DOI: 10.17803/1994-1471.2025.179.10.133-143

Я. А. Климова*

Основные положения частной криминалистической методики расследования преступлений, совершенных с использованием технологии дипфейк: от теории к практике киберследствия

Аннотация. Цифровизация, выступающая в роли главного драйвера трансформации общества, способствует популяризации и востребованности информационных систем в повседневной жизни. Эта тенденция оказывает существенное влияние на становление новой преступной парадигмы — экспоненциального роста числа преступлений, совершенных с применением дипфейк-технологий. В связи с этим всё бóльшую актуальность приобретает поиск эффективных криминалистических инструментов выявления, раскрытия и расследования преступлений, совершенных с использованием технологии подмены контента. Современная криминалистическая наука вследствие своей способности оперативно интегрировать передовые научно-технические достижения и быстро адаптироваться к инновационным изменениям в обществе занимает лидирующие позиции в сфере борьбы с преступностью. Существенное влияние на улучшение качества и эффективность расследования преступлений, совершенных с использованием технологии дипфейк, может оказать выработка научно обоснованных рекомендаций и их применение в практической деятельности органов предварительного расследования. Посредством изучения и анализа статистических данных, научных работ, нормативных правовых актов и эмпирического материла выделены ключевые этапы механизма совершения преступления, сформулированы методологические основы частной криминалистической методики расследования рассматриваемой категории преступлений, предложена оптимальная программа расследования. Требует дальнейшего научного осмысления проблема необходимости формирования IT-компетенций у сотрудников органов предварительного следствия.

Ключевые слова: дипфейк; цифровизация; частная методика расследования; IT-технологии; искусственный интеллект; программа расследования; следственные действия; специальные знания; расследование преступлений.

Для цитирования: *Климова Я. А.* Основные положения частной криминалистической методики расследования преступлений, совершенных с использованием технологии дипфейк: от теории к практике киберследствия // Актуальные проблемы российского права. — 2025. — Т. 20. — № 10. — С. 133–143. — DOI: 10.17803/1994-1471.2025.179.10.133-143.

* *Климова Яна Александровна*, кандидат юридических наук, доцент, профессор кафедры криминалистики учебно-научного комплекса по предварительному следствию в ОВД Волгоградской академии МВД России
Историческая ул., д. 130, г. Волгоград, Российская Федерация, 400089
aya3008@yandex.ru

Core Principles of a Special Forensic Methodology for Investigating Crimes Committed Using Deepfake Technology: From Theory to Cyber-Investigation Practice

Yana A. Klimova, Cand. Sci. (Law), Associate Professor, Professor, Department of Forensic Science, Educational and Scientific Complex for Preliminary Investigation in the Internal Affairs Directorate, Volgograd Academy of the Ministry of Internal Affairs of Russia, Volgograd, Russian Federation
aya3008@yandex.ru

Abstract. Digitalization, acting as the main driver of societal transformation, contributes to the popularization and demand for information systems in everyday life. This trend significantly influences the formation of a new criminal paradigm — an exponential increase in the number of crimes committed using deepfake technology. In this regard, the search for effective forensic tools for identifying, solving, and investigating crimes committed using content substitution technology is becoming increasingly relevant. Due to its ability to rapidly integrate advanced scientific and technical achievements and quickly adapt to innovative changes in society, modern forensic science holds a leading position in the fight against crime. The development of scientifically grounded recommendations and their application in the practical work of preliminary investigation bodies can significantly affect the quality and effectiveness of investigating crimes committed using deepfake technology. Based on the study and analysis of statistical data, scientific works, regulatory legal acts, and empirical material, the main stages of the crime commission mechanism have been identified, the methodological foundations of a special forensic investigation methodology for this category of crimes have been formulated, and an optimal investigation program has been proposed. The problem of the need to develop IT competencies among preliminary investigation officers requires further scientific consideration.
Keywords: deepfake; digitalization; private investigation methodology; IT technologies; artificial intelligence; investigative program; investigative activities; specialized knowledge; crime investigation.
Cite as: Klimova YaA. Core Principles of a Special Forensic Methodology for Investigating Crimes Committed Using Deepfake Technology: From Theory to Cyber-Investigation Practice. *Aktual'nye problemy rossijskogo prava*. 2025;20(10):133-143. (In Russ.). DOI: 10.17803/1994-1471.2025.179.10.133-143.

Введение

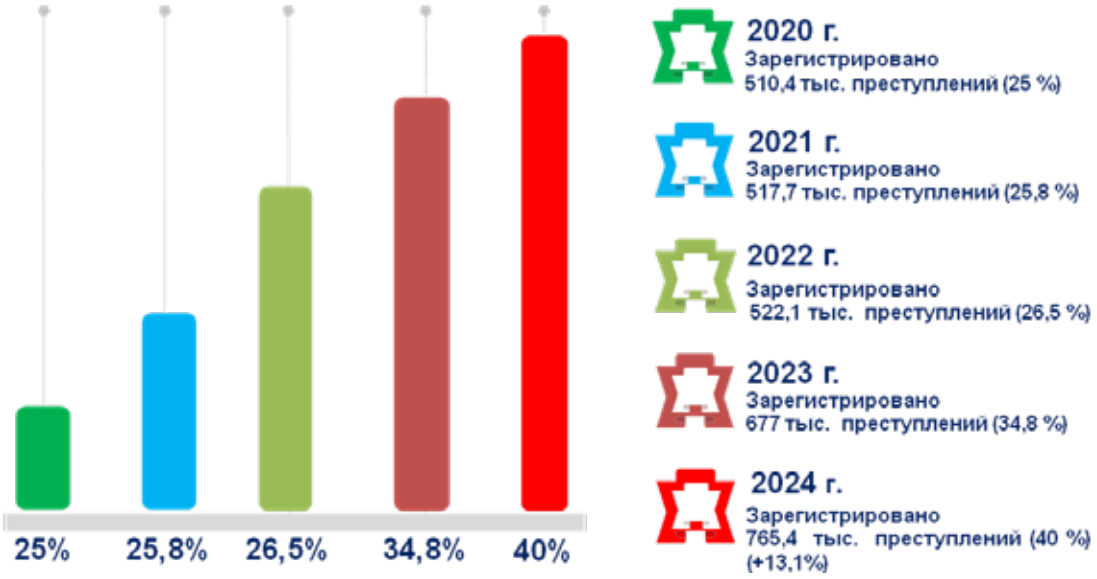
Интенсивное применение информационных технологий в различных аспектах современной жизни радикально трансформировало облик криминального мира. Сегодня IT-продукты выходят за рамки развлекательного контента и становятся мощным орудием в руках преступников. В связи с этим проблема необходимости трансформации криминалистической науки в контексте цифровизации получает исключительную актуальность.

Президент РФ В. В. Путин, принимая участие в ежегодном расширенном заседании коллегии МВД России, состоявшемся 5 марта 2025 г., обратил особое внимание на низкую раскрываемость IT-преступлений, которая составляет всего 23 %. В заключение выступления Президент России поставил перед органами правоохранительного блока задачу — искать новые, более эффективные методы борьбы с этой угрозой[1].

Об актуальности проблемы свидетельствует тенденция стабильного увеличения статистических показателей роста высокотехнологичных преступлений, которая сохраняется на протяжении последних лет (см. диаграмму)[2].

[1] Владимир Путин выступил на ежегодном расширенном заседании коллегии Министерства внутренних дел России (Москва, 5 марта 2025 г.) // URL: http://www.kremlin.ru/events/president/transcripts/deliberations%20/76408 (дата обращения: 29.04.2025).

[2] См.: Портал правовой статистики: официальный сайт Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/analytics (дата обращения: 12.09.2024) ; Статистические сведения МВД о состоянии



Статистические данные правоохранительных органов РФ о количестве преступлений, совершенных с использованием информационно-телекоммуникационных технологий за 2020–2024 гг.

Анализ статистических данных позволяет констатировать, что к 2024 г. вследствие развития искусственного интеллекта IT-преступность достигла пика за рассматриваемые пять лет: 40 % от всех зарегистрированных в России преступлений. Это наивысший показатель с 2020 г.

В I квартале текущего года вектор роста количества преступлений сохраняется. При этом уже в январе — марте 2025 г. зарегистрировано на 3 % больше таких деяний, чем за аналогичный период прошлого года[3].

Постановка проблемы

Специфика расследования киберпреступлений обусловливается их ключевой особенностью: использованием цифровых технологий в качестве средства достижения преступных целей.

Ярчайший пример: стремительно набирающий обороты преступный тренд — совершение преступлений с применением технологии дипфейк (deepfake). Мир накрывает эпидемия высокотехнологического обмана, охватывающая различные государства, независимо от их исторического пути развития, социально-экономического уровня, политического устройства и прочих различий. В 2024 г. в мировом масштабе количество дипфейков увеличилось на 118 % по сравнению с 2023 г. Кроме того, искусственный интеллект стал средством совершения 42,5 % всех финансовых преступлений в мире, что подчеркивает серьезность угрозы[4]. Проблема выходит за пределы национальных границ отдельных стран и приобретает транснациональный масштаб, становясь международным феноменом.

Ключевая суть концепции дипфейков заключается в стремлении к максимальной достовер-

преступности за 2020–2022 г. // Официальный сайт МВД Российской Федерации. URL: https://xn--b1aew.xn--p1ai/news/item/42987324/ (дата обращения: 30.09.2024).

[3] См.: Состояние преступности в Российской Федерации за январь — март 2025 г. // URL: https://мвд.рф/reports/item/64450541/ (дата обращения: 20.04.2025).

[4] Обзор итогов Российского форума по управлению интернетом (RIGF 2025) (Москва, 7 апреля 2025 г.) // URL: https://rigf.ru/press/opublikovan-obzor-itogov-rigf-2025/ (дата обращения: 05.05.2025).

ности, что в результате провоцирует резкий рост модифицированного контента, используемого как для манипуляции общественным мнением, так и с целью оказания воздействия на сознание конкретного человека.

Современные нейросетевые алгоритмы обрабатывают колоссальные массивы цифровой информации в виде фотографий, аудио- и видеоматериалов для того, чтобы обучиться с наибольшей правдоподобностью воспроизводить внешность, голос, движения и мимику определенного лица.

Благодаря потенциалу нейронных сетей становится возможной даже доработка донорского контента путем создания различных визуальных эффектов, поражающих своей достоверностью (искусственное состаривание, отображение широкого спектра эмоций, применение различных стилей макияжа и другие визуальные трансформации).

Учитывая обилие медиаконтента, находящегося в открытом доступе в социальных сетях, мессенджерах, видеохостингах и иных ресурсах сети Интернет, эти системы научились создавать практически точную копию любого человека — так называемого цифрового двойника, что было продемонстрировано в ходе прямой линии с Президентом России[5].

Так, согласно исследованию, проведенному Международной ассоциацией по фактчекингу (Global Fact-checking Network, GFCN), в России за первые три месяца 2025 г. обнаружены 61 уникальный дипфейк и 2,3 тыс. их копий. Этот показатель составляет 67 % от всех дипфейков, выявленных в 2024 г., и в 2,6 раза превышает количество подобных материалов, зафиксированных за весь 2023 г.[6]

Таким образом, системообразующим элементом криминалистической характеристики рассматриваемых преступлений будет выступать способ их совершения.

Приведем примеры использования технологий подмены аудио- и видеоизображения в преступных целях. Так, в январе 2025 г. телефонный аферист позвонил 92-летнему пенсионеру по видеосвязи с использованием технологии дипфейк и, выдавая себя за руководителя госоргана и его помощника, убедил принять участие в мнимой операции по поимке лиц, якобы совершивших преступления. Злоумышленники под угрозой проведения обыска дома узнали у москвича о хранящихся 100 тыс. долл. и убедили передать их для размещения в страховой ячейке. Чтобы получить возможность распоряжаться деньгами, аферист уговорил пенсионера выбросить их с балкона после условного сигнала, что потерпевший и сделал. Спустя непродолжительное время пострадавший понял, что стал жертвой обмана, и обратился в правоохранительные органы.

Впоследствии при координирующей роли прокуратуры округа с поличным задержан 20-летний курьер, получивший часть денег от пенсионера[7].

Не менее показательный случай произошел в Нижнем Новгороде: бухгалтеру местной компании позвонила ее начальница и попросила передать 1 млн руб. наличными. Голос был максимально похож, поэтому подозрений не возникло — банальный разговор руководителя и подчиненного. «Руководительница» сказала взять наличные из сейфа и отправить ей с курьером. Курьер тут же подъехал, всё забрал. Позднее выяснилось, что это мошенники, которым удалось подделать голос и интонации человека[8].

---

[5] См.: Итоги года с Владимиром Путиным — 2023 // URL: https://www.pnp.ru/story/itogi-goda-s-vladimirom-putinym-2023/ (дата обращения: 29.04.2025).

[6] В РФ за I квартал 2025 г. выявили более 60 уникальных дипфейков // URL: https://tass.ru/obschestvo/23621185 (дата обращения: 07.05.2025).

[7] Установление всех обстоятельств мошенничества в отношении пенсионера на контроле в прокуратуре // URL: https://basman.mos.ru/public-safety/information-tape/detail/12823466.html (дата обращения: 10.05.2025).

[8] Однажды из-за дипфейка инвестор потерял 35 млн долларов // URL: https://www.dk.ru/news/237198863 (дата обращения: 15.05.2025).

Недавно был обнаружен еще один способ мошенничества с использованием искусственного интеллекта. Злоумышленники не только отправляют видео, но и совершают видеозвонки, убедительно подменяя изображение и голос. Так, во время подобных звонков злоумышленник представляется сотрудником ФСБ и информирует о внеплановых проверках с просьбой предупредить об этом своих коллег.

Один из таких эпизодов произошел в начале 2025 г. с главным редактором ИА «Дон 24» В. Серпионовым: мошенники не только попробовали совершить видеозвонок, чтобы сообщить о грядущей проверке, но и в качестве доказательства прислали поддельный приказ ФСБ с подписью и печатью и дополнительно еще несколько материалов[9].

Дипфейки становятся всё более реалистичными и убедительными. Такая трансформация способствует появлению новых мошеннических схем. Сейчас наибольшее распространение получила схема fakeboss — указания от фейкового руководителя с использованием дипфейка и войсфейка, с помощью которых мошенники похищают деньги в «Телеграме».

При этом социальный статус человека не всегда защищает от злоумышленников. Жертвами становятся также педагогические работники, люди, обладающие специальными знаниями в области раскрытия и расследования IT-преступлений[10].

В связи с этим у органов предварительного следствия возникает ряд вопросов при расследовании таких преступлений:

— Что является местом происшествия?

— Где производить следственные осмотры?

— Какие объекты, в том числе цифровые, и где следует изымать?

— Какие судебные экспертизы надо назначать?

— В какой момент хищение считается оконченным, если похищены не безналичные денежные средства, а иные цифровые активы (виртуальная игровая валюта, скины, улучшение экипировки, виртуальные ценности и предметы) или криптовалюта, токены (NFT)? Можно ли их вообще относить к предмету хищения?

У экспертно-криминалистических подразделений, в свою очередь, возникают вопросы:

— Как обеспечить сохранность исследуемых цифровых объектов?

— Какие методики исследования необходимо применять при производстве экспертиз?

Данные вопросы являются весьма дискуссионными. В частности, исследованию проблем законодательной регламентации и вопросам противодействия преступной деятельности с применением технологии дипфейков посвящены работы многих ученых: Н. Ф. Бодрова, А. К. Лебедевой, М. А. Ефремовой, Е. А. Русскевича, А. Б. Смушкина, М. М. Менжеги и др.[11]

Механизм совершения преступления с использованием технологии дипфейк

На основе анализа судебно-следственной практики, эмпирического материала, с помощью форсайт-технологии и методов криминалистического прогнозирования мы смоделировали динамическую систему дипфейк-атаки, определяющей содержание исследуемого уголовного деяния.

---

[9] В Ростовской области мошенники попытались обмануть дончанина с помощью нейросетей // URL: https://pobeda-aksay.ru/2025/02/06/v-rostovskoj-oblasti-moshenniki-popytalis-obmanut-donchanina-s-pomoshhyu-nejrosetej/ (дата обращения: 11.05.2025).

[10] См.: Новая схема мошенничества в соцсетях — преподавателей вузов обманывают от имени замминистра образования, ФСБ и Центробанка // URL: https://usptu.ru/ru/news/novaya-skhema-moshennichestva-v-socsetyakh-prepodavateley-vuzov-obmanyvayut-ot-imeni (дата обращения: 11.05.2025) ; В Краснодаре мошенники звонят педагогам кубанского вуза от имени ФСБ // URL: https://utyug.info/new/48182/ (дата обращения: 11.05.2025).

[11] См., например: *Бодров Н. Ф.*, *Лебедева А. К.* Уголовно-правовые и криминалистические аспекты противодействия распространению и использованию дипфейков в Российской Федерации // Криминалистика: вчера, сегодня, завтра. 2023. № 4. С. 42–55 ; *Ефремова М. А.*, *Русскевич Е. А.* Дипфейк (deepfake)

Моделирование механизма преступления, совершенного с использованием дипфейка, позволило нам выделить основные этапы его подготовки и совершения.

1-й этап. Сбор интернет-досье в цифровом пространстве и из открытых источников, скрампинг данных. Наиболее распространены следующие способы:

— извлечение информации из социальных сетей и веб-сайтов (выяснение анкетных данных, места работы/учебы, круга общения и т.д.);

— использование фото-, видеоматериалов из открытых источников (официальных групп в социальных сетях или мессенджерах, информация о мероприятиях в новостных лентах СМИ, получение данных из личных блогов и страниц в соцсетях);

— получение персональных данных путем фишинга, неправомерного доступа к личному кабинету на портале «Госуслуги» или аккаунтам в приложениях-мессенджерах;

— взлом устройств умного дома путем создания на устройствах ботнета, перехват с использованием искусственного интеллекта управления системой и подключение к видеонаблюдению;

— «случайный звонок» в мессенджере (чаще всего в «Телеграме»): использование видеозвонка с включением демонстрации экрана для получения биометрических данных жертв, включая запись голоса и изображения лица, с последующими обработкой фона и созданием целевого контента.

2-й этап. Совершение звонков и формирование анкеты с личными данными. С этой целью злоумышленники обеспечивают функционирование SIM-боксов, GSM-шлюзов и SIM-банков, обслуживающих мошеннические кол-центры. С помощью этих устройств, использующих нелегальные сим-карты, преступники осуществляют массовый обзвон граждан.

Однако помимо технической составляющей немаловажную роль играют методы социальной инженерии. Приведем пример анкеты, которую на этом этапе по результатам многочисленных звонков (в том числе спам-звонков) составляют мошенники для повышения эффективности психологического воздействия на жертву.

Пример анкеты, составляемой мошенниками в целях использования личной информации

Основная информация	**Иванова Ирина Ивановна, 01.01.1960 г. р., пенсионерка**
Есть ли третьи лица в разговоре?	Муж
Что делал(а) после звонка?	Звонила в соцслужбу. Ей сказали, что обманули ее, от них никто не приезжал
Мошенники «катали» ли раньше	Не «катали»
Дополнительная информация	Есть соцработник, который каждый день названивает
Куда подавала документы?	В больницу, когда у мужа был инфаркт, 16 февраля
Состояние здоровья	Муж неважно ходит
Кодовое слово	Монета
Банки	ВТБ, Сбер
Вклад	2 тыс.
Общая сумма	400 тыс.
Снимала проценты	20 %

3-й этап. Создание дипфейка и применение методов социальной инженерии. На основе собранной информации разрабатывается сценарий и создается адресный дипфейк для манипулирования сознанием выбранной жертвы.

и уголовный закон // Вестник Казанского юридического института МВД России. 2024. № 2. С. 97–105 ; *Смушкин А. Б.*, *Менжега М. М.* Некоторые вопросы цифровизации криминалистики // Lex russica (Русский закон). 2023. № 3. С. 100–109.

По данным Центра разработки AI-продуктов, MTS AI-технология постоянно совершенствуется, и если в 2024–2025 гг. основное распространение получили фейковые видео в мессенджерах (так называемые видеокружки́) и голосовые сообщения, то уже в 2026 г. мошенники смогут в реальном времени имитировать разговор от лица родственников и знакомых жертвы. Поскольку технологии создания и модификации видео, а также клонирования голосов ушли еще на несколько шагов вперед, то уже к концу этого года каждый второй россиянин может стать жертвой дипфейк-атак[12].

Нужно учитывать, что уже сегодня возможна полная генерация контента нейросетями на основании качественно составленного промта и использования генеративно-состязательных нейросетей (generative adversarial network, GAN), представляющих собой архитектуру, состоящую из генератора и дискриминатора, настроенных на работу друг против друга с целью усовершенствования конечного результата. Эти нейронные сети учатся генерировать реалистичные образцы данных, на которых они обучались. Особая опасность для потенциальной жертвы заключается в том, что такие дипфейки выглядят гиперреалистично.

4-й этап. Хищение денежных средств и иных цифровых активов. Считаем целесообразным в качестве предмета преступного посягательства рассматривать не только безналичные денежные средства, но и цифровые активы, виртуальную собственность. При этом ввиду отсутствия у них вещной формы в реальном мире указанные активы следует трактовать как благо (имущество) в самом широком смысле, то есть как объекты, имеющие ценность не столько материальную, сколько цифровую (например, криптовалюта, затраченные временны́е ресурсы, наличие игрового преимущества и т.д.).

О важности устранения лакун в правовой регламентации этого явления свидетельствует внимание законодателя к указанной проблеме. В частности, в конце апреля 2025 г. в Государственную Думу РФ на рассмотрение внесен законопроект о признании цифровой валюты имуществом для целей уголовного судопроизводства. В силу специфики цифровой валюты и особенностей удаленного доступа к ней подчеркивается необходимость оперативной реакции со стороны органов расследования в случае обнаружения цифровой валюты при производстве по уголовному делу и предлагается алгоритм действий следователя при осуществлении изъятия криптовалюты[13].

Программа расследования преступлений, совершенных с использованием технологии дипфейк

На основании сказанного были сформулированы криминалистические рекомендации и разработана оптимальная программа расследования преступлений, совершенных с использованием технологии дипфейк:

I. Осмотр места происшествия. Считаем правильным производить осмотр следующих объектов:

— места расположения IP-адреса. Устанавливается путем направления посредством электронного документооборота в учреждения финансово-кредитной сферы, операторам сотовой связи, интернет-провайдерам и интернет-сервисам запросов о получении сведений о подключенных удаленных каналах обслуживания «Мобильный банк» с указанием IP-адресов и информации о подключенном устройстве с указанием его координат. Однако важно учитывать, что использование динамического IP-адреса, SIM-боксов, GSM-шлюзов и SIM-банков, вирту-

[12] Лживый вызов: каждый второй россиянин столкнется с дипфейк-атакой к концу года // URL: https://iz.ru/1879039/elizaveta-krylova/lzhivyj-vyzov-kazhdyj-vtoroj-rossiyanin-stolknetsya-s-dipfejk-atakoj-k-koncu-goda (дата обращения: 12.05.2025).

[13] Законопроект № 902782-8 от 24.04.2025 «О внесении изменений в статью 104-1 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации (об особенностях изъятия цифровой валюты)» // URL: https://sozd.duma.gov.ru/bill/902782-8 (дата обращения: 12.05.2025).

альных АТС затрудняет возможность установления фактического адреса осмотра;

— места создания исходного кода программы. Устанавливается по метаданным видеоконтента;

— места физического нахождения устройства преступника. Устанавливается в ходе проведения оперативно-разыскных мероприятий, в том числе с использованием технологии OSINT (open source intelligence, то есть «аналитическая разведка», сбор и анализ информации, находящейся в открытом доступе).

II. Допросы:

1. Допрос потерпевшего, в ходе которого необходимо подробно восстановить хронологию действий как злоумышленника, так и потерпевшего для определения конкретного способа и механизма хищения. В ходе допроса следует установить дату, время, абонентский номер, с которого поступил телефонный звонок (сообщение, видео- или аудиофайлы), в каком приложении, имя пользователя, от которого он поступил. Далее надо изложить предмет разговора/переписки со злоумышленником. Выяснить информацию о номерах мобильных телефонов, подключенных к мобильному банку. Получить ответы на вопросы:

— Каким образом были переведены похищенные денежные средства: на какой счет или с использованием какой банковской карты?

— Применялись ли какие-либо системы быстрых переводов?

— Куда именно, по указанию мошенника, потерпевший должен был осуществлять переводы денежных средств?

— На какие абонентские номера они были зачислены?

— Какова сумма ущерба и является ли она значительной с учетом материального положения потерпевшего?

2. Допрос свидетеля, являющегося донором исходного медиаконтента. В процессе допроса определяются дата, точное время и телефонный номер абонента, от которого был получен видеозвонок, в каком приложении, выявляются отобразившееся имя пользователя или никнейм (сетевое имя), выясняется, поступали ли ранее подозрительные звонки или спам.

III. Следственные осмотры:

1. Осмотр принадлежащего подозреваемому устройства, внутри которого имеется физически встроенная память, содержащая криминалистически значимую информацию. При этом необходимо:

— установить физическое место создания модифицированного контента. Для этого нужно зафиксировать метаданные видео, наличие черновиков разных этапов, различных версий видео, следы чат-ботов;

— определить наличие на устройстве предустановленного набора программного обеспечения для создания дипфейков/войсфейков (либо программ, которые потенциально могут использоваться для их создания);

— выявить наличие донорского видеоматериала;

— установить наличие целевого видеоконтента;

— исследовать качества исходных данных дипфейка. Для изучения необходимо наличие начального кода. Выяснить, имеются ли признаки обфускации (запутывание кода, то есть приведение исходного кода программы к виду, сохраняющему ее функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции);

— определить количество итераций — шагов улучшения контента;

— установить признаки перекодировки, тип постобработки: осуществлялась ли покадровая обработка с помощью программного обеспечения человеком или это полная генерация нейросетями.

Кроме этого, немаловажно в процессе осмотра осуществить анализ личности и способностей самого подозреваемого (наличие профессиональных навыков, интересов, поведенческих шаблонов) путем изучения запросов в истории браузера, учетных записей в социальных сетях, посещаемых веб-сайтов и информации о просмотренном контенте в приложениях, изучение круга общения и истории покупок.

2. Осмотр мобильной станции сетей сотовой связи стандарта GSM (мобильного телефона) подозреваемого, в ходе которого необходимо:

— зафиксировать наличие данных о переписке пользователя мобильного телефона с потерпевшим в программном обеспечении (например, «Телеграм»);

— установить наличие в памяти мобильного телефона сведений и приложений, предназначенных для генерации дипфейков/войсфейков;

— проанализировать ленту событий мобильного телефона (установить временные маркеры при использовании приложений);

— произвести осмотр облачных данных, который позволит по GPS-меткам получить информацию о передвижениях подозреваемого в период совершения преступления.

3. Осмотр мобильной станции сетей сотовой связи стандарта GSM (мобильного телефона) потерпевшего. Обязательно зафиксировать способ получения потерпевшим сгенерированного контента (поскольку отправка через мессенджеры сжимает видео, ухудшает его качество, что существенно ограничивает возможности экспертного исследования). Кроме этого, отразить в протоколе следственного действия: установленные приложения, наличие телефонных звонков/сообщений мошенника, программ онлайн-банков, а также при помощи личных кабинетов с участием потерпевшего получить сведения о движении денежных средств по его банковскому счету.

Производство и назначение судебных экспертиз. Целесообразно назначение фото-, видеотехнической, портретной, фоноскопической, компьютерной (исследование компьютерной информации) экспертиз.

Кроме этого, учеными-криминалистами в качестве нового вида экспертизы для оценки цифровых активов предлагается оценочная экспертиза стоимости объектов виртуальной собственности[14].

Вызывает интерес информационно-аналитическая экспертиза, представляющая собой анализ цифровых массивов данных, содержащих сведения о деятельности цифровых систем, устройств, индивидуумов, в целях поиска неочевидных взаимосвязей отдельных элементов (например, исследование сведений о телефонных соединениях, банковских транзакциях, сообщениях в мессенджерах и социальных сетях, данных с камер видеонаблюдения).

Несмотря на то что программные продукты, направленные на распознавание дипфейков, активно разрабатываются, сегодня специалисты выявляют их фактически вручную.

Поэтому в настоящее время при производстве экспертиз возникает проблема отсутствия устойчиво работающей технологии распознавания сгенерированного контента в виде готового продукта искусственного интеллекта, а именно:

а) специальная архитектура нейронной сети, направленная на выявление признаков апскейлинга (технического улучшения качества исходного контента);

б) применение состязательно-генеративных нейросетей для создания дипфейков;

в) низкий перцептивный порог обнаружения артефактов дипфейков (то есть процесса обнаружения модифицированного контента).

Сейчас можно ответить на вопрос, имеются ли на видео признаки монтажа, а если целевое видео полностью качественно сгенерировано, то велика вероятность невозможности экспертного решения поставленного вопроса, то есть с точки зрения доказывания такое исследование не принесет нужного результата.

В связи с этим предлагаем рассматривать дипфейк не только как техническую подделку — внутрикадровый монтаж с заменой лиц одних людей на лица других, направленный на искажение первоначального содержания видеоизображений, но и как своеобразный интеллектуальный подлог: в случае невозможности получения информации посредством экспертного исследования необходимо доказывать факт генерации и модификации контента следственным путем.

[14] *Еремченко В. И.*, *Сафронкина О. В.* Проблемные вопросы определения суммы материального ущерба и пути их решения при расследовании мошенничества в сфере компьютерной информации в области индустрии компьютерных игр // Общество и право. 2019. № 4 (70). С. 64–68.

Выводы

В завершение можно резюмировать:

1. На современном этапе развития криминалистической науки доказывание IT-преступлений возможно преимущественно следственным путем.

2. Назрела необходимость формирования IT-компетенций у сотрудников следственного аппарата. Для повышения эффективности деятельности органов правоохранительного блока в рамках единой системы противодействия киберпреступлениям целесообразны разработка и реализация унифицированных профессиональных программ обучения в сфере получения IT-компетенций, которые будут продуктом консолидации усилий ведомств и организаций, имеющих передовой опыт в борьбе с IT-преступностью, и наиболее эффективных стратегий расследования.

3. Формирование и совершенствование навыков по обнаружению и фиксации следов на всех стадиях механизма совершения преступления рационально осуществлять в ходе образовательного процесса.

Таким образом, решение проблемы использования технологии дипфейка в преступных целях требует комплексного, системного подхода. Представляется перспективным дальнейшее углубленное исследование всех этапов механизма совершения подобных преступлений, получение следователями IT-компетенций для совершенствования навыков своевременного обнаружения, изъятия и фиксации криминалистически значимой цифровой информации.

Реализация предложенных мер будет способствовать повышению эффективности уголовно-процессуальной деятельности, оперативной адаптации к инновационным изменениям, происходящим в обществе, позволит расширить арсенал инструментария расследования и обеспечит передовые позиции в борьбе с преступностью.

БИБЛИОГРАФИЯ

1. *Батоев В. Б.* Использование технологии Deepfake в преступной деятельности: проблемы противодействия и пути их решения // Вестник Воронежского института МВД России. — 2023. — № 1. — С. 165–169.
2. *Бахтеев Д. В.* Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений : автореф. дис. … д-ра юрид. наук. — Екатеринбург, 2022. — 504 с.
3. *Бодров Н. Ф.*, *Лебедева А. К.* Перспективы судебно-экспертного исследования синтезированной звучащей речи // Законы России: опыт, анализ, практика. — 2021. — № 3. — С. 9–13.
4. *Бодров Н. Ф.*, *Лебедева А. К.* Уголовно-правовые и криминалистические аспекты противодействия распространению и использованию дипфейков в Российской Федерации // Криминалистика: вчера, сегодня, завтра. — 2023. — № 4. — С. 42–55.
5. *Ефремова М. А.*, *Русскевич Е. А.* Дипфейк (deepfake) и уголовный закон // Вестник Казанского юридического института МВД России. — 2024. — № 2. — С. 97–105.
6. *Зайцева Е. А.* Стандартизация доказывания — путь к оптимизации уголовного судопроизводства // Вестник Волгоградской академии МВД России. — 2025. — № 1 (72). — С. 9–15.
7. *Ларина Е. С.* Криминальная жизнь дипфейков // Информационные войны. — 2022. — № 3 (63). — С. 69–73.
8. *Лужинская Е. Л.*, *Чванкин В. А.* Особенности исследования изображений внешнего облика человека, измененного при помощи программных средств // Вопросы криминологии, криминалистики и судебной экспертизы. — 2022. — № 2 (52). — С. 116–121.
9. *Поляков В. В.* Источники и принципы формирования частной методики расследования высокотехнологичных преступлений // Lex russica (Русский закон). — 2022. — № 75 (6). — С. 85–96.
10. *Расторопова О. В.* Противодействие использованию искусственного интеллекта в преступных целях // Вестник Университета прокуратуры Российской Федерации. — 2021. — № 4 (84). — С. 52–58.

11. *Смушкин А. Б., Менжега М. М.* Некоторые вопросы цифровизации криминалистики // Lex russica (Русский закон). — 2023. — № 3. — С. 100–109.

Материал поступил в редакцию 25 июня 2025 г.

REFERENCES (TRANSLITERATION)

1. Batoev V. B. Ispolzovanie tekhnologii Deepfake v prestupnoy deyatelnosti: problemy protivodeystviya i puti ikh resheniya // Vestnik Voronezhskogo instituta MVD Rossii. — 2023. — № 1. — S. 165–169.
2. Bakhteev D. V. Kontseptualnye osnovy teorii kriminalisticheskogo myshleniya i ispolzovaniya sistem iskusstvennogo intellekta v rassledovanii prestupleniy: avtoref. dis. … d-ra yurid. nauk. — Ekaterinburg, 2022. — 504 s.
3. Bodrov N. F., Lebedeva A. K. Perspektivy sudebno-ekspertnogo issledovaniya sintezirovannoy zvuchashchey rechi // Zakony Rossii: opyt, analiz, praktika. — 2021. — № 3. — S. 9–13.
4. Bodrov N. F., Lebedeva A. K. Ugolovno-pravovye i kriminalisticheskie aspekty protivodeystviya rasprostraneniyu i ispolzovaniyu dipfeykov v Rossiyskoy Federatsii // Kriminalistika: vchera, segodnya, zavtra. — 2023. — № 4. — S. 42–55.
5. Efremova M. A., Russkevich E. A. Dipfeyk (deepfake) i ugolovnyy zakon // Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii. — 2024. — № 2. — S. 97–105.
6. Zaytseva E. A. Standartizatsiya dokazyvaniya — put k optimizatsii ugolovnogo sudoproizvodstva // Vestnik Volgogradskoy akademii MVD Rossii. — 2025. — № 1 (72). — S. 9–15.
7. Larina E. S. Kriminalnaya zhizn dipfeykov // Informatsionnye voyny. — 2022. — № 3 (63). — S. 69–73.
8. Luzhinskaya E. L., Chvankin V. A. Osobennosti issledovaniya izobrazheniy vneshnego oblika cheloveka, izmenennogo pri pomoshchi programmnykh sredstv // Voprosy kriminologii, kriminalistiki i sudebnoy ekspertizy. — 2022. — № 2 (52). — S. 116–121.
9. Polyakov V. V. Istochniki i printsipy formirovaniya chastnoy metodiki rassledovaniya vysokotekhnologichnykh prestupleniy // Lex russica (Russkiy zakon). — 2022. — № 75 (6). — S. 85–96.
10. Rastoropova O. V. Protivodeystvie ispolzovaniyu iskusstvennogo intellekta v prestupnykh tselyakh // Vestnik Universiteta prokuratury Rossiyskoy Federatsii. — 2021. — № 4 (84). — S. 52–58.
11. Smushkin A. B., Menzhega M. M. Nekotorye voprosy tsifrovizatsii kriminalistiki // Lex russica (Russkiy zakon). — 2023. — № 3. — S. 100–109.