M., Battiato S., et al. Deepfake Media Forensics: Status and Future Challenges // Journal of Imaging. 2025. Vol. 11 (3). P. 1–42.

Bendiab G., Haiouni H., Moulas I., Shiaeles S. Deepfakes in digital media forensics: Generation, AI-based detection and challenges // Journal of Information Security and Applications. 2025. Vol. 88. Art. 103935.

Galyashina E. I., Nikishin V. D. The protection of megascience projects from deepfake technologies threats: information law aspect // Journal of Physics : Conference Series. 2022. Vol. 2210. P. 012007.

Sandoval M. P., Almeida Vau M. de, Solaas J., Rodrigues L. Threat of deepfakes to the criminal justice system: a systematic review // Crime Science. 2024. Vol. 13. Art. 41.

REFERENCES

- Ali A, Khushboo KF, Naseem H, et al. Battle of Deep Fakes: Artificial Intelligence Set to Become a Major Threat to the Individual and National Security. International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 6–7 October 2022. Institute of Electrical and Electronics Engineers (IEEE); 2022. P. 1–38.
- Amerini I, Barni M, Battiato S, et al. Deepfake Media Forensics: Status and Future Challenges. *Journal of Imaging*. 2025;11(3):1-42.
- Anichkina ES, Sorokina VV, (eds.). Legal counteraction to the «fakification» of the information space: A collective monograph. Barnaul: Altai University Publishing House; 2025. (In Russ.).
- Bakhteev DV. Private forensic theories as a source for the development of applied artificial intelligence systems in investigative activities. *Sibirskie ugovolno-protsessualnye i kriminalisticheskie chteniya [Siberian criminal process and criminalistic readings]*. 2020;2(28):32-43. (In Russ.).
- Belkin RS. Course of criminalistics: in 3 volumes. Vol. 3: Forensic tools. Techniques and recommendations. Moscow: Yurist Publ.; 1997. (In Russ.).
- Bendiab G, Haiouni H, Moulas I, Shiaeles S. Deepfakes in digital media forensics: Generation, AI-based detection and challenges. *Journal of Information Security and Applications*. 2025;88:103935.
- Bodrov NF, Lebedev AK. Criminal law and criminalistic aspects of countering the spread and use of deepfakes in the Russian Federation. *Criminalistics: Yesterday, today, tomorrow*. 2023;28(4):42-55. (In Russ.).
- Danilenko YuA. Problems of investigation of certain types of cybercrimes committed using artificial intelligence. In: Problems of obtaining and using evidentiary and criminalistically significant information. Proceedings of the International Scientific and Practical Conference, Miskhor (Bolshaya Yalta), September 26–27, 2019. Simferopol: Arial Publ.; 2019. P. 37–39. (In Russ.).
- Dobrobaba MB. Deepfakes as a threat to human rights. *Lex russica*. 2022;75(11):112-119. (In Russ.).
- Efremova MA, Ruskevich EA. Deepfake and criminal law. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii [Bulletin of the Kazan Law Institute of MIA Russia]*. 2024;15-2(56):97-105. (In Russ.).
- Galyashina EI, Nikishin VD. The protection of megascience projects from deepfake technologies threats: Information law aspect. *Journal of Physics: Conference Series*. 2022;2210:012007.
- Galyashina EI. Diagnostics of authenticity of digital phonograms in phonoscopic examination: Possibilities and limits of research. *Vestnik ekonomicheskoy bezopasnosti*. 2018;1:34-41. (In Russ.).
- Golovin AY, Golovina EV. Social engineering in the mechanism of criminal activity in the field of information and telecommunication technologies. *Izvestiya Tuskogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki [Proceedings of the TSU. Economic and Legal Sciences]*. 2013;2(2):3-13. (In Russ.).
- Isakova AG, Osin AV. The use of artificial intelligence in the investigation of crimes using deepfake technology. *Vestnik nauki*. 2024;3-1(70):235-242. (In Russ.).
- Ivanov VG, Ignatovsky YaR. Deepfakes: Prospects for application in politics and threats to personality and national security. *Vestnik Rossiyskogo universiteta družby narodov. Seriya «Gosudarstvennoe i municipal'noe upravlenie» [RUDN Journal of Law. Series: State and municipal government]*. 2020;4:379-386. (In Russ.).
- Khabrieva TYa, Chernogor NN. Law in the conditions of digital reality. *Zhurnal Rossiyskogo Prava [Journal of Russian Law]*. 2018;1:85-102. (In Russ.).
- Kiselyov AS. On the need for legal regulation in the field of artificial intelligence: Deepfake as a threat to national security. *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya «Yurisprudentsiya» [Bulletin of the Moscow State Region University. Jurisprudence Series]*. 2021;3:54-64. (In Russ.).
- Koldin VYa. Electronic information in law. *Vestnik Moskovskogo Universiteta. Seriya 11, Pravo*. 2016;2:96-110. (In Russ.).
- Laptev VA. Deepfake and other artificial intelligence products on the path of online justice development. *Aktual'nye problemy rossijskogo prava*. 2021;16(11):180-186. (In Russ.).
- Meshcheryakov VA. Traces of crimes in the field of high technology. *Biblioteka kriminalista [Criminalist's Library]*. 2013;5(10):265-270. (In Russ.).
- Mironova EA, Obratsov VA. Crime re-enactment as a system of fictions. *Obrazovanie i pravo*. 2019;2:182-196. (In Russ.).
- Osipenko AL. Problems of involving electronic and digital traces in the criminal process. *Nauchnyy vestnik Omskoy akademii MVD Rossii [Scientific Bulletin of the Omsk Academy of the MIA of Russia]*. 2009;4(35):31-34. (In Russ.).

Polyakov VV. Criminalistic classification of means of high-tech crimes. *Vestnik Sankt-Peterburgskogo universiteta. Pravo [Vestnik of Saint Petersburg University. Law]*. 2024;15(2):421-439. (In Russ.).

Polyakov VV. Criminalistic classification of methods of countering the investigation of high-tech crimes. *Yuridicheskaya nauka i pravookhranitel'naya praktika [Legal Science and Law Enforcement Practice]*. 2023;1(63):69-79. (In Russ.).

Polyakov VV. On the problem of using the concept of «artificial intelligence» in criminology. *Yurislilingvistika [Legal Linguistics]*. 2022;25(36):21-28. (In Russ.).

Polyakov VV. The use of social engineering methods in the commission of high-tech crimes. *Kriminalistika: vchera, segodnya, zavtra*. 2023;3(27):175-188. (In Russ.).

Rossinskaya ER. Genesis and problems of development of new genera and types of forensic examinations. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA)*. 2014;3:114-121. (In Russ.).

Sandoval MP, Almeida Vau M de, Solaas J, Rodrigues L. Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*. 2024;13. Art. 41.

Savenkov AN, Rossinskaya ER. The development vector of criminalistic science in the conditions of global digitalization. *Gosudarstvo i Pravo [State and Law]*. 2023;5:100-110. (In Russ.).

Semikalenova AI. Digital footprints: Purpose and production of expertise. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA)*. 2019;5:115-120. (In Russ.).

Vekhov VB. The concept and mechanism of the formation of electronic and digital traces. In: The use of modern information technologies and problems of information security in the activities of law enforcement agencies: Interuniversity thematic collection of scientific papers. Kaliningrad: Kaliningrad Publishing house. Law Institute of the Ministry of Internal Affairs of Russia; 2009. P. 62–72. (In Russ.).

Zheludkov MA. Justification of the necessity to adjust law enforcement agencies to digital transformation of criminality. *Lex russica*. 2021;74(4):63-70. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Поляков Виталий Викторович, кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики Юридического института Алтайского государственного университета
д. 61, Ленина пр., г. Барнаул 656049, Российская Федерация
agupolyakov@gmail.com

INFORMATION ABOUT THE AUTHOR

Vitaly V. Polyakov, Cand. Sci. (Law), Associate Professor, Department of Criminal Procedure and Criminalistics, Altai State University Law Institute, Barnaul, Russian Federation
agupolyakov@gmail.com

Материал поступил в редакцию 28 апреля 2025 г.

Статья получена после рецензирования 13 мая 2025 г.

Принята к печати 15 июля 2026 г.

Received 28.04.2025.

Revised 13.05.2025.

Accepted 15.07.2026.