МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЛГОГРАДСКАЯ АКАДЕМИЯ

Я. А. Климова

ОРГАНИЗАЦИОННО-ТАКТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Монография

Волгоград
ВА МВД России
2025

УДК 343.98
ББК 67.523
К 49

Одобрено
редакционно-издательским советом
Волгоградской академии МВД России

Климова, Я. А.

К 49 Организационно-тактическое обеспечение расследования преступлений в условиях цифровизации : монография / Я. А. Климова. – Волгоград : ВА МВД России, 2025. – 128 с.

ISBN 978-5-7899-1609-4

В монографии рассмотрены вопросы теории и практики расследования преступлений в условиях цифровизации. Систематизированы современные тенденции организационно-тактического обеспечения расследования. Раскрыты сущность и содержание цифровой криминалистики, сформулировано ее определение, произведен анализ перспектив использования ее возможностей. Особое внимание уделено актуальным вопросам тактики производства отдельных следственных действий в условиях цифровизации, предложены дополнения, внесение которых в действующее законодательство позволит уточнить, конкретизировать важнейшие понятия, связанные с перспективами совершенствования юридической науки и практики.

Издание предназначено курсантам, слушателям, адъюнктам и педагогическим работникам образовательных организаций системы МВД России, сотрудникам органов внутренних дел Российской Федерации.

УДК 343.98
ББК 67.523

Рецензенты: начальник кафедры криминалистики и оперативно-разыскной деятельности Ростовского юридического института МВД России доктор юридических наук, профессор, заслуженный деятель науки РФ *А. В. Варданян*; профессор кафедры оперативно-разыскной деятельности ОВД учебно-научного комплекса противодействия экономическим и налоговым преступлениям Нижегородской академии МВД России доктор юридических наук, профессор *В. И. Шаров;* начальник Волгоградского ЛУ МВД России на транспорте *Т. К. Гасанов*.

ISBN 978-5-7899-1609-4

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования обусловлена тем, что в настоящее время цифровизация, развитие информационно-телекоммуникационных технологий, внедрение технологий искусственного интеллекта входят в число приоритетных направлений стратегического развития внутренней политики России. Это определяет необходимость создания соответствующей нормативной правовой базы, регламентирующей и охраняющей рассматриваемую сферу общественных отношений, являющихся для современного общества относительно новым явлением. Сложившаяся общественная ситуация обусловила повышенный спрос на современные информационные технологии, возросло и число преступлений, совершенных с их использованием. Современные технологии проникли практически во все сферы нашей жизни, и остро актуализировалась необходимость их цифровизации. Увеличилась популярность различных информационных систем, технологий, стали более востребованными интернет-магазины и онлайн-оплата, электронные способы получения государственных и муниципальных услуг, использование виртуального пространства и IT-технологий стало массовым. Указанные факторы в целом обусловливают тенденцию увеличения количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Анализ статистических данных позволяет выявить стабильный рост преступности данного вида. Так, согласно материалам официальной статистики, в 2018 г. зарегистрировано 174 674 преступления, совершенных с использованием информационно-телекоммуникационных технологий. В 2019 г. правоохранительными органами Российской Федерации зафиксировано уже 294 409 подобных общественно опасных деяний. Условия пандемии спровоцировали резкий скачок роста преступности в сфере высоких технологий: с января по декабрь 2020 г. зарегистрировано 510 400 преступлений рассматриваемой категории[1]. В 2021 г. число преступлений, совершенных с помощью информационных технологий, возросло до 517 700. В 2022 г. среди всех зарегистрированных преступлений к таковым

[1] См.: Официальная статистика // Генеральная прокуратура Российской Федерации: офиц. сайт. URL: http://crimestat.ru/analytics (дата обращения: 25.03.2025).

относится каждое четвертое (522 100 преступлений)[1]. Согласно статистическим данным, в 2023 г. с использованием информационно-телекоммуникационных технологий совершено уже 676 951 преступление, то есть каждое третье из всех. На 30,7 % возросло число зарегистрированных киберпреступлений[2].

Тенденция стабильной прогрессии роста количества высокотехнологичных преступлений сохранилась и в 2024 г.: за период с января по октябрь более трети преступлений было совершено с использованием информационно-телекоммуникационных технологий (зарегистрировано 643 142 таких деяния), что на 14,6 % превышает показатели аналогичного периода предыдущего года. Зафиксировано увеличение удельного веса преступлений рассматриваемой категории в общей структуре преступности с 33,9 % до 39,8 %. Вместе с тем следует отдельно подчеркнуть низкую раскрываемость указанных преступлений: она составляет всего 25 %[3].

Данные статистики свидетельствуют о более чем значительном количестве преступлений, при совершении которых использовались информационно-телекоммуникационные технологии, о высоком уровне опасности, которую они представляют для общества, и наличии проблем в их раскрытии и расследовании. Полагаем, что это обусловлено постоянным развитием и обновлением способов совершения таких преступлений. В силу как объективных, так и субъективных причин вероятность их расследования является очень низкой. Положительное влияние на качество расследования преступлений рассматриваемой категории может оказать выработка научно обоснованных рекомендаций и их применение в практической деятельности органов предварительного расследования.

Об актуальности и значимости исследуемой проблемы свидетельствует внимание к ней на самом высоком государственном

---

[1] См.: Портал правовой статистики // Генеральная прокуратура Российской Федерации: офиц. сайт. URL: http://crimestat.ru/analytics (дата обращения: 12.04.2025); Статистические сведения МВД о состоянии преступности за девять месяцев 2023 года // МВД России: офиц. сайт. URL: https://xn--b1aew.xn--p1ai/news/item/42987324/ (дата обращения: 30.05.2025).

[2] См.: Состояние преступности в России за 2023 год. URL: file:///C:/Users/HOME/Downloads/Sbornik_23_12.pdf (дата обращения: 02.06.2025).

[3] См.: Состояние преступности в России за январь – октябрь 2024 года. URL: file:///C:/Users/HOME/Downloads/Sbornik_2410_UOS.pdf (дата обращения: 03.05.2025).

уровне. Так, В. В. Путин в выступлении, состоявшемся в рамках проведения ежегодного расширенного заседания коллегии МВД России 3 марта 2021 г., подчеркнул важность активной работы правоохранительных органов по борьбе с преступлениями в сфере информационных технологий, поскольку их количество выросло более чем в десять раз за последние шесть лет[1]. Кроме того, на расширенном заседании коллегии МВД России, состоявшемся 17 февраля 2022 г., глава государства снова обратил внимание на непрекращающийся рост числа преступлений в сфере информационных технологий и телекоммуникаций и – с учетом стремительного развития кибертехнологий – призвал правоохранительные органы действовать на опережение путем обновления нормативной базы и укрепления технических возможностей МВД, чтобы не позволять преступникам паразитировать на технологическом прогрессе[2]. «В ближайшие десять лет в стране необходимо массово внедрить искусственный интеллект в различные сферы жизнедеятельности и обновить стратегии цифровой трансформации во всех сферах», – заявил Президент России на Международной конференции «Путешествие в мир искусственного интеллекта» 24 ноября 2022 г.[3]

На заседании Международной конференции по искусственному интеллекту и машинному обучению Artificial Intelligence Journey 2023, состоявшемся 24 ноября 2023 г., глава государства снова сделал акцент на необходимости применения современных технологий: «Это вообще новая страница в развитии человечества… это новое качество жизни и новые возможности для профессиональной деятельности».[4]

В ходе Прямой линии в рамках мероприятия «Итоги года с Владимиром Путиным – 2023», проходившего 14 декабря 2023 г., к Президенту России с вопросом обратился «цифровой двойник»,

---

[1] См.: Путин отметил рост числа преступлений в IT-сфере. URL: https://ria.ru/20210303/prestupleniya-1599747056.html (дата обращения: 29.05.2025).

[2] См.: Расширенное заседание коллегии МВД России в 2022 году. URL: http://kremlin.ru/events/president/news/67795 (дата обращения: 02.06.2025).

[3] Путин призвал обеспечить массовое внедрение искусственного интеллекта. URL: https://ria.ru/20221124/intellekt-1833975245.html (дата обращения: 24.03.2025).

[4] Международная конференция по искусственному интеллекту и машинному обучению «Artificial Intelligence Journey 2023». URL: http://kremlin.ru/events/president/news/72811 (дата обращения: 06.06.2025).

созданный с использованием технологии дипфейк (рис. 1). После этого российский лидер подчеркнул, что предотвратить развитие искусственного интеллекта невозможно, а значит, нужно стремиться быть лидерами в этом направлении.[1]

Рис. 1. Президенту РФ Владимиру Путину в ходе Прямой линии задал вопрос его цифровой двойник[2]

В своем выступлении на пленарной сессии XXI ежегодного международного дискуссионного клуба «Валдай» в ноябре 2024 г. Президент еще раз подчеркнул, что искусственный интеллект является важнейшим инструментом развития и одним из приоритетных направлений для России[3].

Сказанное выше и анализ современной общественной ситуации убеждают в том, что в условиях складывающихся мировых тенденций и продолжающегося реформирования российского уголовного судопроизводства все более актуальной становится проблема использования возможностей цифровой криминалистики при разработке рекомендаций, способствующих эффективному и качественному

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

[2] «Это мой первый двойник»: студент СПбГУ скопировал речь и внешность Путина через нейросети и задал вопрос президенту на Итогах года. URL: https://www.spb.kp.ru/daily/27594/4866167 (дата обращения: 29.05.2025).

[3] См.: Заседание дискуссионного клуба «Валдай». URL: http://kremlin.ru/events/president/news/75521 (дата обращения: 07.04.2025).

расследованию преступлений, совершенных с использованием современных информационно-телекоммуникационных технологий. Этим определяются *практическая значимость* и *теоретическая актуальность* проблематики настоящей монографии.

Объект исследования – совокупность правоотношений, складывающихся в процессе расследования преступлений в условиях цифровизации, а также систематизация сведений о современном состоянии расследования преступлений.

Предмет исследования – организационные основы и правовое регулирование осуществления деятельности по расследованию преступлений в условиях цифровизации, практика ее применения, а также пути повышения эффективности расследования преступлений.

Цель исследования: разработать обоснованные рекомендации по оптимизации организационно-тактического обеспечения расследования преступлений с учетом анализа соответствующих современных возможностей в условиях цифровизации.

Задачи исследования:

– проанализировать перспективы цифровой криминалистики;

– систематизировать информацию о современных технико-криминалистических средствах;

– разработать тактические рекомендации по производству отдельных следственных действий с учетом интеграции цифровых технологий.

Нормативную базу исследования образуют связанные с его тематикой положения международных нормативных правовых актов, Конституция Российской Федерации, действующее уголовное и уголовно-процессуальное законодательство России, ряд федеральных законов: № 3-ФЗ от 7 февраля 2011 г. «О полиции», № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации», № 126-ФЗ от 7 июля 2003 г. «О связи», Указ Президента Российской Федерации № 400 от 2 июля 2021 г. «О Стратегии национальной безопасности Российской Федерации», Указ Президента Российской Федерации от 15 февраля 2024 г. № 124 «О внесении изменений в Указ Президента Российской Федерации от 10 октября 2019 г. № 490 “О развитии искусственного интеллекта в Российской Федерации” и в Национальную стратегию, утвер-

жденную этим Указом», постановления Конституционного Суда РФ и Пленума Верховного Суда РФ, иные нормативные правовые акты, регламентирующие вопросы исследуемой проблематики.

Научная новизна заключается в систематизации и анализе деятельности по расследованию преступлений в условиях цифровизации, разработке научно обоснованных рекомендаций, применение которых способно обеспечить повышение эффективности деятельности органов предварительного расследования по уголовным делам о преступлениях, совершенных с использованием современных информационно-коммуникационных технологий.

ГЛАВА 1. ПОНЯТИЕ И ПЕРСПЕКТИВЫ ЦИФРОВОЙ КРИМИНАЛИСТИКИ

В настоящее время назрела необходимость активного освоения криминалистической наукой «продуктов» глобальной цифровизации – основной тенденции развития современного общества. Об актуальности обращения к исследуемой проблеме свидетельствует тот факт, что цифровизация проникает во все сферы общественных отношений, делая привычным использование различных современных информационно-коммуникационных (далее также – IT) технологий в повседневной жизни.

Достижению указанной цели способствует создание и планомерная реализация национальной программы «Цифровая экономика Российской Федерации», действовавшей до конца 2024 г., и пришедшего ей на смену проекта «Экономика данных и цифровая трансформация государства», являющегося логичным продолжением последовательной политики государства.

В рамках нацпрограмм активно рассматриваются законопроекты, направленные на урегулирование различных правоотношений, возникающих в связи с цифровой трансформацией общества.

Реализующийся проект «Искусственный интеллект» обеспечит внедрение ИИ-сервисов во все отрасли жизни и работу всех сфер гражданского общества по новым принципам за счет создания инфраструктуры вычисления и хранения данных.

Федеральный проект «Цифровое государственное управление» будет осуществлять перевод госуслуг в онлайн-формат, производить запуск и поддержку государственных сайтов и приложений.

Проект «Отечественные решения» поможет операторам связи перейти на российские базовые станции.

Проект «Прикладные исследования и перспективные разработки» поддержит развитие сетей связи.

Проект «Инфраструктура кибербезопасности» будет отвечать задачам разработки онлайн-платформы, предоставляющей возможность обмена данными для борьбы с мошенниками и DDoS-атаками.

Такое внимание со стороны государства к одной из наиболее острых проблем современности подчеркивает колоссальную важность интеграции IT-технологий в правоохранительную деятельность

и, в свою очередь, ставит перед общественными науками, в том числе криминалистикой, ряд новых задач.

Цифровизация, выступающая в роли главного драйвера трансформации общества, способствует повышению популярности различных информационных систем в целом, что обусловливает и развитие современного преступного тренда – увеличения количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Криминалистическая наука, способная на современном этапе оперативно внедрять новейшие достижения научно-технического прогресса и реагировать на происходящие инновационные изменения в обществе, должна находиться в авангарде борьбы с преступностью.

Считаем правильным присоединиться к мнению известного отечественного ученого-криминалиста Р. С. Белкина, который еще четверть века назад четко подметил значение использования достижений научно-технического прогресса для ускорения развития криминалистики, повышения ее научного потенциала и общественной значимости в связи с растущей актуальностью борьбы с преступностью[1].

Опираясь на данные судебно-следственной практики, мы можем констатировать, что для раскрытия и расследования преступлений правоохранительные органы широко используют фотографии и видеозаписи, сделанные с помощью цифровых фото- и видеокамер, установленных в помещениях банков, магазинов, а также на городских улицах, а в следственно-криминалистической практике все чаще применяются цифровые способы фиксации следов преступления, моделирования внешности преступника и поиска информации, относящейся к событию преступления.

Однако тот эффект, который может быть получен в результате применения указанных средств, пока не достигнут. Полагаем, что одной из основных причин этого является правовая неопределенность норм, регулирующих использование цифровой информации в доказывании по уголовным делам.

---

[1] См.: Белкин Р. С. Курс криминалистики: учеб. пособие для вузов. 3-е изд., доп. М.: Юнити-Дана: Закон и право, 2001. С. 98.

Анализ научной литературы и судебной практики позволяет сделать вывод о высокой степени интереса ученых к рассматриваемой проблематике.

Особенности расследования преступлений в условиях информационно-технологического развития общества рассматривались в работах ученых-криминалистов А. А. Бессонова, В. Б. Вехова, С. В. Зуева, Е. П. Ищенко, П. С. Пастухова, Е. Р. Россинской, А. Б. Смушкина и др.

Различные аспекты уголовно-процессуальной регламентации цифровых доказательств анализировались в недавних трудах А. И. Зазулина (2018 г.), А. А. Балашовой (2020 г.), О. А. Ефремовой (2021 г.), В. С. Черкасова (2022 г.).

Криминалистические аспекты расследования преступлений и использования искусственного интеллекта в противоправной деятельности исследовались Д. В. Бахтеевым, Д. С. Клюевым, Ю. В. Соколовой, С. Е. Платоновым, Е. Л. Лужинской, О. В. Расторопова, В. А. Чванкиным и др.[1]

В последние годы опубликованы диссертационные исследования, посвященные вопросам интеграции технологий в практическую деятельность (Д. В. Бахтеев, 2022 г.), использования криминалистических знаний в верификации копий материально-фиксированных следов-отображений (М. Г. Мусаэлян, 2023 г.), модернизации криминалистических положений по использованию цифровых доказательств (Х. Х. Рамалданов, 2024 г.).

Перечисленные исследования внесли значительный вклад в развитие криминалистической науки и позволили существенно продвинуться в понимании отдельных аспектов расследования преступлений в условиях цифровизации. Вместе с тем большинство

[1] См.: Бахтеев Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования // Уголовный процесс и криминалистика. 2018. № 2. С. 43–49; Анализ возможностей искусственного интеллекта для расследования мошенничества / Д. С. Клюев, А. Б. Смушкин, Ю. В. Соколова, С. Е. Платонов // Физика волновых процессов и радиотехнические системы. 2023. Т. 26, № 3. С. 116–122; 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; Расторопова О. В. Противодействие использованию искусственного интеллекта в преступных целях // Вестник Университета прокуратуры Российской Федерации. 2021. № 4 (84). С. 52–58.

ученых-криминалистов затрагивают частные случаи применения возможностей цифровизации в процессе расследования преступлений. В то же время эти работы не являются исчерпывающими при исследовании всех проблем, касающихся возможностей и перспектив внедрения цифровых технологий в деятельность по расследованию преступлений, следовательно, требуется новое комплексное исследование в этой сфере.

Данные статистики свидетельствуют о более чем значительном увеличении количества преступлений, совершенных с использованием информационно-телекоммуникационных технологий (рис. 2).

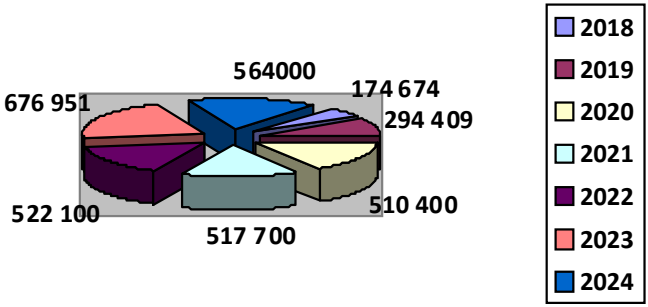


Рис. 2. Статистические данные правоохранительных органов Российской Федерации о количестве преступлений, совершенных с использованием информационно-телекоммуникационных технологий за 2018–2024 гг.[1]

[1] См.: Портал правовой статистики // Генеральная прокуратура Российской Федерации: офиц. сайт. URL: http://crimestat.ru/analytics (дата обращения: 12.04.2025); Статистические сведения МВД о состоянии преступности за девять месяцев 2023 года // МВД Российской Федерации: офиц. сайт. URL: https://xn--b1aew.xn--p1ai/news/item/42987324/ (дата обращения: 30.05.2025); Состояние преступности в России за 2023 год. URL: file:///C:/Users/HOME/Downloads/ Sbornik_23_12.pdf (дата обращения: 02.06.2025); Состояние преступности в России за январь – октябрь 2024 года. URL: file:///C:/Users/HOME/Downloads/ Sbornik_2410_UOS.pdf (дата обращения: 03.05.2025).

В связи с изложенным необыкновенную актуальность приобрела проблема поиска эффективных методов и средств выявления, раскрытия и расследования преступлений, совершенных с использованием IT-технологий, что обусловило возникновение и развитие нового вектора криминалистической науки.

Среди ученых-криминалистов и практиков ведется острая дискуссия о дефиниции исследуемого криминалистического направления. Так, В. Б. Вехов считает правильным название «электронная криминалистика», под которой он понимает систему научных положений, являющихся основой для разработки технических средств, приемов, методик и рекомендаций по собиранию, исследованию и использованию компьютерной информации, средств ее обработки и защиты в целях раскрытия, расследования и предупреждения преступлений[1].

И. В. Медведев предлагает название «форензика», подразумевая, что форензика «отвечает» за сбор, исследование и оценку следов преступлений в компьютерной области[2]. Схожего мнения придерживаются Н. В. Шухова и А. Л. Снигирев[3].

Иную точку зрения имеет П. С. Пастухов, считающий точным название «компьютерная криминалистика» и включающий в функции этой отрасли изучение особенностей сбора, сохранения, анализа и представления данных, имеющих отношение к любым компьютерным средствам, мобильным телефонам и другим устройствам, осуществляющим фиксацию информации в цифровой форме[4].

М. А. Романенко предлагает ввести термин «судебная дигитология», обосновывая это необходимостью разработки знаний о сборе, закреплении (фиксации) и исследовании электронно-цифровых уст-

---

[1] См.: Вехов В. Б., Пастухов П. С. Формирование стратегий расследования преступлений на основе положений электронной криминалистики // Ex jure. 2019. № 4. С. 129.

[2] См.: Медведев И. В. Компьютерная криминалистика «Форензика» и киберпреступность в России // Пролог: журнал о праве. 2013. № 3. С. 66.

[3] См.: Шухова Н. В., Снигирев А. Л. О роли форензики в криминалистическом обеспечении расследования преступлений // Информатизация и информационная безопасность правоохранительных органов: сб. тр. XX Междунар. науч. конф. М., 2011. С. 331–332.

[4] См.: Пастухов П. С. О необходимости развития компьютерной криминалистики // Пермский юридический альманах. 2018. № 1. С. 453.

ройств, программ и явлений, в основе функционирования которых лежат объективно выраженные вычислительные процессы[1].

А. Б. Смушкин считает, что наиболее точным является определение «электронная цифровая криминалистика». Так характеризуется концепция собирания, исследования и использования электронной цифровой информации и информационно-технологических устройств[2].

Интерес представляет мнение Е. Р. Россинской, предлагающей более фундаментальную разработку – «теорию информационно-компьютерного обеспечения криминалистической деятельности», позволяющую совершенствовать существующие разделы криминалистики: технику, тактику и методику[3].

Считаем правильным присоединиться к мнению, высказанному Е. П. Ищенко, полагающему, что максимально полно отражающим содержание особенностей расследования преступлений, совершаемых в сфере информационных и коммуникационных технологий, является термин «цифровая криминалистика»[4].

В работах Л. А. Спектор и А. Д. Малютина с определенной долей условности выделены основные предпосылки возникновения цифровой криминалистики:

1. Появление и развитие кибернетического пространства, которое по сути является новой специфической средой, где множество современных людей осуществляют свою активную деятельность.

2. Возникновение новых «виртуальных» правоотношений, не имеющих аналогов в классической правовой регламентации.

---

[1] См.: Романенко М. А. Новый подход к содержанию системы криминалистической техники // Вестник Пермского университета. Серия «Юрид. науки». 2008. № 2. С. 117.

[2] См.: Смушкин А. Б. Цели, задачи и функции электронной цифровой криминалистики // Криминалистика: вчера, сегодня, завтра. 2020. № 1 (13). С. 107.

[3] См.: Россинская Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 194.

[4] См.: Ищенко Е. П. У истоков цифровой криминалистики // Вестник Университета имени О. Е. Кутафина. 2019. № 3 (55). С. 15.

3. Зарождение киберпреступности, появление новых механизмов, способов совершения преступления в киберпространстве[1].

Такой плюрализм мнений, возникший при определении понятия и содержания нового криминалистического знания, свидетельствует о сложности и малой изученности явления. Каждое из приведенных определений отражает только одну (или некоторые) из сторон изучаемого феномена.

Но объединяет ученых-криминалистов взгляд на дефиницию именно с точки зрения криминалистической деятельности, осуществляемой при производстве правоохранительными органами расследования в отношении преимущественно киберпреступлений.

Полагаем, что такая позиция не совсем верна, поскольку инструментарий цифровой криминалистики, как видится нам, целесообразно использовать не только при расследовании высокотехнологичных преступлений, но и в ходе осуществления уголовного судопроизводства по «традиционным» уголовным делам.

Разрешение этой острой дискуссии имеет принципиальное значение для дальнейшего осмысления сути деятельности правомочных субъектов расследования, осуществляемой в рамках цифровой криминалистики.

Исходя из логики исследования, необходимо дать определение рассматриваемому понятию. Полагаем, что **под *цифровой криминалистикой* следует понимать, с одной стороны, систему научных положений, изучающих закономерности возникновения цифровых следов, отражающих механизм совершения преступлений с использованием информационно-телекоммуникационных технологий, а также возможности адаптации традиционных методов для обнаружения цифровых следов и доказательств, особенности фиксации и изъятия цифровых доказательств, их использование в выявлении, раскрытии и расследовании различных видов и групп преступлений; с другой – целесообразно рассматривать ее в качестве надстройки над традиционными разделами криминалистики, нового витка развития всей криминалистической науки, концепции, ориентированной на циф-**

[1] См.: Спектор Л. А., Малютин А. Д. Цифровая криминалистика в условиях компьютеризации современного общества // Вестник Алтайской академии экономики и права. 2022. № 9 (ч. 1) С. 159–164.

ровую трансформацию всего процесса расследования, в том числе деятельности по собиранию, фиксации и исследованию криминалистически значимой информации с помощью не только «устоявшихся» средств и методов, но и новых современных технологий.

Переходя к вопросу о методологической основе цифровой криминалистики, приведем справедливые доводы В. Б. Вехова и С. В. Зуева, которые считают, что учение, посвященное рассматриваемому явлению, обладает своими специальными методами[1]. К таковым можно отнести следующие:

1. Собственно-криминалистические, состоящие из технико-криминалистических и структурно-криминалистических. Если первые определяют способы работы в условиях цифровизации с различными материальными следами, обладающими криминалистически значимой информацией (например, применение цифровых сканеров – устройств считывания информации кожного покрова рук человека[2], баллистическое исследование огнестрельного оружия, изготовленного с использованием аддитивных технологий[3], биометрические исследования в габитоскопии), то вторые содержат рекомендации по целесообразному использованию современных технологий при производстве отдельных следственных действий.

2. Методы обнаружения, изъятия, фиксации, предварительного исследования цифровых следов-доказательств.

3. Методы криминалистического компьютерного моделирования (например, воссоздание последовательности образования следов или механизма совершения преступления).

4. Методы цифрового сканирования и 3D-фиксации следовой картины на месте происшествия (в том числе с целью визуализации).

5. Методы искусственного интеллекта (рис. 3).

---

[1] См.: Цифровая криминалистика: учебник для вузов / под ред. В. Б. Вехова, С. В. Зуева. 2-е изд., перераб и доп. М.: Юрайт, 2024. С. 22–25.

[2] См.: Яровенко В. В., Пяткова О. В., Чередниченко А. В. Применение цифровых технологий в дактилоскопии (переход на создание, хранение и исследование материалов в электронном формате) // Юридические исследования. 2022. № 2. С. 55.

[3] См.: Четвергов М. А. Компетентность эксперта-баллиста при исследовании объектов, изготовленных с применением современных технологий // Криминологический журнал. 2024. № 1. С. 187.

Рис. 3. Классификация методов искусственного интеллекта

Таким образом, инструментарий цифровой криминалистики включает совокупность различных методов и средств, помогающих собирать и исследовать криминалистически значимую информацию с целью дальнейшего использования ее в качестве доказательств по уголовному делу, а также способствующих более эффективному расследованию преступлений.

По нашему мнению, в структуре цифровой криминалистики можно выделить несколько взаимосвязанных и взаимодополняющих направлений в зависимости от конкретного предмета исследования:

1. Исследование различных устройств – носителей электронной информации с целью получения цифровых доказательств и установления механизма следообразования (компьютеров, планшетов, смартфонов и других девайсов, гаджетов, внешних съемных запоминающих устройств, беспилотных воздушных судов, видеорегистраторов и т. д.).

2. Исследование сетевых устройств для установления следовой картины (маршрутизаторов, серверов, межсетевых экранов (файрволов) и т. д.).

3. Исследование различных баз данных с целью получения информации о личности преступника, потерпевшего, об их финансовых потоках, медицинских записях и т. д.

4. «Облачные» исследования (изучение данных, находящихся в облачных хранилищах, виртуальных машинах, на удаленных рабочих столах и т. д.).

5. Исследование IoT-устройств (интернет вещей), позволяющее получать и анализировать данные с устройств, входящих в «Умный дом».

6. Исследование мультимедийных данных: аудио-, видео-, фотоизображений, в том числе дипфейков.

7. Исследование киберпространства.

Кроме этого, интерес представляет перспектива использования в качестве инструментария цифровой криминалистики LegalTech – межотраслевой способ цифровой трансформации, находящийся на стыке юриспруденции и IT. В широком смысле дефиницию следует рассматривать как концепцию внедрения различных современных технологий в практическую деятельность с целью оптимизации последней (рис. 4)[1].

В традиционном понимании LegalTech – класс цифровых продуктов, прежде всего программного обеспечения, направленного на автоматизацию деятельности юристов (например, базы нормативно-правовых актов и судебных актов)[2].

Полагаем, что применительно для сферы правоохранительной деятельности следует в широком смысле понимать LegalTech как любое программное обеспечение – и специализированное, и неспециализированное, которое потенциально может быть использовано для повышения эффективности расследования преступлений при выполнении следующих функций:

– поиска, анализа и обобщения юридической информации;

– составления предиктивной аналитики;

– создания документов (например, использование бланков процессуальных документов в виде конструкторов позволит минимизировать ошибки технического характера и заметно упростит работу следователей).

---

[1] См.: Карта LegalTech России. URL: https://legaltechmap.ru/ (дата обращения: 21.05.2025).

[2] См.: Что юристу нужно знать о LegalTech. URL: https://www.law.ru/article/27878-chto-yuristu-nujno-znat-o-legaltech-produkty-primery-obuchenie (дата обращения: 21.05.2025).

Рис. 4. Карта LegalTech России

Исследованные нами теоретические аспекты цифровой криминалистики необходимы для дальнейшего рассмотрения перспектив интеграции современных информационных технологий в процесс расследования преступлений.

ГЛАВА 2. СПЕЦИФИКА ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Понятие «трансформации в условиях цифровизации» применительно к технико-криминалистическому обеспечению расследования преступлений следует рассматривать в трех значениях:

1) в историческом аспекте – как формирование, становление и эволюцию технико-криминалистических средств на различных этапах цифровизации в течение продолжительного временного отрезка;

2) с функциональной точки зрения – как изменение функциональной направленности криминалистической деятельности посредством изменения объема полномочий, реализуемых лицами, осуществляющими собирание следов – в зависимости от конкретных следственных действий и этапа расследования, на котором они производятся;

3) в перспективном аспекте – как объективную потребность внедрения современных технологий в процесс расследования с учетом динамично реформирующегося уголовно-процессуального законодательства и совершенствования криминалистической науки, а также появления новых высокотехнологичных способов совершения преступлений.

Следует согласиться с мнением И. И. Литвина, обосновывающего тезис о том, что использование современных технологий в качестве технико-криминалистических средств при проведении следственных и других процессуальных действий с целью получения доказательств, соответствующих всем требованиям уголовно-процессуального законодательства, детерминировано их способностью объективно фиксировать, хранить и воспроизводить криминалистически значимую информацию, необходимую для разрешения дела. Однако эти вопросы либо вообще не урегулированы в Уголовно-процессуальном кодексе Российской Федерации (далее –

УПК РФ), либо их регулирование несовершенно и не принимает во внимание последние достижения науки и техники[1].

Для уяснения специфики технико-криминалистического обеспечения расследования преступлений необходимо рассмотреть подробнее сам термин.

Представляется правильным вывод, сделанный Т. Ф. Дмитриевой, об отсутствии единого мнения в криминалистической литературе относительно таких понятий, как «технические средства», «специальные технические средства», «научно-технические средства», «криминалистическая техника» и «технико-криминалистические средства», которые зачастую отождествляются[2].

С точки зрения, доминирующей среди ученых-криминалистов, технические средства, которые используются при проведении следственных действий, целесообразно определять как «научно-технические средства» (Г. И. Грамович, С. Д. Цомая, В. Г. Болычев) либо как «технико-криминалистические средства» (Р. С. Белкин, Т. В. Аверьянова, П. Т. Скорченко).

Однако, несмотря на тесную взаимосвязь уголовно-процессуального права и криминалистики, законодатель отдает предпочтение дефиниции «технические средства».

Мы не склонны считать эту позицию верной, поскольку полагаем, что технико-криминалистические средства следует рассматривать в самом широком смысле как обобщающее понятие, охватывающее весь спектр инструментов и методов, используемых в криминалистике, и включающее целый комплекс заимствованных, адаптированных и специально разработанных криминалистической наукой технических средств, приспособлений, приборов, инструментов, веществ и материалов, а также рекомендаций, приемов и способов, используемых для противодействия преступности в процессе собирания, закрепления, фиксации, исследования и последующей демонстрации доказательств.

---

[1] См.: Литвин И. И. Современные технические средства и проблемы их применения в доказывании на досудебных стадиях уголовного судопроизводства: автореф. дис. … канд. юрид. наук: 12.00.09. Екатеринбург, 2018. С. 3–4.

[2] См.: Дмитриева Т. Ф. О соотношении понятий «Технико-криминалистические средства» и «Научно-технические средства» // Вестник Полоцкого государственного университета. Серия D. Экономические и юридические науки. 2013. № 5. С. 191–197.

Полагаем, что к технико-криминалистическому обеспечению расследования преступлений в условиях цифровизации следует относить и возможности цифровой дактилоскопии, аудиоцифрования, баллистического моделирования и др. Считаем целесообразным при производстве следственных действий помимо традиционных технико-криминалистических средств применять GPS-информаторы, ГЛОНАСС, геолокаторы, мобильные графические редакторы, лазерные дальномеры, навигаторы, беспилотные воздушные суда, 360-градусные камеры (снимают сферическое изображение во всех направлениях одновременно для записи панорамных фото и видео и обладают такими преимуществами, как отличная стабилизация, отсутствие «слепых зон»), 3D-сканеры и 3D-принтеры, VR-технологии.

Перспективным направлением развития технико-криминалистического обеспечения расследования преступлений в условиях цифровизации является, по нашему мнению, интеграция в процесс расследования сквозных IT-технологий (табл. 1).

Таблица 1

Перспективные сквозные технологии		
Digital identity создание цифрового профиля человека	Искусственный интеллект, нейротехнологии, *LLM*	*BigData* (большие данные)
Internet of things (интернет вещей)	*SmartContract* (создание протоколов коммуникации, не требующих априорного доверия между сторонами)	*Blockchain* (блокчейн) – системы распределенного реестра

Перспективные сквозные технологии		
Digital Signature (цифровая подпись)	Иммерсивные технологии – совокупность *AR* (дополненной реальности), *VR* (виртуальной реальности) и *XR* (расширенной реальности)	Цифровая сенсорика

В справедливости данного предположения убеждает следующее: в государственной национальной программе «Цифровая экономика Российской Федерации» обеспечение ускоренного внедрения цифровых технологий в различные сферы жизнедеятельности общества закреплено как основная задача развития государства[1]. В качестве сквозных цифровых технологий предусмотрены нейротехнологии и искусственный интеллект, робототехника, и особо оговаривается необходимость системного нормативно-правового обеспечения применения цифровых технологий.

Рассмотрим некоторые возможности их использования в криминалистике. Так, в настоящее время разрабатывается программное обеспечение Crimeserieslinkage, предназначенное для выявления серийных преступлений и преступников[2]. Оно уже зарегистрировано в реестре программ для ЭВМ[3]. Ожидается, что благодаря привлечению к расследованию больших данных и нейронных сетей эта система сможет определять личность преступника (пол, возраст, социальный статус, наличие судимостей и т. д.) на основе информа-

[1] См.: О национальных целях развития Российской Федерации на период до 2030 года: указ Президента РФ от 21 июля 2020 г. № 474 // КонсультантПлюс: справ.-правовая сист. URL: https://www.consultant.ru/document/cons_doc_LAW_357927/ (дата обращения: 17.06.2025).

[2] См.: Интервью руководителя Главного управления криминалистики Следственного комитета Российской Федерации З. З. Ложиса. URL: https://sledcom.ru/search?q=+crimeserieslinkage (дата обращения: 29.05.2025).

[3] См.: Федеральный институт промышленной собственности (ФИПС): офиц. сайт. URL: https://new.fips.ru/registers-web/action?acName=clickTree&nodeId=1977&maxLevel=1 (дата обращения: 29.05.2025).

ции о лицах, совершивших более одной тысячи серийных преступлений.

Еще одна перспективная технология для интеграции в процесс расследования – BigData. В современном цифровом мире весьма значителен объем криминалистически значимой информации, которая находится в разных форматах и источниках. Благодаря технологии BigData можно будет упорядочить, проанализировать и получить информацию, важную для быстрого и эффективного расследования уголовных дел.

Работа с цифровым профилем человека в сфере цифровой криминалистики также весьма перспективна. В рамках национального проекта «Цифровая экономика Российской Федерации» планируется создание единой системы идентификации и аутентификации, включающей биометрическую идентификацию, облачную квалифицированную электронную подпись и цифровые профили физических и юридических лиц. Согласно закону о создании единой государственной системы данных единая биометрическая система будет переведена в статус государственной информационной системы. Таким образом, использование ее данных и интернета вещей позволит отслеживать объекты или типы информации в пространстве и времени в криминалистических целях.

Интерес представляет развитие такого направления, как блокчейн-криминалистика, цель которого можно определить так: криминалистический анализ сервисов смешивания биткойнов (биткойн-миксеров) и разработка способов и методов деанонимизации преступников. Следует согласиться с мнением А. В. Подобных и Н. В. Мануйловой, полагающих, что в ближайшем будущем появятся криминалистические инструменты с применением поддельных нод (промежуточных узлов) Tor (The Onion Router) и дистанционным сбором информации с хостов и облачных ресурсов для нужд криминалистической экспертизы[1].

[1] См.: Подобных А. В. Биткойн-криминалистика для деанонимизации криптомиксеров и транзакций CoinJoin // Информационная безопасность. 2022. № 5. С. 44–45; Подобных А. В., Мануйлова Н. В. Цифровая криминалистика распределенных реестров: учебно-методическое пособие. СПб.: Самиздат (ЛитРес), 2024. С. 3.

Считаем, что использование искусственного интеллекта в качестве инструмента цифровой криминалистики открывает широкие перспективы для деятельности специалистов в сфере эффективного и качественного раскрытия и расследования современных преступлений. Важно отметить, что различные информационные технологии, включая искусственный интеллект, активно разрабатываются в течение последних лет, и в прошлом году этот сектор стал одним из наиболее инвестируемых. Актуальность нашего исследования также обусловлена повышенным – в последнее время – вниманием законодателей и ученых-криминалистов к технологиям искусственного интеллекта[1].

По этому поводу интересное мнение высказывает Д. В. Бахтеев, считающий, что криминалистика всегда была чувствительна к технологиям, потенциально полезным для расследования и раскрытия преступлений, поэтому изучение возможностей искусственного интеллекта должно представлять для нее интерес[2].

Мониторинг глобальных тенденций цифровизации за последние пять лет показывает, что искусственный интеллект трижды занимал первое место по интегральному показателю, основанному на количестве научных публикаций, патентов и объеме инвестиций в эту технологию[3]. В 2019 г. принята Национальная стратегия развития искусственного интеллекта в России до 2030 г. Это одна из первых попыток законодательного регулирования развития и применения технологии[4].

Однако использование искусственного интеллекта в расследовании преступлений сегодня сталкивается с рядом проблем, вызванных наличием правовых лакун, отсутствием нормативно-правовой

---

[1] См.: Национальная стратегия развития искусственного интеллекта на период до 2030 года, утв. Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». URL: https://a-ai.ru/wp-content/uploads/2024/03/Национальная_стратегия_развития_ИИ_2024.pdf?ysclid=mcy7k7yv46402130895 (дата обращения: 17.06.2025).

[2] См.: Бахтеев Д. В. Указ. соч. С. 43.

[3] См.: Мониторинг глобальных трендов цифровизации за 2022 год // Ростелеком. 2023. URL: https://www.company.rt.ru/upload/iblock/109/rostelekom_monitoring_2022.pdf (дата обращения: 16.06.2025).

[4] См.: Национальная стратегия развития искусственного интеллекта на период до 2030 года.

базы и вопросами этических норм. Для устранения перечисленных проблем необходимо разработать и усовершенствовать законодательство в этой области.

Сегодня существуют технические средства для обеспечения работы цифровой криминалистики, основанные на применении искусственного интеллекта. Например, программное обеспечение «Мобильный Криминалист», UFED и BELKASOFT EVIDENCE CENTER позволяет специалистам анализировать электронные носители информации и извлекать криминалистически значимую информацию из мобильных устройств, ноутбуков, персональных компьютеров и облачных сервисов. Искусственный интеллект помогает анализировать данные, устанавливать графы связей, распознавать тексты и лица, а также выявлять различные угрозы.

Перспективным направлением считается также интеграция нейротехнологий в процесс расследования.

В соответствии с универсальной теоремой аппроксимации любую существующую функцию можно «предсказать» с помощью нейронов. В самом широком смысле аппроксимация – это метод нахождения в целом наиболее ближнего значения, построение приближенной (аппроксимирующей) функции. В этой связи под нейронной сетью в цифровой криминалистике предлагаем понимать метод искусственного интеллекта, основанный на осуществлении глубокого обучения (Deep Learning), позволяющего обучать модель «предсказывать» результат, основываясь на наборе входных данных, путем воспроизведения работы человеческого мозга, воссоздания абстрактного мышления в программе при помощи слоев нейронов, направленный на изучение и получение информации в целях раскрытия и расследования преступлений.

Учитывая сказанное, полагаем также, что расширить возможности расследования позволит применение нейротехнологий, обозначенных в таблице 2.

Таблица 2

Нейротехнологии в процессе расследования	***Создание трехмерных сцен и 3D-панорамы из 2D-изображений*** Модель может быстро обработать несколько десятков фотографий, приняв при этом в расчет ракурсы камеры, с которых велась съемка, и затем визуализировать получившуюся 3D-сцену (например, нейросеть NeRF, приложение Luma Al). В ходе расследования такая технология позволит создавать трехмерные модели участков местности, помещений, жилищ, транспортных средств, предметов, фотографирование которых осуществлялось в ходе производства следственных действий, таких как следственный осмотр, обыск, выемка, осмотр предметов и др.)
	Редактирование людей на видео с функцией изменения эмоций, возраста, макияжа Отличие от других методов в том, что для обработки одного кадра используются изменения, которые применяли в предыдущих (есть зависимость от времени), например, генеративно-состязательная нейросеть (Generative adversarial network). Использование данной технологии позволит улучшать видео, полученное с камер видеонаблюдения, с целью установления личности либо идентификации лица, запечатленного на месте совершения преступления
	Кластеризация данных Метод можно использовать для выявления закономерностей и связей, позволяющих устанавливать людей, занимающихся преступной деятельностью (например, блокчейн-технологии, алгоритм Deep Claster), группы

Интересным может быть зарубежный опыт в рассматриваемой сфере. Так, 29-летний мужчина из китайской провинции Фуцзянь в ходе конфликта задушил свою девушку. Вспомнив, что у убитой на банковском счете были большие деньги, Чжан решил воспользоваться накоплениями. Преступник запустил банковское приложение Money Station и поднес смартфон к лицу мертвой, но алгоритмы отказались авторизовать его. Искусственный интеллект «заподозрил» неладное и «попросил» девушку подмигнуть, чего она, естественно, не сделала. В итоге убийца не смог снять деньги. Но на этом его неудачи не закончились. Программа зарегистрировала подозрительную попытку входа в систему, так как искусственный интеллект не смог найти признаков движения в глазах жертвы, и передала информацию в правоохранительные органы. Те вручную проверили данные, которые собрала программа, и увидели след от веревки на шее девушки, а также услышали вместо женского голоса мужской. До того как преступник успел сжечь тело девушки, полиция его задержала. Так искусственный интеллект помог раскрыть преступление[1].

В полиции Нидерландов заявили о запуске масштабного проекта по использованию систем искусственного интеллекта для поиска «зацепок» в нераскрытых преступлениях. С этой целью нейронная сеть сопоставит улики в уголовных делах, заведенных в течение последних 30 лет. После составления базы данных самообучающаяся нейронная сеть проанализирует информацию и попытается найти совпадения в формально не связанных между собой отчетах. Сопоставление данных из сгенерированной базы большого объема позволит полицейским получить подсказки о возможной взаимосвязи между уголовными делами, которые расследовались независимо друг от друга. Предполагается, что искусственный интеллект укажет и на возможные улики, упущенные при ведении следствия. Интеллектуальная система сможет оперировать сведениями из уже

[1] См.: South China Morning Post. URL: https://www.scmp.com/news/china/society/article/3023964/chinese-murder-suspect-caught-ai-software-spotted-dead-persons (дата обращения: 09.06.2025).

существующих баз данных, в которых хранится информация о преступниках[1].

В МВД Турции с 2022 г. успешно используется система Analiz Sistemleri Narkotik Agı (Asena) (Система анализа наркотической паутины). Система, выявляя нетипичное поведение людей, начинает отслеживать их перемещения. Анализ, сформированный путем сравнения различных данных, позволяет правоохранительным органам устанавливать торговцев наркотиками[2].

Проведенный анализ применения при расследовании преступлений технологий искусственного интеллекта позволяет объективно оценить опыт, имеющийся в других странах, и рассмотреть возможность его внедрения в отечественную практику раскрытия и расследования преступлений.

Необходимость использования таких технологий подтверждает и проведенное нами исследование, посвященное изучению перспектив использования искусственного интеллекта в профессиональной деятельности. Среди правоприменителей был проведен опрос на тему «Искусственный интеллект: помощник или конкурент?»[3]. Большинство респондентов (83,7 %) положительно оценивают перспективу применения технологий искусственного интеллекта при расследовании преступлений (рис. 5).

[1] См.: Искусственный интеллект привлекут для расследования нераскрытых преступлений. URL: https://euronus.com/news-tech/1442-iskusstvennyj-intellekt-privlekut-dlya-rassledovaniya-neraskrytykh-prestuplenij.html (дата обращения: 04.06.2025).

[2] См.: Turkey using AI software ASENA in fight against drugs. URL: https://www.hurriyetdailynews.com/turkey-using-ai-software-asena-in-fight-against-drugs-173912 (дата обращения: 15.06.2025).

[3] См.: Опрос на тему «Искусственный интеллект: помощник или конкурент?». URL: https://docs.google.com/forms/d/e/1FAIpQLSduMvdom9bGnU_AvT3q5fuoMLwTmiRrK8dbNbzF1A0EtW_PuQ/viewform?usp=sf_link (дата обращения: 01.04.2025).

Искусственный интеллект: помощник или конкурент?
118 ответов

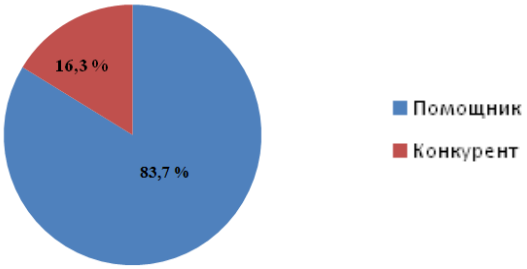


Рис. 5. Результаты опроса на тему
«Искусственный интеллект: помощник или конкурент?»

Передовыми системами искусственного интеллекта следует считать большие языковые модели (large language model, LLM) – это тип моделей глубокого обучения, предназначенных для обработки, понимания и составления текста, подобного созданному человеком. Они базируются на методах глубокого обучения и обучены на массивных наборах данных (рис. 6).

Рис. 6. Примеры больших языковых моделей
искусственного интеллекта

Так, в мае 2023 г. в ЕС был разработан первый в мире нормативно-правовой акт, регулирующий применение искусственного интеллекта (в том числе речь шла о ChatGPT и Midjourney).

Полагаем, что использование алгоритмов искусственного интеллекта призвано повысить эффективность расследования за счет сокращения времени обработки данных и оперативного получения криминалистически значимой информации.

Использование таких нейросетевых моделей в процессе расследования современных преступлений видится нам возможным прежде всего при разработке и использовании специальной архитектуры нейронной сети, направленной на выявление признаков апскейлинга (технического улучшения качества исходного контента), применения состязательно-генеративных нейросетей для создания дипфейков.

Однако в настоящее время существуют ограничения применимости моделей, вызванные целым рядом факторов (табл. 3).

Таблица 3

Ограничения применимости нейросетевых моделей		
Ограничения по объему текстовой информации	Галлюцинация моделей	Плохое состояние данных для обучения
Конфиденциальность	Обучение на неспецифической информации	Не всегда качественное состояние данных для обучения

Несмотря на значительные перспективы применения современных технологий, основанных на деятельности искусственного интеллекта, включая его использование в расследовании преступлений, быстрое развитие этой области вызывает обеспокоенность об-

щества. Широко известным стало опубликованное 28 марта 2023 г. на сайте организации Future of Life открытое письмо, под которым подписались глава Tesla, SpaceX и Twitter[1] Илон Маск, основатель Apple Стив Возняк и более тысячи экспертов в области разработки искусственного интеллекта[2].

В письме предлагается временно приостановить обучение мощных систем искусственного интеллекта, чтобы разработать и внедрить общие протоколы безопасности и создать регулирующие органы для контроля новых систем.

Подводя итог, можем констатировать, что интеграция искусственного интеллекта в сферу расследования преступлений представляется многообещающим направлением, требующим дальнейшего научного анализа. В то же время необходимо тщательно регламентировать правовые аспекты применения этой технологии, учитывая требования по соблюдению прав и законных интересов граждан.

[1] Заблокирован на территории РФ.

[2] См.: Создателей искусственного интеллекта призвали остановить разработки // Газета «Известия»: офиц. сайт. URL: https://iz.ru/1490348/2023-03-29/sozdatelei-iskusstvennogo-intellekta-prizvali-ostanovit-razrabotki (дата обращения: 24.05.2025).

ГЛАВА 3. ТАКТИКА ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

В настоящее время эффективность методики расследования современных преступлений прямо зависит от совершенствования системы своевременного мониторинга состояния преступности.

На сегодняшний день спектр регистрируемых преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, очень широк (табл. 4).

Таблица 4

Классификация преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	
Совершенные с использованием или применением расчетных (пластиковых) карт, компьютерной техники, программных средств, фиктивных электронных платежей, сети Интернет, средств мобильной связи, в том числе кража (ст. 158 УК РФ)	
Мошенничество (ст. 159 УК РФ), мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ)	
Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма (ст. 205.2 УК РФ)	
Незаконные	– организация и проведение азартных игр (ст. 171.2 УК РФ)
	– приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение оружия, основных частей огнестрельного оружия, боеприпасов (ст. 222 УК РФ)
	– приобретение, передача, сбыт, хранение, перевозка, пересылка или ношение взрывчатых веществ или взрывных устройств (ст. 222.1 УК РФ)

Классификация преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации	
	– производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества (ст. 228.1 УК РФ)
	– изготовление и оборот порнографических материалов или предметов (ст. 242 УК РФ); изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1 УК РФ); использование несовершеннолетнего в целях изготовления порнографических материалов или предметов (ст. 242.2 УК РФ)
Публичные призывы к осуществлению экстремистской деятельности (ст. 280 УК РФ)	
Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации (ст. 280.1 УК РФ)	
Неправомерный доступ к компьютерной информации (ст. 272 УК РФ); незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения (ст. 272.1 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)	

Проанализируем системообразующий элемент криминалистической характеристики механизма таких преступлений – способ их совершения (поскольку специфика расследования определяется именно способом совершения преступления). Анализ следственно-судебной практики позволяет объединить способы в несколько основных групп в соответствии со спецификой преступного действия:

– использование цифровых технологий, таких как искусственный интеллект, нейросети, виртуальные валюты (криптовалюты), интернет вещей (IoT), большие данные, а также цифровых устройств для сбора, хранения, анализа информации и обмена ею в цифровом формате;

– применение оборудования и программного обеспечения для достижения преступных целей, таких как терроризм, незаконный оборот наркотиков и оружия, мошенничество, а также применение технологий в качестве орудия совершения преступлений (например, для подделки документов);

– совершение преступлений в виртуальном пространстве.

Последнее целесообразно проиллюстрировать следующим примером. Используя метод криминалистического прогнозирования, можем предположить, что в условиях роста количества преступлений, связанных с использованием различных технологий, в ближайшем будущем более актуальными станут преступные действия, направленные на цифровые активы. В связи с этим представляет особый интерес рассмотрение невзаимозаменяемых токенов (Non-Fungible Tokens, NFT) в качестве предмета преступных посягательств. NFT осуществляет цифровое представление уникальных объектов (физических и виртуальных). В настоящее время наиболее распространенное использование токенов – это представление цифровых произведений искусства или коллекционных предметов.

Проникновение NFT в традиционный мир искусства началось с 2020 г. Однако первый случай, когда произведение изобразительного искусства, относящееся к физическому традиционному миру искусства, было преобразовано в NFT, произошел в сентябре 2018 г. Картина, созданная в 1980 г., состоит из 14 небольших фрагментов, расположенных в два ряда. 31,5 % акций физически существующей картины Энди Уорхола «14 маленьких электрических стульев» (рис. 7) были проданы нескольким людям в виде NFT через смарт-контракт на аукционной платформе Maecenas нескольким инвесторам за 1,7 млн долларов США. В аукционе участвовали 800 претендентов[1].

[1] См.: Картину Уорхола продали по частям на первом криптовалютном аукционе. URL: https://style.rbc.ru/repost/5b321d3d9a79472e748915c7 (дата обращения: 23.05.2025).

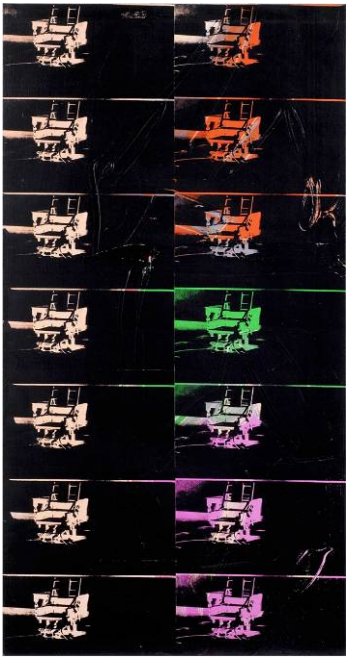


Рис. 7. Картина «14 маленьких электрических стульев»[1].
Художник – Энди Уорхол

Преимущество NFT заключается в создании практически невозможной ранее формы собственности на небольшую часть произведения искусства. Этот метод «закрепления владения» связан с большими финансовыми вложениями и может рассматриваться как новая экономическая стратегия в мире цифровых изображений.

Продолжая рассматривать векторы развития преступности, отметим, что разнообразие и функциональность устройств умного дома создают потенциальные риски для пользователей: при взломе и перехвате контроля – с помощью искусственного интеллекта – над умным домом (например, наличие критической уязвимости в технологии беспроводной связи Wi-Fi позволяет преступникам подключиться к системе управления умным домом для слежки, майнинга криптовалюты и т. д.).

[1] См.: Картину Уорхола продали по частям на первом криптовалютном аукционе. URL: https://style.rbc.ru/repost/5b321d3d9a79472e748915c7 (дата обращения: 23.05.2025).

Представляет интерес мониторинг, посвященный киберпреследованию и незаконному получению персональных данных. «Лаборатория Касперского» провела опрос[1], чтобы выяснить отношение россиян к различным формам цифрового преследования со стороны бывших или нынешних партнеров – вне зависимости от того, сталкивались респонденты с подобным или нет. Среди наиболее неприятных и пугающих форматов онлайн-слежки опрошенные назвали требование предоставить доступ к личным данным на смартфоне (52 %), слежку через сталкерские программы (48 %) и использование трекеров (беспроводных меток) для определения местоположения (45 %). Последние два заметно сильнее беспокоят женщин, чем мужчин.

Специалисты по кибербезопасности обращают внимание: на рынке существуют программы, которые помогают пользователям выявить потенциальную слежку в том случае, если, например, речь идет об онлайн-преследовании с применением Bluetooth-устройств и сталкерских программ. Эксперты подчеркивают, что проблема использования последних становится все более острой.

По данным анонимизированной статистики, «за 10 месяцев 2024 г. количество пользователей android-устройств в России, столкнувшихся со сталкерскими программами, выросло на 25 % по сравнению с аналогичным периодом 2023 г. Используя такие программы, недоброжелатели могут делать скриншоты и запись происходящего на экране зараженного смартфона, отслеживать геолокацию жертвы, получать доступ к перепискам в соцсетях и мессенджерах, при этом никак себя не выдавая. Неспециалисту бывает крайне трудно определить, что на устройстве установлено такое ПО. Лучше использовать для проверки на заражение защитные решения. В случае обнаружения такой программы не рекомендуем ее сразу

[1] Опрос проведен компанией ОнИн по заказу «Лаборатории Касперского» осенью 2024 г. в России. Всего опрошено 1 006 человек. Подробнее об этом здесь: На четверть выросло количество российских пользователей, столкнувшихся со сталкерскими программами в 2024 году. URL: https://www.kaspersky.ru/about/press-releases/na-chetvert-vyroslo-kolichestvo-rossijskih-polzovatelej-stolknuvshihsya-so-stalkerskimi-programmami-v-2024-godu (дата обращения: 23.05.2025).

удалять, следует обратиться за помощью к специалистам, в кризисные центры или правоохранительные органы»[1].

Ранее «Лаборатория Касперского» представила обновление бесплатной версии приложения Kaspersky для Android. Теперь решение помогает бороться не только с цифровой слежкой с применением шпионских программ и сталкерского ПО, но и уведомляет пользователя о подброшенных Bluetooth-устройствах, в том числе о беспроводных метках.

Пожалуй, самым инновационным, интересным и многообещающим концептом является метавселенная (metaverse). В современном мире она приобретает все большую значимость. Метавселенная представляет собой новую цифровую среду, объединяющую разнообразные платформы и технологии.

Растущая популярность метавселенных создает риски, связанные с использованием этой среды для совершения преступлений, таких как кибербуллинг, киберфизическое насилие (особенно в отношении несовершеннолетних), кража персональных данных, NFT, 3D-собственности, виртуальных предметов, цифровых активов, хищение и подделка цифровых идентификаторов личности, отмывание денег, мошенничество и другие виды цифровых преступлений. По мере увеличения числа пользователей и развития технологий этот список будет расти.

С криминалистической точки зрения метавселенная – это соединение физической, дополненной и виртуальной реальностей в общее киберпространство. Можно предположить, что metaverse – благодаря своим свойствам – станет следующим поколением глобальных сетей (табл. 5).

[1] Данные анонимизированной статистики на основе срабатывания решений «Лаборатории Касперского» за январь – октябрь 2023 г. и январь – октябрь 2024 г.

Таблица 5

Основные и дополнительные свойства метавселенной

Базовые характеристики метавселенной	***Дополнительные черты***
– ощущение полного погружения	– взаимодействие между платформами и устройствами
– интерактивность в реальном времени	– одновременное взаимодействие тысяч людей
– возможности управления и владения со стороны пользователя	– использование в различных сферах за пределами игр

Metaverse – это постоянно функционирующая виртуальная среда, где пользователи могут взаимодействовать друг с другом и с цифровыми объектами через свои аватары, используя иммерсивные технологии (совокупность AR (дополненной реальности), VR (виртуальной реальности) и XR (расширенной реальности). Такие взаимодействия могут носить преступный характер и стимулировать развитие MetaCriminal.

Так, в начале января 2024 г. британская полиция впервые начала расследование сексуального преступления в метавселенной. Жертвой стала девочка в возрасте до 16 лет, аватар которой подвергся групповому изнасилованию. Подчеркивается, что использованная пострадавшей VR-гарнитура благодаря встроенным дисплеям и аудиосистеме создает эффект полного погружения. Нападение расследуется полицией на том основании, что, хотя девочка не получила никаких телесных повреждений, из-за захватывающего иммер-

сивного характера воздействия она была так же психологически и эмоционально травмирована, как если бы изнасилование произошло в реальности[1].

Заслуживает интереса тот факт, что в 2022 г. Интерпол создал собственную метавселенную INTERPOL Metaverse для оптимизации взаимодействия полицейских подразделений во всем мире и борьбы с киберпреступностью, поскольку обеспечить полную безопасность виртуального мира на данный момент оказывается практически невозможно (рис. 8)[2].

Рис. 8. Метавселенная INTERPOL Metaverse

Отечественные компании тоже начинают проявлять интерес к концепту. В середине мая 2024 г. МТС объявила о запуске своей метавселенной Verse. Как сообщает пресс-служба телекомоператора, игровое 3D-пространство предполагает новый формат взаимодействия пользователей с продуктами цифровой экосистемы МТС.

[1] См.: Впервые полиция начала расследование в метавселенной. URL: https://xn--80aafkca5bdpa3bj2p.xn--p1ai/ (дата обращения: 17.05.2025).

[2] См.: Интерпол представил собственную метавселенную. URL: https://habr.com/ru/news/694758 (дата обращения: 17.05.2025).

ВТБ тестирует собственную метавселенную – трехмерное интерактивное пространство для виртуального взаимодействия пользователей. Проект обладает потенциалом для реализации нового формата предоставления услуг, в том числе открытия банковских киберофисов. Об этом банк сообщил 17 апреля 2024 г.

Кроме этого, в Москве продолжается активное внедрение технологии цифровых двойников и метавселенных. Речь идет, в частности, о создании единой интеллектуальной цифровой платформы для анализа, моделирования и управления городом в реальном времени на основе геопространственной информации.

Специфика способов совершения преступлений с применением современных информационно-коммуникационных технологий определяет необходимость привлечения специалистов соответствующего профиля не только из организаций, подведомственных МВД, но и из других учреждений, в том числе частных, в рамках уголовного процесса. Это обусловлено особенностями проведения отдельных следственных действий с их участием.

По нашему мнению, отличительное свойство цифровых доказательств заключается в том, что некоторые из них могут быть представлены на материальных носителях (ноутбуки, телефоны, гаджеты, внешние съемные запоминающие устройства, роутеры, видеорегистраторы и т. д.), в то время как другие существуют исключительно в виртуальном пространстве (так называемая «интернет-тень», информация о посещении различных интернет-ресурсов, веб-страниц, данные об электронных транзакциях, данные, хранящиеся в облачных сервисах и на серверах и т. д.). Разнообразие способов совершения преступлений обусловливает возможность появления широкого спектра цифровых следов.

Однако нормативная регламентация вопроса применения возможностей цифровизации в процессе расследования преступлений богата правовыми коллизиями, недосказанностями и пробелами в праве, изучение которых позволит существенно улучшить правоприменительную практику, создать единый алгоритм цифровизации расследования и, как следствие, обеспечит повышение качества и эффективности предварительного расследования и правосудия в целом.

С нашим мнением согласуются результаты исследования, проведенного Х. Х. Рамалдановым: положительно оценивают использо-

вание современных цифровых технологий в процессе расследования 95 % респондентов – сотрудников органов предварительного расследования. При этом применение искусственного интеллекта допускают 50,2 % опрошенных, использование технологии анализа больших данных для извлечения значимой информации – 29,3 % респондентов.

Представляет особый интерес следующий факт: большинство опрошенных сотрудников (91 %) указали, что в ходе оценки доказательств, полученных с помощью информационных технологий, прокурором при реализации им надзорной функции за процессуальной деятельностью предварительного расследования и судом на стадии судебного разбирательства исследуемые доказательства признаются относимыми, допустимыми и достоверными[1].

Полагаем, что внедрение технологий, позволяющих систематизировать, обобщать криминалистически значимую информацию на данном этапе, способствовало бы скорейшему выдвижению версий и выработке наиболее эффективной программы первоначальных действий следователя.

Подтверждением этого является следующий пример из практической деятельности. Так, сотрудниками ГУ МВД по Саратовской области был раскрыт ряд преступлений по ч. 2 и ч. 3 ст. 159 УК РФ. Обвиняемый размещал на сайте «Авито» объявления о продаже автомобилей по низкой цене, но с осуществлением полной предварительной оплаты. После перечисления денежных средств обвиняемый скрывался[2]. В результате проведения анализа использованных IP-адресов и осуществления детализации телефонных разговоров преступления были раскрыты, но, возможно, это произошло бы и в более короткий срок, если бы существовал механизм, позволяющий заранее систематизировать информацию о схожих эпизодах преступной деятельности, о потерпевших.

[1] См.: Рамалданов Х. Х. Процесс доказывания по уголовным делам в условиях тотальной цифровизации общественных отношений: дис. ... канд. юрид. наук: 5.1.4. М., 2024. С. 233–240.

[2] См.: Материалы судебной практики. URL: sudact.ru/regular/doc/MLht2ESs1yrT/ (дата обращения: 29.06.2025).

Положительный опыт использования чат-ботов в правоохранительной деятельности имеется в Республике Беларусь[1]. Пользователю нужно коротко изложить суть правонарушения и – по возможности – прикрепить к сообщению фото. Сообщение регистрируется и передается по территориальной подследственной для проверки (рис. 9).

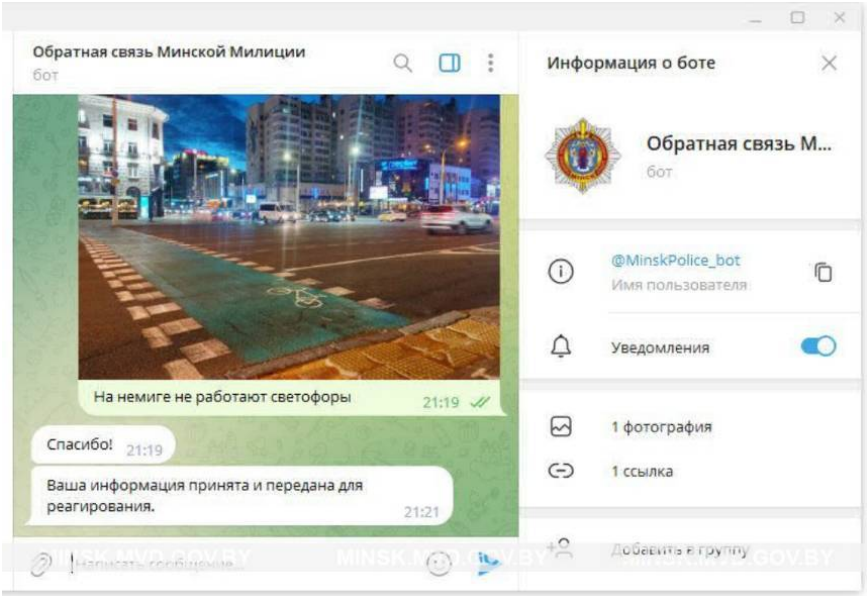


Рис. 9. Чат-бот «Обратная связь Минской милиции»

В Республике Казахстан разработано мобильное приложение 102, предоставляющее гражданам возможность использовать чат-боты для обращения в полицию[2]. Чат-бот работает в режиме 24/7/365. В нем предусмотрена авторизация пользователей с вводом логина, пароля и электронной почты. При обращении граждане

[1] См.: Главное управление внутренних дел Мингорисполкома: офиц. сайт. URL: https://minsk.mvd.gov.by/ru/news/10744 (дата обращения: 31.05.2025).

[2] См.: Комсомольская правда Казахстан: офиц. сайт. URL: https://www.kp.kz/daily/27453/4656857 (дата обращения: 17.05.2025).

могут отправить текстовую информацию, прикрепить фото и видеоматериалы. В зависимости от выбора категории вопроса обращение маршрутизируется, назначается ответственный сотрудник (рис. 10).

Рис. 10. Мобильное приложение 102 с чат-ботом

Считаем данный опыт перспективным для использования в России, поскольку именно оперативное поступление криминалистически значимой информации позволяет эффективно раскрывать и расследовать современные преступления.

Изучение уголовных дел этой категории позволило выявить некоторые изъяны в их расследовании.

Несвоевременное возбуждение уголовных дел препятствует быстрому раскрытию преступлений (по горячим следам) и приводит к утрате важных следов. Долгие сроки проверки материалов могут быть вызваны отсутствием эффективных методов оперативного сбора цифровых следов преступлений, таких как текстовые

данные, аудио- и видеозаписи, технические сведения о месте, времени удаленного доступа, взаимодействии пользователей с информационными системами, об используемом оборудовании и т. д.

В процессе расследования хищений с расчетных счетов финансовых учреждений следователи не в полной мере используют возможности электронного взаимодействия с банками (ПАО «Сбербанк», АО «Альфа Банк»). Не делая самостоятельно соответствующих запросов, следователи опираются только на предоставленные потерпевшими документы. Кроме того, не рассматриваются и не признаются вещественными доказательствами такие документы, как выписки о движении средств, кассовые чеки, договоры о кредитах и другие материалы, собранные в ходе следствия. В итоге теряется ценная криминалистическая информация[1].

Следует отметить, что одной из основных проблем является недостаточно качественное производство следственных действий. Так, при расследовании преступления, совершенного с использованием информационно-телекоммуникационных технологий, в ходе производства осмотра места происшествия, обыска или выемки помимо материальных следов преступления необходимо изымать и цифровые следы, содержащие электронную информацию, которая впоследствии может быть использована в качестве доказательств (далее – цифровых доказательств).

Изменение качественного содержания «традиционных» преступлений можно проследить при рассмотрении примеров из судебной практики[2]. Так, в июне 2021 г. районный суд Перми приговорил четырех жителей Московской области к тюремному заключению за распространение героина на территории Тюменской области через интернет-магазин.

Другое уголовное дело расследовано Томским региональным управлением Федеральной службы безопасности. Установлено, что осенью 2023 г. молодой человек получил в сети Интернет от неизвестного предложение об организации работы лаборатории по

[1] См.: Обзор результатов работы по профилактике, раскрытию и расследованию преступлений в сфере информационно-телекоммуникационных технологий в Волгоградской области за 2023 г. (на основании материалов уголовных дел).

[2] См.: Судебные и нормативные акты РФ (СудАкт). URL: https://sudact.ru (дата обращения: 18.04.2025).

производству и сбыту наркотических средств. Стремление получить «легкие» деньги побудило его привлечь к этой работе своего друга. Вместе они арендовали дом в Первомайском районе Томской области, приобрели необходимое оборудование, сырье и, следуя инструкциям организатора, приступили к производству синтетического наркотика. Изготовив более 35 кг «соли» и расфасовав ее по пакетам, молодые люди разложили наркотики в тайниках в лесных массивах Первомайского района. Забирал их оттуда, чтобы впоследствии сбывать более мелкими партиями, заранее подысканный организатором курьер[1].

Исследование цифровых доказательств является перспективным при производстве расследования не только киберпреступлений, но и преступлений традиционных видов, совершенных с использованием информационно-коммуникационных технологий. Однако существенным пробелом в процессе доказывания при расследовании таких преступлений является неиспользование всех возможностей цифровой криминалистики, в частности специальных познаний; вследствие этого происходит утрата цифровых доказательств, что подтверждается многочисленными примерами из правоприменительной и судебной практики.

Так, в период с 10 ноября 2018 г. по 15 марта 2019 г. Цуканов Д. П., располагая информацией о возможности осуществления незаконного сбыта наркотических средств через тайники, с помощью имеющегося при нем личного сотового телефона с доступом к информационно-телекоммуникационной сети (включая сеть Интернет) и установленной на нем системой мгновенных сообщений в кроссплатформенном мессенджере Telegram, используя виртуальное имя (никнейм) «Неприметная личность», посредством смс-сообщений вступил с ранее неизвестным ему лицом, использующим в Telegram виртуальное имя (никнейм) «Хомяк», в преступный сговор о совместном незаконном сбыте наркотических средств на территории г. Орла и Орловской области – бесконтактным способом (посредством тайников, с использованием ИТКС «Интернет») в крупном размере. Согласно договоренности, достиг-

[1] См.: В Томске вынесен приговор участникам организованной преступной группы. URL: https://epp.genproc.gov.ru/ru/web/proc_sibfo/mass-media/news/news-regional?item=99301354 (дата обращения: 01.06.2025).

нутой между Цукановым Д. П. и не установленным следствием лицом, последний оставлял в тайниках наркотические средства, сведения о местонахождении которых сообщал посредством сообщений в Telegram, а Цуканов Д. П., согласно отведенной ему роли, бесконтактным способом – через тайники – получал для последующего незаконного сбыта наркотические средства, самостоятельно осуществлял закладки и посредством Telegram сообщал не установленному следствием лицу о месте их нахождения. После задержания Цуканова Д. П., в ходе личного досмотра, сотрудники правоохранительных органов обнаружили и изъяли у него смартфон iPhone. В ходе производства предварительного расследования указанный смартфон был осмотрен, обнаружилась переписка в приложении Telegram с неустановленным лицом, содержащая информацию о местах закладок. В ходе расследования личность и местонахождение указанного лица не были установлены, однако материалы в отношении него были направлены в отдельное производство.

Приведем и другой пример из судебной практики. Иванов И. И., имея умысел на хищение чужого имущества путем обмана, действуя в качестве продавца ООО «Гринтек», используя электронный почтовый ящик vargo.vitos@bk.ru, разместил в информационно-телекоммуникационной сети Интернет на сайте «Авито» объявление о продаже новых видеокарт Gigabyte Radeon RX 580 8 gb gddr5 стоимостью 24 000 руб. за единицу товара. Сведения о наличии у него указанных товаров не соответствовали действительности. Иванов И. И., представляясь вымышленным именем «Игорь», посредством переписки на сайте «Авито» сообщил заведомо ложные сведения потерпевшей Петровой А. А. о том, что у него имеются в наличии для продажи десять новых видеокарт Gigabyte Radeon RX 580 8 gb gddr5, которые (с учетом предоставляемой скидки) он готов продать за 230 000 руб. С целью придания своим действиям видимости сделки гражданско-правового характера Иванов И. И. сообщил потерпевшей, что для приобретения видеокарт необходимо внести стопроцентную предоплату на указанный им банковский счет, открытый ООО «Гринтек» в АО «Тинькофф Банк», к которому Иванов И. И. имел доступ. Однако в действительности взятые на себя обязательства он исполнять не собирался и не имел реальной возможности их исполнить. Таким образом, Иванов И. И. обманул

Петрову А. А. относительно своих истинных намерений и похитил принадлежащие ей денежные средства[1].

Данный пример подтверждает, что при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий, особое внимание следует обращать на изучение цифровых доказательств.

Можно сделать вывод о том, что эффективное обнаружение и фиксация цифровых доказательств возможны вследствие интеграции технологий искусственного интеллекта в процесс производства следственных действий.

Безусловно, стремительное развитие современных технологий, а также условия, сложившиеся во время пандемии, способствовали активной цифровизации всех сфер жизни, в том числе и наркобизнеса. Расширился ассортимент синтетических наркотических средств и их аналогов, появились «дизайнерские» наркотики и полинаркомания, активизировалась пропаганда и реклама наркотиков, распространяемая посредством мессенджеров и социальных сетей, сформировались рынки сбыта через законспирированные каналы поставки, были созданы теневые интернет-площадки, организованы сбыт с использованием инновационных информационно-телекоммуникационных технологий и онлайн-оплата с помощью криптовалюты (биткоинов (Bitcoin, BTC), лайткоинов (Litecoin, LTC)), являющаяся простым, анонимным и распространенным, фактически не контролируемым государством способом перечисления средств за наркотики.

На фоне такого темпа развития незаконного оборота наркотических средств стало особенно заметным объективное отставание методики расследования преступлений данного вида. В этой связи целесообразно рассмотреть особенности основополагающей категории методики расследования – криминалистической характеристики. Определяющим элементом криминалистической характеристики преступлений, связанных с незаконным оборотом наркотических средств и их аналогов, является способ их совершения – с использованием современных информационно-телекоммуникационных технологий.

[1] См.: Государственная автоматизированная система Российской Федерации «Правосудие». URL: https://sudact.ru/regular/doc/RYL0iMpCRAgC/ (дата обращения: 25.05.2025).

Полагаем, что для решения проблем, связанных с установлением личности преступников, использовавших анонимайзеры и VPN-сервисы, проведением осмотра «виртуального» места происшествия, обнаружением и изъятием цифровых следов в ходе производства следственных действий и экспертиз при расследовании преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ и их аналогов, совершаемых в сети Darknet, необходимо комплексное совершенствование законодательного регулирования рассматриваемых общественных отношений, использование инновационных технологий для выявления интернет-площадок, применение технологий больших данных, привлечение специалистов в сфере IT-технологий к проведению следственных действий и оперативно-разыскных мероприятий с целью эффективного выявления, раскрытия и расследования указанных преступлений.

Насколько велико значение именно цифровых доказательств для успешного расследования рассматриваемого вида преступлений, можно судить по конкретному примеру из практики. Алимов О. А., использовавший в расположенном на интернет-платформе hydraruzxpnew4af.onion интернет-магазине TimeCrime учетную запись Olega143, в интернет-мессенджере WickrMe – ник kraduserdca, действуя умышленно, из корыстных побуждений, в ходе переписки на сайте указанного интернет-магазина вступил в преступный сговор с неустановленным лицом, использовавшим в интернет-магазине TimeCrime учетную запись «Оптовичок», в интернет-мессенджере WickrMe – ник Razorbtc, с целью незаконного сбыта неопределенному кругу лиц наркотического средства «масло каннабиса (гашишное масло)» в крупном размере с использованием сети Интернет бесконтактным способом – путем размещения наркотического средства в тайниках-«закладках» на территории Ставропольского края.

После этого Алимов О. А. в соответствии с определенной ему (при взаимодействии с неустановленным лицом с ником Razorbtc) преступной ролью в течение длительного времени производил тайники-«закладки» с наркотическим средством «масло каннабиса (гашишное масло)», сведения о местонахождении которых он предоставлял в интернет-мессенджере WickrMe указанному выше

неустановленному лицу с целью последующего незаконного сбыта неопределенному кругу лиц через интернет-магазин TimeCrime[1].

Так, в апреле 2020 г. трое самарцев – М. Власов, В. Востриков и В. Пивоваров – вступили в преступный сговор о производстве и последующем сбыте наркотических средств. К незаконной деятельности они привлекли еще одного подельника, некоего Твердовского Ю. О., занимавшегося организацией тайников-«закладок» в Самаре, а также неустановленное лицо, распространявшее наркотики в Санкт-Петербурге.

Согласно отведенной ему преступной роли Твердовский зарегистрировал интернет-магазин с названием Reboot на «Гидре» – крупнейшем российском даркнет-наркорынке. Оплата за наркотики перечислялась на криптокошельки. У всех членов преступной группы были секретные ники в мессенджерах. Твердовский имел ник FatherOfMane или RUSHIMMM, Пивоваров – Resetthecounters и «Погодный Сомелье», Востриков – «Уважаемый человек», Власов – «Курьер Самара Алекс (центр)», их неустановленный подельник – PumpMaker и LufPounce.

Участники организованной группы имели четко распределенные роли. Так, двое из них, в том числе организатор преступной деятельности, занимались производством наркотических средств, третий участник группы осуществлял непосредственную реализацию наркотиков через магазин в даркнете, еще двое занимались «закладками» в Самаре и Санкт-Петербурге.

Преступная деятельность наркодилеров была пресечена в октябре 2020 г. в ходе оперативных мероприятий сотрудников ГУ МВД России по Самарской области.

При обыске, проведенном в нарколаборатории, расположенной в дачном массиве в Красноярском районе Самарской области, были изъяты более 500 г наркотических веществ, оборудование для производства и фасовки наркотиков, свыше 20 кг прекурсоров наркотических средств. Кроме того, установлено, что наркоторговцами в ходе преступной деятельности путем совершения теневых финансовых операций в легальный оборот выведено более 1 млн руб.

---

[1] См.: Приговор Шпаковского районного суда Ставропольского края от 9 февраля 2022 г. № 1-467/2021. URL: //sudact.ru/regular/doc/MLht2ESs1yrT/ (дата обращения: 29.05.2025).

В ходе расследования у подозреваемых были обнаружены и изъяты мобильные телефоны и ноутбук. При помощи телефона осуществлялось фотографирование участков местности с тайниками-«закладками» наркотических средств, велась переписка; в ноутбуке хранилась информация о незаконном сбыте наркотических средств, а именно фотографии и координаты тайников-«закладок».

Таким образом, в каждом из описанных случаев осмотры позволили установить наличие в памяти телефонов и ноутбука фотографических снимков мест нахождения тайников, в которых оставлялись пакетики с наркотическими средствами, и переписки с другими лицами о фактах сбыта наркотических средств. Мобильные телефоны и ноутбук были признаны вещественными доказательствами, их изучение позволило установить масштабы преступной деятельности злоумышленников. Однако в ходе расследования не все цифровые следы были обнаружены и изучены, в результате чего личность и местонахождение соучастника с никами PumpMaker и LufPounce установлены не были, уголовное дело выделено в отдельное производство[1].

В условиях современного развития технологий особое значение для обнаружения, изъятия и фиксации цифровых доказательств в целях осуществления эффективного расследования современных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, приобретает применение технологии искусственного интеллекта.

Первые попытки законодательной регламентации использования этой технологии и ее результатов предприняты в 2019 г.: именно тогда была принята Национальная стратегия развития искусственного интеллекта на период до 2030 года[2].

Ранее в ходе обсуждений, состоявшихся на научном совете при Совете Безопасности Российской Федерации, эксперты пришли

---

[1] См.: Приговор Самарского областного суда № 02-34/2024 2-34/2024 от 29 октября 2024 г. по делу № 02-34/2024. URL: https://sudact.ru/regular/doc/spLKUQAD2CrM/?regular-txt=228&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=1000&regular-court=Самарский+областной+суд+%28Самарская+область%29&regular-judge=&_=1752213330839&snippet_pos=20236#snippet (дата обращения: 29.05.2025).

[2] См.: Национальная стратегия развития искусственного интеллекта на период до 2030 года.

к выводу о целесообразности внедрения современных информационных технологий, в том числе искусственного интеллекта, в деятельность правоохранительных органов[1].

Анализ действующего законодательства и правоприменительной практики, основанный на данных уголовно-правовых наук, позволяет сформулировать определение искусственного интеллекта. **Под *искусственным интеллектом* предлагаем понимать комплекс технологических решений, включающий информационно-коммуникационную инфраструктуру и программное обеспечение, воспроизводящий когнитивные возможности мозга человека для решения конкретных задач по обработке большого массива данных и поиска оптимальных решений согласно заданному алгоритму.**

Таким образом, эффективное обнаружение и фиксация цифровых доказательств возможны при интеграции технологий искусственного интеллекта в процесс производства следственных действий.

Обязанность лица, осуществляющего предварительное расследование, по обнаружению и фиксации цифровых доказательств прямо закрепляет п. 21 постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть “Интернет”»[2], содержащий положение о том, что необходимо установить, какие именно устройства и программы использовались при совершении преступных действий, поскольку доступ может осуществляться с различных устройств, технологически предназначенных для этого, с исполь-

[1] См.: Эксперты посоветовали силовикам РФ внедрять в работу искусственный интеллект // Информагентство «Интерфакс»: офиц. сайт. URL: https://www.interfax.ru/russia/797839 (дата обращения: 18.06.2025).

[2] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // Интернет-портал «Российской газеты». URL: https://rg.ru/documents/2022/12/28/document-postanovlenie-plenuma-verkhovnogo-suda.html (дата обращения: 30.05.2025).

зованием программ, имеющих разнообразные функции (браузеров, программ, предназначенных для обмена сообщениями, – мессенджеров, специальных приложений социальных сетей, онлайн-игр, других программ и приложений).

Полагаем, что для этого необходимо во всех случаях использовать соответствующие технические средства. К средствам технико-криминалистического обеспечения, основанным на алгоритме искусственного интеллекта, применимым в ходе осмотра электронных носителей информации для обнаружения цифровых доказательств, относится программное обеспечение для компьютерно-технического исследования устройств. Работать с ним должен специалист, привлеченный для участия в производстве следственного действия.

Такие программы позволяют извлекать криминалистически значимую информацию из мобильных устройств, ноутбуков, персональных компьютеров и облачных сервисов. Искусственный интеллект обеспечивает возможность делать аналитику извлечений – строить графы связей, осуществлять распознавание лиц и текста, определять различные виды угроз (оружие, наркотики и т. д.) и многое другое.

Хорошо зарекомендовало себя использование программного обеспечения для компьютерно-технического исследования устройств «Мобильный криминалист», UFED, Belkasoft evidence center и др.

Выявим особенности обнаружения цифровых доказательств в ходе производства отдельных следственных действий (осмотра) с применением электронного носителя информации – смартфона программного комплекса «Мобильный криминалист».

С точки зрения криминалистической тактики к проведению осмотра необходимо привлекать профессионалов в сфере IT-технологий. При этом следователю важно заранее согласовать со специалистом порядок действий и создать необходимые технические условия для его успешной работы.

Если в осмотре участвует владелец электронного носителя, в протокол следственного действия заносятся следующие сведения: действующие аккаунты, логины и пароли, используемые для разблокировки телефона, а также для доступа к защищенным данным, позволяющим получить криминалистически значимую информа-

цию для расследования дела (доступ в облачное хранилище, к электронной почте, социальным сетям и т. п.). При необходимости снятия блокировки телефона с помощью отпечатка папиллярного узора пальца руки или осуществления идентификации, реализуемой функцией Face ID, владельцу предлагается разблокировать устройство и отменить блокировку в настройках. Об указанных действиях делается отметка в протоколе.

Далее в ходе осмотра с использованием алгоритма искусственного интеллекта программного обеспечения «Мобильный криминалист» фиксируется содержание носителя: при непосредственном участии специалиста отражаются все приложения, графы связей, звонки, геотеги, временные маркеры, в том числе содержащиеся на облачных сервисах, а также удаленные данные (рис. 11–13).

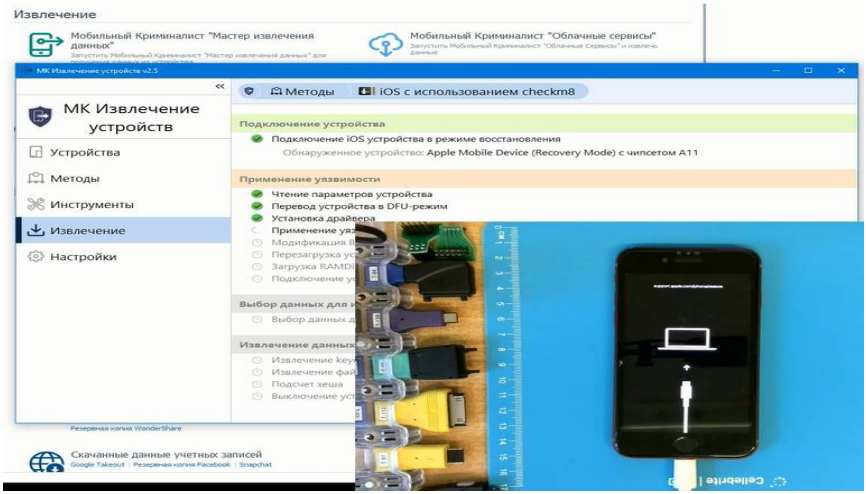


Рис. 11. Подключение устройства с использованием программного обеспечения «Мобильный криминалист»

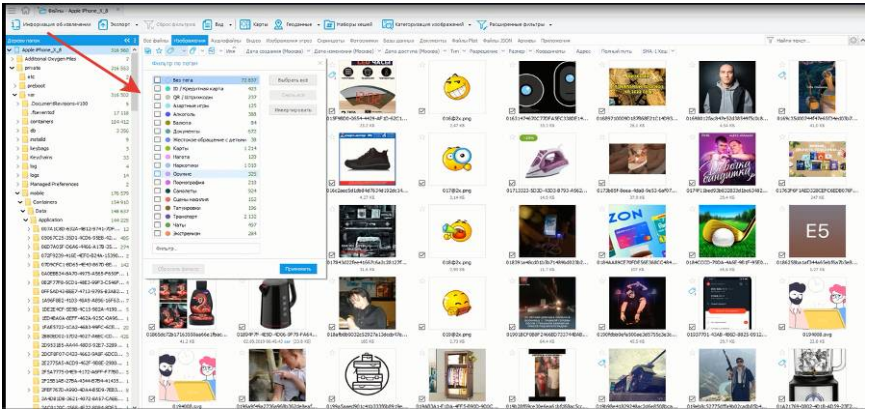


Рис. 12. Аналитика и извлечение данных с использованием алгоритма искусственного интеллекта программного обеспечения «Мобильный криминалист» (стрелкой указаны теги, позволяющие найти информацию по различным видам угроз)

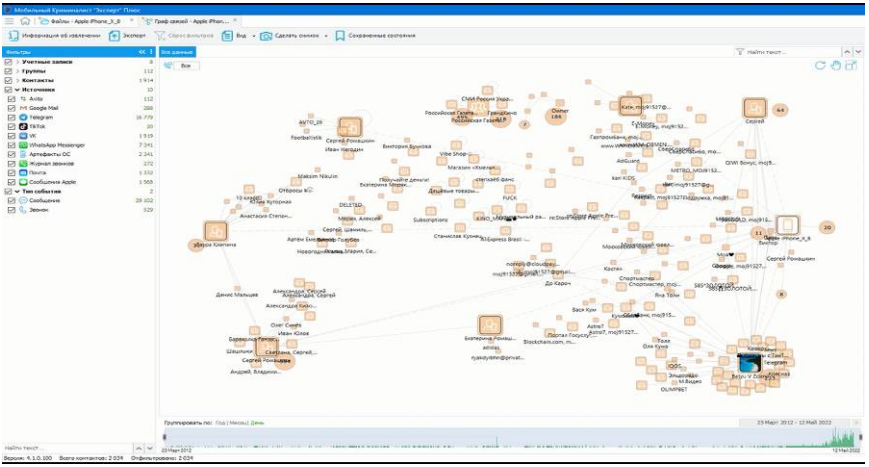


Рис. 13. Установление графов взаимосвязей с использованием алгоритма искусственного интеллекта программного обеспечения «Мобильный криминалист»

Рассматриваемая тактика будет эффективна для производства всех видов следственных действий, в ходе которых предполагаются изъятие и осмотр любых видов мобильных телефонов – как смартфонов, так и фичерфонов.

Возможность использования технологии искусственного интеллекта и цифровых доказательств в расследовании предоставляется, по нашему мнению, в случае выполнения ряда условий.

Во-первых, необходима законодательная регламентация рассматриваемых понятий.

В связи с этим предлагаем внести следующие изменения в нормативные правовые акты (приложения 2, 3).

Приложение 2 содержит предложение дополнить статьи Уголовно-процессуального кодекса Российской Федерации несколькими пунктами:

– статью 5 дополнить пунктом: «58.1) цифровые доказательства – любые сведения в электронном виде, устанавливающие наличие или отсутствие обстоятельств, имеющих значение для уголовного дела, зафиксированные на носителях электронной информации либо хранящиеся или передаваемые с использованием информационно-телекоммуникационных технологий»;

– часть 2 статьи 74 дополнить пунктом: «4.1) цифровые доказательства».

Нуждается, по нашему мнению, в дополнении и Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ[1]. Приложение № 3 содержит соответствующее предложение:

– статью 2 дополнить пунктом: «4.1) искусственный интеллект – комплекс технологических решений, включающий информационно-коммуникационную инфраструктуру и программное обеспечение, воспроизводящий когнитивные возможности мозга человека для решения конкретных задач по обработке большого массива данных и поиска оптимальных решений согласно заданному алгоритму».

[1] См.: Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ // КонсультантПлюс: справ.-правовая сист. URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 17.06.2025).

Во-вторых, необходимо дальнейшее исследование проблем применения сквозных IT-технологий, привлечение специалистов в сфере IT-технологий к проведению следственных действий и оперативно-разыскных мероприятий, а также разработка частной криминалистической методики с целью эффективного расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

Таким образом, изучение и применение алгоритмов искусственного интеллекта уже сегодня позволяет эффективно обнаруживать, изымать и фиксировать цифровые доказательства, что становится все более востребованным при расследовании IT-преступлений.

Сказанное, несомненно, актуально для производства *следственного осмотра*. Отметим, что тема фиксации следов преступления с помощью современных технических средств и компьютерных технологий, получившая развитие в трудах В. С. Экономюк, актуальна еще и потому, что в связи с изменениями, внесенными в Уголовно-процессуальный кодекс РФ, стало возможным проведение ряда следственных действий без участия понятых – при условии надлежащей фиксации с помощью технических средств.

В настоящее время методика фиксации еще не полностью разработана, и наиболее эффективным может быть создание рекомендаций, способствующих расследованию отдельных видов преступлений. Применение дронов (в том числе БПЛА) во время осмотра места происшествия соответствует требованиям процессуальной фиксации следственного действия.

Д. Н. Лозовским, Н. Н. Лозовской, И. Р. Ульяновой предлагается следующий порядок действий с участием специалиста – оператора БПЛА (специалиста по эксплуатации беспилотных летательных аппаратов), управляющего аппаратом во время осмотра места происшествия[1].

Перед выездом на место происшествия, где планируется использовать БПЛА, необходимо

[1] См.: Лозовский Д. Н., Лозовская Н. Н., Ульянова И. Р. Использование беспилотных летательных аппаратов в процессе расследования преступлений: вопросы теории и практики // Юристъ-Правоведъ. 2021. № 3 (98). С. 162–165.

– проверить наличие всех компонентов, необходимых для подготовки и использования аппарата, включая работоспособность программного обеспечения;

– убедиться в полной зарядке батарей технического средства, пульта управления, планшета и другого оборудования;

– собрать информацию о полетах других летательных аппаратов в воздушном пространстве над местом происшествия (разрешено проводить неотложный осмотр без предварительного разрешения).

По прибытии на место оператор устанавливает связь БПЛА с устройством (планшетом или смартфоном), проводит калибровку и ориентируется на местности с помощью навигатора глобальной системы позиционирования, сопоставляя полученные данные с картами.

Во время подготовки аппарата к работе окружающая обстановка оценивается на предмет наличия возможных препятствий для взлета и дальнейшей работы (зданий, построек, деревьев, линий электропередач и т. д.). Затем выбирается место для взлета БПЛА – ровная площадка размером 1×1 м с твердым покрытием.

Для эффективного проведения общего осмотра используется дрон, так как он охватывает большую территорию и исключает перемещение по ней, сохраняя следы.

На рабочем этапе с помощью дрона можно делать фотографии с воздуха, способные служить доказательством по делу и дополнять фототаблицу. Камера БПЛА позволяет распознавать лица правонарушителей, снимать видео и фото, передавать материалы в реальном времени на пульт оператора.

БПЛА может быть оснащен приборами ночного видения, тепловизорами и спутниковой навигацией, позволяющими ему работать в разных условиях. В любом случае при осмотре рекомендуется поднимать квадрокоптер на высоту 30–40 м (следует учитывать, что разрешенный максимум – 50 м). Высота зависит от размера осматриваемой территории и объектов, которые нужно найти (орудия преступления, трупы, следы техники или людей).

Прежде всего следует осмотреть всю предполагаемую площадь, чтобы определить участки (узлы), на которых нужно сосредоточиться при детальном осмотре. Рекомендуется брать с собой на место происшествия ноутбук для просмотра фото- и видеоматериалов, полученных с помощью дрона.

Аналогичный алгоритм действий можно применять не только для БПЛА, но и для надземных и подводных дронов.

Л. А. Спектор и А. Д. Малютин справедливо указывают на формирование принципиально новых видов правоотношений, складывающихся вокруг объектов и явлений в кибернетическом пространстве, не имеющих аналогов в традиционном материальном мире. В частности, речь идет об интернет-сайтах, системе доменных имен, компьютерных программах (особенно самовоспроизводящихся, известных как компьютерные вирусы), системах распределенных реестров (Blockchain), ставших основой для построения целого спектра криптовалют, социальных сетях, беспилотных транспортных платформах и др.

Появление новых объектов инициирует возникновение новых видов посягательств на складывающиеся правоотношения в кибернетическом пространстве (использование вредоносных программ, зеркалирование и подмена интернет-ресурсов, перехват реальной и генерация фиктивной (намеренно искаженной) информации и т. д.), расширение представления о механизме следообразования за счет дополнения его знаниями о закономерностях кибернетического пространства, а именно об электронно-цифровом отображении, виртуальных следах, новых свойствах возникающих следов, особенностях формирования следовой картины и т. д.[1]

Интересным представляется рассмотрение использования потенциала иммерсивных технологий при производстве следственных действий. В условиях трансформации и цифровизации современный следователь должен использовать его максимально, открывая новые эффективные возможности для расследования.

Так, использование технологии Chromakey позволяет создавать обстановку разнообразных мест происшествий и различные объекты. Назначение технологии Chromakey – выводить статические изображения и видео с полотна на экран телевизора или мобильного устройства; технологии дополненной реальности (AR) дополняют физический мир виртуальными изображениями и 3D-эффектами. Специалисты могут воссоздавать место происшествия, неоднократно обращаться к обстановке совершения преступления, детально

[1] См.: Спектор Л. А., Малютин А. Д. Указ. соч.

изучать объекты и следы преступления, их структуру, свойства, индивидуальные идентифицирующие признаки.

Использование технологии Chromakey способствует активизации памяти допрашиваемого, реконструкции обстановки места происшествия при подготовке к производству проверки показаний на месте, проведению следственного эксперимента, обыска, выемки.

Отметим, что существенным пробелом в процессе доказывания рассматриваемой нами категории преступлений является неиспользование всех возможностей цифровой криминалистики, в частности специальных познаний, в результате чего происходит утрата цифровых доказательств.

Примеры из практики показательны, поскольку в большинстве случаев следователи ограничиваются осмотром мобильных телефонов и иных электронных носителей информации, подтверждая только факты наличия переписки с неустановленными лицами и единого умысла на сбыт наркотических средств бесконтактным способом. Полагаем, что изучение цифровых следов было бы более информативным в случае привлечения специалиста к осмотру телефона и ноутбука, назначения и проведения соответствующих судебных экспертиз.

В частности, использование в ходе осмотра и исследования цифровых доказательств таких современных криминалистических программных комплексов, как, например, «Мобильный криминалист», UFED, Belkasoft Evidence Center, позволяет не только получить данные из установленных приложений, программ обмена сообщениями, электронной почты, но и извлечь сведения о геолокации, о временных маркерах и восстановить удаленную информацию.

О востребованности использования таких специальных знаний свидетельствует увеличение количества произведенных компьютерно-технических экспертиз. Так, в ЭКЦ ГУ МВД России по Волгоградской области в 2018 г. было произведено 396 экспертиз, а в 2023 г. – уже 691 экспертиза[1].

Особая значимость производства экспертизы заключается в том, что в ходе проведения исследования эксперт при помощи специаль-

[1] См.: Анализ статистических данных по организации производства компьютерно-технической экспертизы в ЭКЦ ГУ МВД России по Волгоградской области (на основании материалов уголовных дел).

ного программного обеспечения может извлечь физический образ устройства, составить графы взаимодействия, восстановить удаленные записи из баз данных различных мобильных приложений, сформировать отчет о работе приложений в удобном для просмотра виде и выгрузить контент, в том числе ранее удаленный.

Это способствует установлению совокупности данных о времени осуществления звонка или отправки сообщения, о месте нахождения, скорости и траектории движения лица в этот момент. При исследовании фотоснимков и видеозаписей механизмы временного маркирования и геотегирования позволяют установить точное время и место создания конкретного фотоснимка, личности находящихся на фотоснимках, круг их общения.

При сопоставлении указанной информации с данными о совершении преступления, зафиксированными с помощью аппаратно-программного комплекса «Безопасный город», различных камер видеонаблюдения, видеорегистраторов, а также со сведениями, имеющимися на «умных» гаджетах (о скорости движения, пульсе и т. д.), с данными о присоединении устройств к роутерам по сети Wi-Fi, с анализом биллингов операторов сотовой связи можно не только установить соучастников преступления, свидетелей, потерпевших, но и получить информацию о возможном местонахождении вещественных доказательств, подтвердить или опровергнуть различные следственные версии и в целом достаточно полно реконструировать картину совершения преступления.

Представляет интерес зарубежный опыт использования информации, сохраненной в памяти гаджетов, для раскрытия преступлений. Так, в США в феврале 2021 г. мужчина сообщил правоохранительным органам, что его жена скончалась, видимо, уже после того, как он лег спать (около 22:30). Он утверждал, что супруга могла умереть из-за несчастного случая (якобы она была пьяна и, вероятно, неудачно упала). Опровергнуть версию мужчины помогли полученные правоохранительными органами данные из фитнес-приложения Health, согласно которым смерть жены наступила примерно в 22:00, а мужчина в это время совершил несколько шагов

около ее тела[1]. В Германии было раскрыто убийство отчимом падчерицы. Мужчина заявлял о своей непричастности к ее смерти, однако с помощью сохранившейся в фитнес-браслете Fitbit информации о том, что сердце жертвы остановилось, когда отчим был еще рядом с ней в доме[2], удалось установить личность преступника.

Согласно положениям ч. 2 ст. 195 УПК РФ судебная экспертиза производится государственными судебными экспертами и иными экспертами из числа лиц, обладающих специальными знаниями. В этой связи отдельно следует сказать о возможностях других экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, – современных экспертиз, с помощью которых исследуют цифровые доказательства.

Среди относительно новых видов таковых – экспертное исследование видеозаписей с целью определения эмоционального состояния лица и установления наличия признаков оказываемого на лицо психологического воздействия. Объектом исследования является видеоматериал, содержащий общие психологические сведения о лице, особенностях его состояния и поведения в период, представляющий интерес для следствия. Рекомендуемый вопрос специалисту при назначении такой экспертизы – «Имеются ли на представленной видеозаписи признаки оказываемого на лицо психологического воздействия?».

Интересны особенности использования специальных знаний при назначении судебных психолого-лингвистических экспертиз. Так, при проведении экспертизы по делам, связанным с противодействием экстремизму и терроризму, специалист исследует аудио- и видеозаписи, видеоролики, зафиксированное содержание интернет-страницы, интернет-форума, страницы персонального пользователя социальной сети и др. Рекомендуемый вопрос эксперту – «Содержатся ли в тексте лингвистические и психологические признаки побуждения (в том числе в форме призыва) к каким-либо действиям

[1] См.: Он не спал: фитнес-приложение раскрыло убийство. URL: https://www.gazeta.ru/tech/2021/02/10/13473764/criminal_apps.shtml?updated (дата обращения: 27.05.2025).

[2] См.: Умные браслеты. URL: https://www.oxygensoftware.ru/ru/news/articles/141-fitnes-kriminalistika-kak-umnye-braslety-pomogayut-raskryvat-prestupleniya (дата обращения: 25.05.2025).

(включая насильственные, дискриминационные) против какой-либо группы, выделенной по национальному, религиозному, социальному и другим признакам, или ее представителей?».

С помощью экспертизы информационных материалов по делам о побуждении к самоубийству специалисты исследуют направленность информационного материала или коммуникативной деятельности субъекта на побуждение жертвы к самоповреждающему либо суицидальному поведению. Объектами исследования в этом случае могут являться переписка в социальных сетях и различного рода сообществах, личная переписка, а также иная письменная и изобразительная «продукция» лица, совершившего суицидальные действия. В рамках таких исследований решаются следующие задачи: установление наличия (отсутствия) направленности на формирование готовности адресата к причинению себе вреда и (или) лишению себя жизни, средств формирования готовности, информации о способах самоубийства. Рекомендуемый вопрос специалисту – «Содержатся ли в материале психологические и лингвистические признаки побуждения к совершению самоубийства?».

Таким образом, использование возможностей цифровой криминалистики и специальных знаний, позволяющих исследовать цифровые доказательства, является перспективным для эффективного расследования преступлений, совершенных с применением информационно-телекоммуникационных технологий.

Решение указанной проблемы – поиска эффективных средств, позволяющих расследовать преступления в условиях цифровизации – нам видится возможным в случае достижения определенных результатов: во-первых, необходимо использовать инновационные технологии для выявления виртуальных мест преступлений и исследования цифровых доказательств, применения сквозных IT-технологий, привлечения специалистов в сфере IT-технологий к проведению следственных действий и оперативно-разыскных мероприятий с целью эффективного расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий; во-вторых, требуется совершенствование законодательного регулирования рассматриваемых общественных отношений[1].

[1] См.: Приложения 2, 3.

Стремительные темпы цифровизации способствуют появлению разнообразных высокотехнологичных способов совершения преступлений. В последнее время все большую популярность в преступном мире приобретает «тренд», связанный с использованием в преступных целях технологии искусственного интеллекта.

Страны охватывает «эпидемия» высокотехнологического обмана, проникающего во все сферы цифрового пространства. В течение последних двух лет особой проблемой стало распространение такого вида преступления, как мошенничество с применением технологии DEEPFAKE (далее – дипфейк).

Об актуальности обозначенной выше проблемы свидетельствует внимание к ней на самом высоком государственном уровне. Так, 14 декабря 2023 г. в рамках мероприятия «Итоги года с Владимиром Путиным – 2023» в ходе прямой линии к Президенту России Владимиру Путину обратился с вопросом «цифровой двойник», созданный с использованием технологии дипфейк. После этого российский лидер подчеркнул, что предотвратить развитие искусственного интеллекта невозможно, а значит, нужно стремиться быть лидерами в этом направлении[1].

Однако отсутствие легитимной дефиниции и законодательной регламентации дипфейков предопределяет их преступный потенциал. На устранение лакун в нормативном регулировании дипфейков направлена законодательная инициатива о введении ответственности за несанкционированное использование голоса и изображений человека в целях мошенничества[2].

Кроме того, на заседании Правительственной комиссии по профилактике правонарушений, состоявшемся 20 декабря 2023 г., было принято решение, согласно которому в результате совместной работы МВД, Минцифры и Роскомнадзора предполагалось создать алгоритм правового регулирования «цифровых портретов» в целях недопущения их противоправного использования[3].

---

[1] См.: Итоги года с Владимиром Путиным – 2023.

[2] См.: В Госдуме работают над законопроектом о запрете дипфейков. URL: https://pravo.ru/news/251111 (дата обращения: 09.05.2025).

[3] См.: Владимир Колокольцев провел заседание Правительственной комиссии по профилактике правонарушений. URL: https://mvdmedia.ru/news/official/vladimir-kolokoltsev-provel-zasedfanie-pravitelstvennoy-komissii-po-profilaktike-pravonarusheniy/ (дата обращения: 06.05.2025).

Исследованию проблем законодательной регламентации и противодействия распространению технологии дипфейков также посвящены работы многих ученых – В. Б. Батоева, А. В. Пучнина, Е. С. Лариной, В. С. Овчинского, С. В. Лемайкиной и др.[1]

Согласно статистическим данным за 2022–2023 гг., предоставляемым платформой Statista[2], в мире наблюдается взрывной рост мошенничеств, связанных с использованием технологии дипфейк (рис. 14).

Рис. 14. Стремительный рост количества случаев мошенничества с использованием технологии дипфейк (указаны страны с наибольшим прогрессированием) за период с 2022 по 2023 г. (в %)

[1] См., например: Батоев В. Б., Пучнин А. В. Использование технологии Deepfake в преступной деятельности: проблемы противодействия и пути их решения // Вестник Воронежского института МВД России. 2023. № 1. С. 165–169; Ларина Е. С., Овчинский В. С. Криминальная жизнь дипфейков // Информационные войны. 2022. № 3 (63). С. 69–73; Лемайкина С. В. Актуальные вопросы противодействия использованию технологии дипфейков // Юристъ-Правоведъ. 2022. № 3 (102). С. 175–178.

[2] См.: Statista – международная глобальная платформа данных с обширной коллекцией статистических данных, отчетов и аналитической информации. URL: https://www.statista.com/aboutus/ (дата обращения: 02.06.2025).

Было проанализировано два миллиона случаев, зафиксированных в 124 странах. Очевидным стало, что эти преступления буквально охватили весь мир – вне зависимости от социально-экономического развития, политического режима и иных особенностей государств.

Так, в 2023 г. на Филиппинах число случаев мошенничества с использованием дипфейков возросло на 4 500 % по сравнению с 2022 г. Во Вьетнаме рост составил более 3 000 %, в Японии – 2 800 %. Четырехзначные цифры, определяющие темпы роста, зафиксированы в США, ОАЭ, ЮАР и многих странах Европы.

В отчете Onfido (компании, разрабатывающей платформы безопасной цифровой идентификации личности), авторы которого основываются на анализе мошеннических схем с личными данными в 2024 г., прогнозируется увеличение на 3 000 % количества цифровых атак[1].

Считаем правильным присоединиться к мнению В. Б. Батоева и А. В. Пучнина, полагающих, что количество дипфейков находится в прямой зависимости от уровня развития информационных технологий[2]. Раньше этот информационный продукт встречался относительно редко из-за сложности его создания. Сейчас же наблюдается тенденция к упрощению и общедоступности применения технологии. Сегодня существует множество онлайн-сервисов, приложений, ботов, позволяющих производить дипфейки (например, DeepFaceLab, Zao, FaceSwap, Neuman, Deepfakes web и т. д.). Как только технология стала доступна большинству, ее начали активно использовать и мошенники.

Сказанное обусловливает необходимость подробного рассмотрения технологии.

Дипфе́йк (англ. Deepfake, от deep learning – глубокое обучение и fake – подделка) – технология на базе искусственного интеллекта, позволяющая создавать ложные изображения и видео на основе реальных кадров[3].

---

[1] См.: Отчет о мошенничестве с личными данными, 2024 г. Onfido. URL: https://onfido.com/landing/identity-fraud-report/ (дата обращения: 07.05.2025).

[2] См.: Батоев В. Б., Пучнин А. В. Указ. соч. С. 166.

[3] См.: Большая российская энциклопедия: офиц. сайт. URL: http://bigenc.ru/c/dipfeik-f9f89b (дата обращения: 03.05.2025).

Алгоритм анализирует большое количество снимков, аудио, видео и учится тому, как может выглядеть, говорить и двигаться конкретный человек. Нейросеть собирает из интернета, в том числе из открытых источников в социальных сетях, аудио- и видеофайлы, фотографии человека с разными выражениями лица и создает из них новое изображение, аудио- или видеозапись. Дипфейки выглядят гиперреалистично, поскольку инструменты искусственного интеллекта были обучены на десятках тысяч изображений реальных людей.

Таким образом, нейросети научились создавать цифрового двойника практически любого человека. Они могут подделывать не только внешность, но и голос. В условиях широкой доступности технология стала мощным орудием, которое преступники используют для мошенничества, вымогательства, шантажа, разжигания конфликтов (рис. 15, 16).

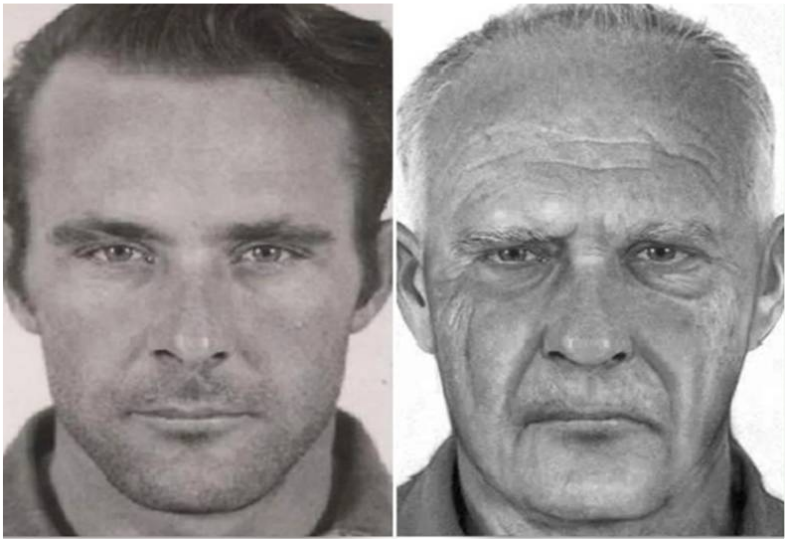


Рис. 15. Нейронные сети, используя специальные алгоритмы, создают эффекты старения (пример использования технологий искусственного интеллекта)[1]

[1] См.: Фото сбежавших из Алькатраса преступников состарили с помощью нейросети. URL: https://moya planeta.ru/news/view/foto_sbezhavshikh_iz_alkatrasa_prestupnikov_sostarili_s_pomoschyu_nejroseti (дата обращения: 03.05.2024).

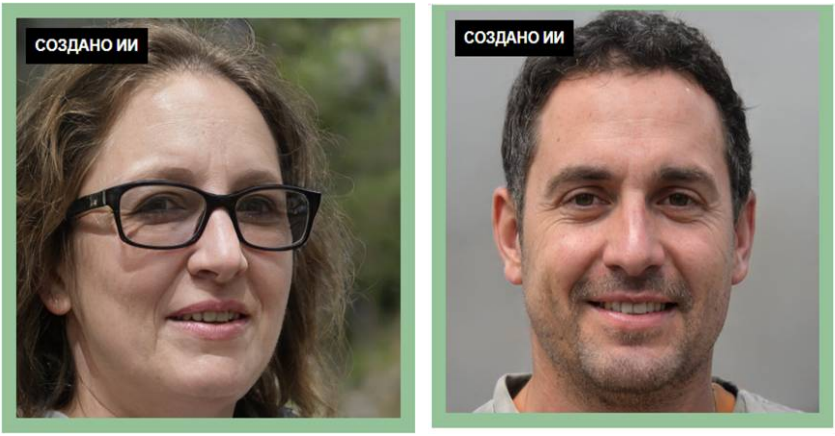


Рис. 16. Примеры изображений, сгенерированных нейросетями

Кроме того, мошенники, стараясь получить образцы голосов, стали размещать в интернете объявления с предложением работы – платной озвучки рекламы и фильмов (рис. 17). Целью фальсификаторов является обучение нейросетей и последующая генерация аудиосообщений для вымогательства денег у родственников и друзей.

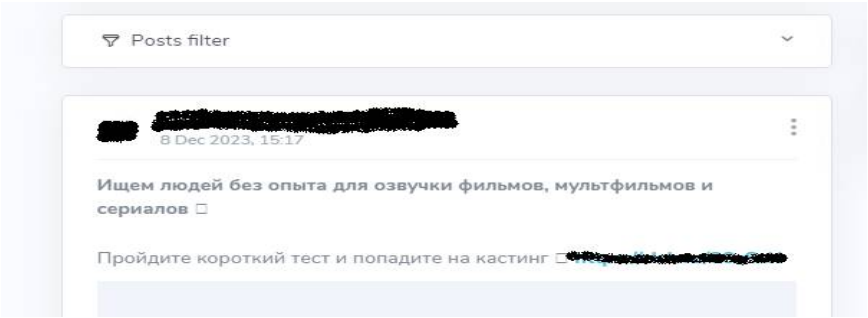


Рис. 17. Объявление в мессенджере

Дипфейки становятся все более реалистичными и убедительными. Эволюция качества способствует появлению все новых мошеннических схем. Рассмотрим некоторые способы совершения таких преступлений.

Сейчас наибольшее распространение получила схема fake boss – указания от фейкового руководителя. Сначала в мессенджер (чаще всего Telegram или WhatsApp*) приходит сообщение – текстовое – о том, что сотруднику будет звонить начальник (представитель государственных органов), или голосовое – аналогичного содержания. Затем, используя методы социальной инженерии, под видом форс-мажора, мошенники заставляют потерпевшего перевести деньги на «безопасный счет».

Другим способом обмана является использование образа популярной личности. Так, в конце ноября 2023 г. в сети появилось видео следующего содержания: известный комик и киноактер Нурлан Сабуров рекламирует приложение онлайн-казино. На самом деле это дипфейк – так мошенники завлекают пользователей на фишинговый сайт[1].

Поскольку генеральная идея любых дипфейков – максимальная реалистичность и правдоподобность, то уже сегодня можно наблюдать лавинообразный рост модифицированного контента, созданного с целью манипуляции сознанием отдельно взятого человека.

Появился, например, такой вид мошенничества: преступники с помощью нейросети генерируют голосовые обращения владельцев аккаунта и вымогают деньги у его контактов, прикрепляя фото банковской карты с именем и фамилией. На первом этапе преступники взламывают аккаунты в мессенджерах (например, Telegram или WhatsApp*) с помощью фейковых голосований. Затем они скачивают сохраненные голосовые сообщения и создают новые – с нужным текстом. Далее происходит рассылка этих сообщений в личные и групповые чаты с просьбой об одолжении большой суммы денег, подкрепленной сгенерированными голосовыми записями и отфотошопленными банковскими картами с поддельными именами получателей (рис. 18).

---

* Принадлежит компании Meta, которая признана экстремистской и запрещена в РФ.

[1] См.: Фейковая реклама казино от имени стендап-комика Нурлана Сабурова распространяется в Сети. URL: https://stopfake.kz/ru/archives/21066 (дата обращения: 30.04.2025).

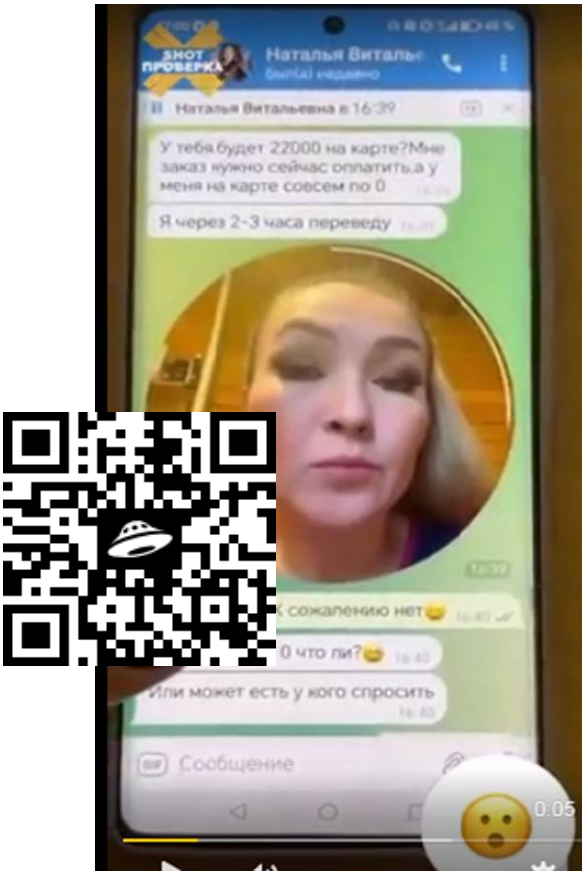


Рис. 18. Пример дипфейка, с помощью которого мошенники получают деньги в Telegram (полное видео по QR-коду)[1].

Другим распространенным (и при этом легким) дипфейк-способом изъятия денежных средств является запись мошенниками голоса жертвы, например, при спам-звонках. Главная задача состоит в том, чтобы добиться произнесения ключевых слов, например, «да», на основе которых генерируется типовая звуковая дорожка

[1] См.: Пример дипфейка, с помощью которого «разводят» на деньги в телеграмме. URL: https://t.me/mig41/32028 (дата обращения: 18.05.2025).

для «общения» с роботом службы поддержки банка. Грамотно синтезированная на базе ключевых фрагментов запись позволяет «достоверно» ответить на все вопросы робота для перевода средств на нужный мошенникам счет.

В начале 2024 г. в России были зафиксированы попытки использования еще одного способа мошенничества: преступники, используя технологию дипфейка для подтверждения личности владельца аккаунта посредством совершения видеозвонка, обращаются в банк с просьбой привязать личный кабинет к новому номеру телефона. После указанных действий мошенники получают полный доступ к личному кабинету и ко всем денежным средствам потерпевшего (рис. 19).

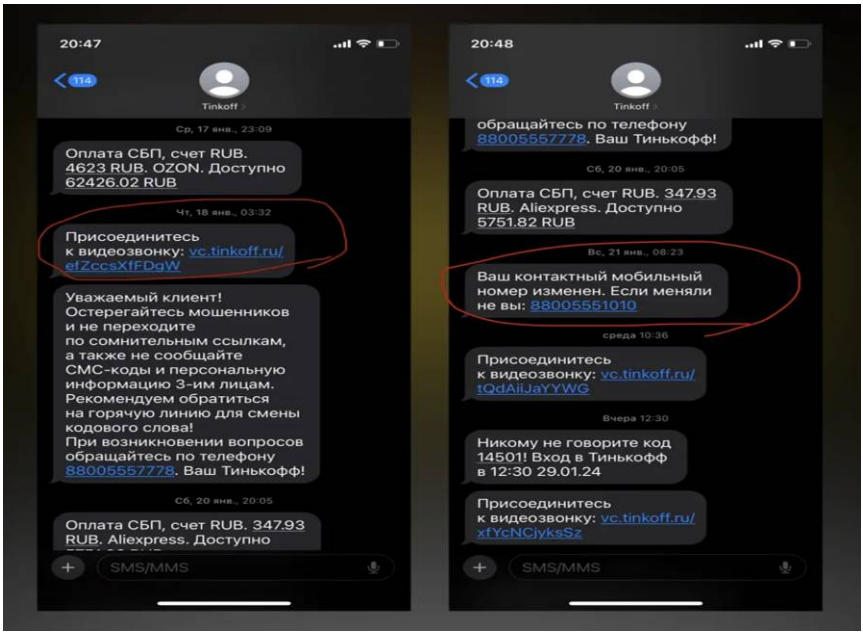


Рис. 19. Переписка мошенника с сотрудником банка (январь 2024 г.)[1]

[1] См.: Как мошенники научились подтверждать личность в банке. Все оказалось проще… URL: https://habr.com/ru/articles/791074/ (дата обращения: 20.05.2025).

В Даркнете набирают обороты услуги по созданию фейковых видео для криптостримов на платформах популярных социальных сетей и фальшивых розыгрышей криптовалют, в рамках которых мошенники побуждают зрителей переводить криптовалюту.

Главная особенность всех рассмотренных способов заключается в том, что выявить подделку может только профессионал в сфере компьютерных технологий с помощью специальных программ.

Так, в конце 2023 г. СБЕР запатентовал технологию распознавания дипфейков, предназначенную для повышения точности и эффективности обнаружения синтетического изменения изображений лиц людей на видео[1]. Основу технологии составляют ряд ансамблей нейросетевых моделей класса EfficientNet (патент № 2768797) и метод амплификации и анализа средствами искусственного интеллекта микроизменений в цветах объектов на кадрах (патент № 2774624). Объединенные в систему, они позволяют с высокой точностью определить синтетически измененные изображения лиц на видео.

Особенностью системы является присущая ей возможность обработки видеоконтента с несколькими лицами в кадре. В этом случае система выявляет отдельное лицо, созданное синтетическим образом, и оценивает его достоверность, что позволяет противодействовать реализации ряда методов обхода систем обнаружения дипфейков.

Кроме того, разработана система мониторинга дипфейков «Зефир», выявляющая дипфейки в аудио и видео.

Упомянутые выше технологии предназначены прежде всего для обеспечения защиты граждан от мошеннических действий.

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

Для исследования объектов, содержащих признаки дипфейков, целесообразно назначение компьютерной, видеотехнической и фоноскопической экспертиз. Вопрос, на который отвечают эксперты в этом случае, – «Имеются ли в представленной записи признаки применения технологии дипфейка?».

---

[1] См.: Сбер создал одну из лучших в мире технологий распознавания дипфейков. URL: https://www.ferra.ru/news/techlife/sber-sozdal-odnu-iz-luchshikh-v-mire-tekhnologii-raspoznavaniya-dipfeikov-09-02-2023.htm (дата обращения: 29.04.2025).

При производстве экспертизы выявляются следующие признаки подделки: муар (волнообразный узор, возникающий из-за наложения одного изображения на другое), излишняя пикселизация, дефекты, нечеткое или смазанное изображение, дрожание или запаздывание речи, неестественное лицо, неестественные движения и мимика человека, отсутствие моргания, нарушения потоков аудиозаписи, различие в освещенности и тенях, мелкие детали, низкое качество видео, «маскирующее» попытку скрыть факт использования нейросетей и др.

Все сказанное ранее дает основания для формулирования наиболее перспективных направлений, реализация которых позволит эффективно расследовать и предупреждать преступления рассматриваемой категории:

1. Разработка уголовно-правовой регламентации и закрепление соответствующих дефиниций в законодательстве России с целью единого правоприменения.

2. Внедрение системы распознавания компьютерного (клавиатурного) почерка, строящейся на основе интеллектуального анализа времени удержания объектов на экране, то есть того, как именно пользователь набирает текст и с какой скоростью (у каждого человека этот фактор уникален и может меняться в зависимости от психофизиологического состояния). При походке система анализирует положение гаджета в пространстве. За счет применения сверхточных нейронных сетей из динамики походки выявляются те перемещения в пространстве, которые идентифицируют непосредственно пользователя (15.03.2024 отечественные ученые представили разработку)[1].

3. Авторизация пользователя по сетчатке глаза. Данный метод в качестве идентификатора использует уникальный рисунок кровеносных сосудов глазного дна. Сканирование происходит с помощью инфракрасного излучения низкой интенсивности, направляемого через зрачок к задней стенке глаза. «Центр биометрических

[1] См.: В РФ разработали систему идентификации пользователя по клавиатурному почерку. URL: https://www.m24.ru/news/nauka/15032024/674543?utm_source=CopyBuf (дата обращения: 09.05.2025).

технологий» изучает возможность применения такой идентификации с конца 2023 г.[1]

4. Разработка специальных программ, позволяющих автоматизировать выявление дипфейков, и внедрение их в экспертную деятельность.

5. Изучение механизма совершения преступления и разработка частной криминалистической методики расследования.

Таким образом, полагаем, что проблема выявления случаев использования технологии дипфейка для совершения преступлений требует комплексного решения как на законодательном, так и на технологическом уровне. При этом дальнейшее исследование механизмов совершения преступлений рассматриваемой категории будет способствовать обеспечению эффективности предварительного расследования.

Стремительная цифровизация всех сфер жизни общества оказала существенное влияние на способы совершения преступлений экстремистской и террористической направленности. Особенности криминалистической методики, применяемой в этих случаях, можно охарактеризовать при рассмотрении примеров расследования публичных призывов к осуществлению террористической деятельности, публичного оправдания терроризма или пропаганды терроризма, совершенных с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей, в том числе сети Интернет (ч. 2 ст. 205.2 УК РФ).

В первую очередь при расследовании преступления, ответственность за которое предусмотрена ст. 205.2 УК РФ, следует установить круг обстоятельств, имеющих особое значение:

1) свидетельствует ли заявление лица о признании им идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании (примечание к ст. 205.2 УК РФ);

2) совершены ли названные действия публично, то есть открыто, гласно, с доведением мнения лица, оправдывающего терроризм, до неопределенно широкого круга граждан различными способами, в числе которых использование виновным электронных или ин-

[1] См.: ЦБТ изучает возможность идентификации по сетчатке глаза. URL: https://ria.ru/20231109/identifikatsiya-1908290911.html (дата обращения: 07.05.2025).

формационно-телекоммуникационных сетей, в том числе сети Интернет;

3) присутствует ли прямой умысел (лицо сознает, что публично оправдывает терроризм, и желает совершить это действие).

Основной целью лица при совершении преступлений данной категории (в соответствии с представленной фабулой) является оправдание терроризма.

Спецификой реализации данного способа оправдания терроризма является необходимость совершения действия публично. В большинстве случаев ученые-криминалисты показателем публичности считают осуществленное открытое, гласное, предназначенное для широкого круга лиц выражение своего мнения в устной (выступление) или письменной форме, в том числе с использованием компьютерных сетей (Интернет).

В подтверждение наших доводов приведем следующий пример: в середине июля 2024 г. Владимирские сотрудники Федеральной службы безопасности РФ возбудили дело в отношении местного жителя, который хотел вступить в вооруженные формирования Украины. Как установили сотрудники правоохранительных органов, 28-летний житель г. Коврова Владимирской области оказался причастен к публичному оправданию терроризма и призывам к террористической деятельности. Мужчина был активным пользователем сети Интернет. С начала осуществления специальной военной операции (СВО) он размещал в публичном доступе тексты, формирующие негативное отношение к ней и содержащие призывы к террористической деятельности. Зная, что националистическая проукраинская организация, запрещенная на территории России, является террористической структурой, ковровец все же решил выехать на территорию Украины, чтобы вступить в нее и участвовать в ее деятельности. Мужчина продал мотоцикл, приобрел рюкзак, спальник, ряд других вещей и в июне 2024 г. на поезде приехал в Москву. Далее он собирался лететь на самолете, но был задержан сотрудниками УФСБ России по Владимирской области[1].

[1] См.: ФСБ завела на жителя Владимирской области дело об оправдании терроризма. URL: https://rg.ru/2024/07/11/reg-cfo/fsb-zavela-na-zhitelia-vladimirskoj-oblasti-delo-ob-opravdanii-terrorizma.html (дата обращения: 11.06.2025).

Следует подчеркнуть, что размещение информации, содержащей призывы к террористической деятельности, может осуществляться также пользователями при опубликовании на их открытых страницах в мессенджерах или в социальной сети «ВКонтакте» репостов, содержащих сведения о факте совершенных террористических актов, с высказыванием, выражающим одобрение осуществленных насильственных и аморальных террористических действий в отношении российского государства, признание идеологии и практики терроризма правильными, нуждающимися в поддержке и подражании. Такой репост доступен неограниченному числу пользователей, то есть любому человеку, имеющему компьютер, подключенный к глобальной сети, и интересующемуся такой проблематикой. Кроме того, информационный материал может быть оценен общественностью: просмотревшие ставят реакции, иногда выражают поддержку.

Для подтверждения наших выводов обратимся к следственно-судебной практике. Так, показательным является пример из «Обзора судебной практики Верховного суда № 1 (2020)» (утв. Президиумом Верховного Суда РФ 10.06.2020). 4 июня 2018 г. преступник С. был осужден за публичные призывы к осуществлению террористической деятельности и публичное оправдание терроризма. 16 мая ранее указанного года С. разместил на своей открытой странице в социальной сети «ВКонтакте» изображения, комментарии и т. д., которые обосновывали и оправдывали террористическую деятельность группировок, исповедующих радикальный ислам[1].

С учетом особенностей механизма совершения преступления полагаем необходимым сказать о следовой картине преступления. Анализ существующей правовой доктрины и практики позволяет выделить цифровые следы, которые могут быть обнаружены и изъяты. К ним относятся:

– данные, содержащиеся в памяти электронного носителя информации, с помощью которого пользователь совершил преступление (смартфона, планшета или компьютера типа «ноутбук», включая облачное хранилище);

[1] См.: Обзор судебной практики Верховного Суда Российской Федерации № 1 (2020) (утв. Президиумом Верховного Суда РФ 10.06.2020) // КонсультантПлюс: справ.-правовая сист. Режим доступа: для зарегистрир. пользователей.

– цифровая информация гаджетов и девайсов, позволяющая определить местонахождение их владельца;

– социальные сети, страницы и сайты браузеров, их данные истории, ссылки и репосты в сети Интернет и т. д.

Обнаружение и фиксация указанной информации имеют большое криминалистическое значение, поскольку в результате исследования цифровых следов можно получить сведения, собираемые без ведома самого автора репоста, то есть сайт аккумулирует аналитические данные о том, сколько раз он посещался, каковы примерное местонахождение пользователя, IP-адрес устройства, цифровой портрет деятельности лица, создаваемый встроенным искусственным интеллектом на основе репостов и запросов в сети Интернет.

Также с помощью программного обеспечения «Мобильный криминалист» можно установить связи между владельцем устройства и его контактами, извлечь данные из веб-браузеров, определить в дальнейшем и самые посещаемые сайты, продолжительность активности лица на сайте, в мессенджере и его подключения к сети Интернет, а также восстановить удаленные данные и возможные переписки (отражаются все приложения, графы связей, звонки, геотеги, временные маркеры, в том числе содержащиеся на облачных сервисах).

Кроме того, на первоначальном этапе считаем целесообразным провести исследования текста с привлечением лиц, обладающих специальными знаниями в области психологии и лингвистики для разъяснения смысловых аспектов содержания, поставить перед ними следующие вопросы:

– содержатся ли в тексте репоста пользователя высказывания, оправдывающие террористическую деятельность?

– присутствуют ли лингвистические и психологические признаки оправдания осуществления террористической деятельности?

Полагаем, что применение на практике рассмотренной программы расследования в условиях цифровизации будет в целом способствовать повышению эффективности расследования преступлений экстремистской и террористической направленности.

Важно учитывать такие специфические признаки рассматриваемых преступлений, как

– неочевидность, способность длительное время пребывать в скрытом состоянии; вследствие этого между обнаружением сле-

дов преступления и моментом его фактического совершения образуется большой интервал;

– дистанционность, предполагающая значительную удаленность местонахождения преступника от предмета преступного посягательства (не исключается и такое расположение их относительно друг друга, что преступное деяние подпадает под юрисдикцию разных государств). Согласно правовой позиции, сформулированной Верховным судом РФ в п. 19 постановления Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет"», местом совершения деяния будет являться непосредственно та территория, на которой лицо физически находилось в момент использования различных электронных устройств, в том числе переносных, для совершения IT-преступлений[1];

– высокотехнологичность, делающая для преступника возможным почти мгновенное изменение значительных по объему информационных массивов, а также обусловливающая сложность обнаружения и фиксации цифровых следов преступления;

– трудность выявления и фиксации индивидуальной следовой информации, поскольку большинство преступлений совершается с многопользовательских рабочих мест и удаленных рабочих столов[2].

Изучение уголовных дел рассматриваемой категории позволило выявить следующие недостатки в их расследовании:

1. Несвоевременное возбуждение уголовных дел влечет за собой невозможность раскрытия преступлений данной категории по горячим следам и утрату доказательственной базы. Зачастую длитель-

[1] См.: О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37.

[2] См.: Климова Я. А. Искусственный интеллект и цифровые доказательства в расследовании преступлений, совершенных с использованием современных информационно-коммуникационных технологий // Вестник Волгоградской академии МВД России. 2023. № 1 (64). С. 81–88.

ный срок проверки по материалу обусловлен отсутствием действенного инструментария, позволяющего оперативно документировать цифровые следы преступления – текстовые, аудио- и видеоданные, техническую информацию о месте, времени удаленного подключения, об используемом оборудовании и о взаимодействии пользователя с информационными системами и т. д. Для устранения правовой лакуны МВД РФ внесло на рассмотрение законопроект, содержащий предложение о расширении перечня оперативно-разыскных мероприятий, добавив «Исследование предметов, документов и информации, в том числе содержащейся в технологических системах ее передачи, включая информационно-телекоммуникационную сеть “Интернет”»[1].

2. При расследовании хищений денежных средств с расчетных счетов кредитно-финансовых организаций не в полной мере используются возможности электронного документооборота с банками (например, с ПАО «Сбербанк» и АО «Альфа-Банк»). Вместо того чтобы направлять соответствующие запросы, следователи ограничиваются документами, предоставленными потерпевшими.

3. Не рассматриваются в качестве вещественных доказательств выписки о движении денежных средств по счетам, кассовые чеки, договоры на предоставление кредитных обязательств и иные предметы и документы, полученные в ходе расследования по уголовному делу, вследствие чего также происходит утрата криминалистически значимой информации[2].

Изложенное позволяет сделать вывод об актуальности дальнейшей разработки частной криминалистической методики расследования преступлений, совершенных с использованием современных информационно-коммуникационных технологий. Необходимо определить перечень следственных, организационно-подготовительных и процессуальных действий и разработать научно обосно-

[1] См.: Проект Федерального Закона «О внесении изменения в статью 6 Федерального закона «Об оперативно-розыскной деятельности» от 14 августа 2023 г. // Федеральный портал проектов нормативных правовых актов. URL: https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=140881 (дата обращения: 28.05.2025).

[2] См.: Обзор результатов работы по профилактике, раскрытию и расследованию преступлений в сфере информационно-телекоммуникационных технологий в Волгоградской области за 2023 г. (на основании материалов уголовных дел).

ванные рекомендации по их наиболее оптимальному применению в целях достижения назначения уголовного судопроизводства.

В результате анализа уголовных дел установлено, что при поступлении от граждан заявлений о совершении преступлений с использованием информационно-телекоммуникационных технологий в большинстве случаев следователи в дежурные сутки выполняют минимальный комплекс первоначальных следственных и процессуальных действий.

Для повышения эффективности их работы наука и практика вырабатывают алгоритмы действий следователя. Рассмотрим оптимальную программу первоначального этапа расследования на примере дела о хищении денежных средств с банковского счета потерпевших путем мошенничества с использованием информационно-телекоммуникационных технологий.

Допрос потерпевшего. После вынесения постановления о признании потерпевшим лица, которому преступлением причинен ущерб, необходимо незамедлительно произвести допрос, в ходе которого требуется выяснить следующие обстоятельства:

– обстановку совершения преступления: точное время, дату, место;

– способ совершения преступления (при телефонном мошенничестве собирается информация об абонентском номере, с которого поступил телефонный звонок, о том, кем представился мошенник, каков был предмет разговора со злоумышленником);

– подробное описание голоса преступника (хриплый, высокий, низкий, молодой или старый, наличие акцента, как говорил преступник – медленно или скороговоркой, иные особенности речи). У потерпевшего уточняется, сможет ли он опознать мошенника по голосу (в том числе при предъявлении аудиозаписи голоса), имеется ли у него аудиозапись разговора с мошенником (при наличии специальной программы в его телефоне);

– номер расчетного счета или номер банковской карты, с использованием которой переведены похищенные денежные средства;

– факт использования (или неиспользования) системы быстрых переводов или терминалов кредитных организаций для внесения денежных средств на банковские счета для якобы их сохранения на безопасном счете;

– абонентские номера, на которые были зачислены денежные средства;

– сумму и размер причиненного ущерба, материальное положение потерпевшего.

Следует помнить, как справедливо отметили А. Н. Литвиненко и М. А. Кирилюк, что каждый пользователь мобильной связи является потенциальным объектом атаки телефонных мошенников[1]. В этой связи в ходе допроса потерпевшего необходимо также устанавливать его финансовое поведение (каковы суммы его доходов, ежедневных платежей, проводимых им за оплату товаров, услуг, суммы кредитных обязательств и ежемесячные платежи по ним).

Отдельно отметим технические аспекты производства следственных действий с использованием систем видео-конференц-связи (далее также ВКС).

Требования к помещению и оборудованию для ВКС.

Освещение помещения с ВКС. Функционал системы видеоконференц-связи предъявляет особые требования к освещению помещения, в котором проводятся следственные действия: цветовая температура от 2 700 до 4 000 К. Допустимо также применение флуоресцентных ламп, но следует предусмотреть возможное мерцание, которое, очевидно, окажется заметным на изображении с камеры.

Для обеспечения качественного освещения важно учитывать не только внутреннее оформление помещения, но и его восприятие удаленными участниками. Для предварительной оценки качества освещения можно использовать камеру мобильного телефона в режиме видеосъемки, чтобы выявить возможные проблемы с фокусировкой, резкостью и мерцанием света.

Жалюзи или шторы помогут исключить попадание прямых солнечных лучей на лица участников и объектив камеры (в противном случае возможны эффекты неестественной контрастности и засветки изображения). Не рекомендуется использовать боковую или заднюю подсветку, так как это может вызвать затемнение лиц, появление контуров и теней.

---

[1] См.: Кирилюк М. А., Литвиненко А. Н. Характеристика способов дистанционных хищений денежных средств как этап ситуационного анализа // Вестник экономической безопасности. 2023. № 1. С. 219–225.

Цвет, фон и интерьер. Фон стены, которая находится напротив камеры, имеет первостепенное значение при проведении видеоконференций. Необходимо избегать наличия на заднем плане дверей, окон, отвлекающих элементов и движущихся людей. Рекомендуется разместить на этой стене часы, показывающие местное время. Желательно избегать использования ярко-белого и черного цветов, а также пестрых комбинаций в оформлении помещения. Матовые поверхности на экране выглядят лучше. Важно помнить, что стекло отражает не только свет, но и звук, поэтому желательно не использовать стеклянные предметы и глянцевые поверхности.

Камера для ВКС. Как ни парадоксально, но в видеоконференциях камера не является основным элементом. Тем не менее для комфортной коммуникации важно учитывать особенности планируемого мероприятия при выборе камеры. По крайней мере, камера должна обеспечивать обзор, достаточный для всех участников следственного действия. При необходимости она может увеличивать изображение группы участников или фокусироваться на крупном плане одного из них, если такая функция предусмотрена. Все необходимые настройки камеры удобно сохранять в виде пресетов, и технический ассистент сможет их переключать при необходимости. Актуальные пресеты способны автоматически активироваться при использовании специализированных контроллеров или определенных конгресс-систем. Однако предсказать это сложно. Устройства для съемки во время видеоконференций имеют множество настроек, включая интеллектуальную подсветку изображения, компенсацию мерцания источников света, баланс белого и ручную коррекцию изображения, а также другие функции.

Средство захвата и воспроизведения звука. Высокое качество микрофонов и средств воспроизведения звука – основное требование к системе ВКС.

Спикерфоны часто используются для средних и малых помещений. Оптимальные модели этих устройств устанавливаются на столы, предназначенные для одного или двух человек, и обеспечивают радиус звукового покрытия до 2,5 м. Если стол длиннее, чем радиус действия микрофона, необходимо расширить зону покрытия.

Входящие в комплект аппаратных терминалов спикерфоны и конференц-телефоны позволяют охватить звук по длине стола. Для этого используются дополнительные микрофоны с направленным углом захвата звука.

Конгресс-система применяется, когда конфигурация столов не позволяет использовать спикерфоны или требуется дополнительный функционал от системы захвата звука. Она состоит из блока управления, пульта председателя и пультов делегатов. Проводные пульты подключаются последовательно и имеют встроенные динамики в дополнение к микрофону. Беспроводные микрофонные пульты без динамика обеспечивают более длительное время автономной работы и требуют дополнительной акустики. Беспроводное решение подходит для быстрого удаления пультов со стола или при отсутствии возможности подключения проводки.

Микрофон активируется голосом или вручную в зависимости от модели. Максимальное количество синхронно активных пультов составляет до шести единиц, и первый подключившийся автоматически отключает каждого нового говорящего (принцип FIFO). Пульт председателя при необходимости может отключить микрофоны всех участников.

Востребованные модели конгресс-систем оснащены интегрированной системой управления пресетами камер: автоматически наводят камеру на говорящего при активации микрофона участника. Это удобно при большом количестве участников.

Средство отображения. Количество панелей для видеоконференций и их размер зависят от длины стола и расстояния до самого удаленного участника. Основные принципы таковы: если помещение используется вдоль длинной стороны, дистанционный участник должен находиться на расстоянии не более шестикратной (или восьмикратной – при наличии дополнительных экранов) высоты панели. Если же помещение используется вдоль короткой стороны, расстояние не должно превышать четырехкратной высоты панели. Это необходимо для обеспечения комфорта дистанционных участников при просмотре видеоконференции и демонстрации изображений (документов и т. д.).

Присутствующие очно участники должны сидеть на расстоянии, превышающем две высоты панели, чтобы обеспечить удобный угол обзора и сохранение пропорций изображения.

Разработчики видеоконференций предлагают два варианта использования переговорных комнат (вдоль длинной и короткой сторон) при проектировании. В первом случае, при использовании длинной

стороны, в комнате помещается больше участников и видеоконференция проходит в традиционном формате. Контент и лица участников отображаются на экранах в разных комбинациях. Второй вариант предполагает использование короткой стороны и приближает видеоконференцию к режиму «Телеприсутствие» (Telepresence). Если на каждую панель вывести по одному участнику, размер панели и расстояние до участников обеспечат реалистичное отображение человека, и такая видеоконференция будет создавать эффект личного присутствия всех участников.

Важно принимать во внимание *все особенности* современного оборудования для ВКС.

Камеры для ВКС обычно имеют разрешение Full HD, функцию PTZ (управление камерой на расстоянии с возможностью масштабирования) и множество предустановок (заранее заданных положений).

К основным параметрам относятся угол обзора, кратность оптического увеличения, кратность цифрового увеличения, углы поворота и наклона.

Средства воспроизведения и записи звука разнообразны и выбираются в зависимости от конфигурации и размера комнаты. Для небольших помещений оптимальным решением является использование встроенных динамиков монитора и встроенного в камеру микрофона. Для небольших групп участников в переговорной комнате среднего размера можно использовать комбинированные устройства – спикерфоны со встроенными направленными микрофонами (обычно с охватом в 360 градусов) и динамиками.

В этом случае крайне важно учитывать радиус качественного улавливания голоса. Если стол в переговорной комнате длинный, то используются дополнительные микрофоны или похожие спикерфоны с возможностью каскадирования[1].

Важная роль отводится средствам отображения контента и видео в ВКС. Диагональ экрана – основной параметр при выборе модели. Проекторы сразу исключаем, так как они больше подходят для пре-

[1] См.: Оборудование ВКС для переговорных комнат. URL: http://pcnews.ru/blogs/oborudovanie_vks_dla_peregovornyh_komnat-708118.html (дата обращения: 20.06.2025).

зентаций (чтобы обеспечить необходимую яркость и контрастность, приходится затемнять помещение). Во время видеоконференции средство отображения должно обеспечивать хорошее качество изображения при достаточной освещенности помещения, необходимой для качественной съемки видео.

После завершения всех формальностей к материалам уголовного дела, кроме протокола, добавляется запись проведенного следственного действия на цифровом носителе. Рекомендуется использовать недорогие вместительные и надежные диски – CD-R или DVD-R. Информация может быть записана только один раз, и изменить ее невозможно. Диск упаковывается, и на упаковке делается пояснительная надпись с указанием содержимого и ставятся подписи следователя, специалиста, понятых и других участников следственного действия.

Программное обеспечение. Статья 189.1 УПК РФ предусматривает использование систем видео-конференц-связи государственными органами, осуществляющими предварительное расследование. Содержанием этой статьи в качестве предпочтительного для органов внутренних дел названо использование ИСОД МВД России (а именно модуля СВКС-М): программное обеспечение и техническое оснащение этой системы постоянно совершенствуются.

Программное обеспечение, используемое для проведения следственных действий, должно предоставлять участникам в обоих пунктах связи возможность взаимного наблюдения. Наличие функции распознавания лиц и возможности отключения изображения в одной из точек с сохранением голосовой связи позволит, например, проводить опознание лица в условиях, исключающих визуальное наблюдение опознающего. Все процессы в обоих пунктах связи должны синхронизироваться.

Следователю необходимо иметь возможность составить протокол следственного действия в текстовом редакторе и предоставить его для прочтения в отдаленном пункте связи по своему усмотрению.

Решаемые на данном этапе задачи таковы:

– получение видео с веб-камеры;

– передача аудио- и видеосигналов по сети;

– передача протоколов следственных действий и других документов;

– шифрование передаваемых данных для обеспечения безопасности и сохранения тайны предварительного следствия;

– распознавание и скрытие лица участника следствия при необходимости.

Система должна выполнять следующие функции (рис. 20):

– обеспечивать взаимодействие участников и следователя, передавая видео, звук и файлы;

– визуализировать передаваемую информацию, включая текст протокола, видеоряд и совмещенные видеоряды из разных источников в одном окне;

– исключать визуальное наблюдение одной из сторон путем ретуширования лица на изображении;

– обеспечивать безопасность передаваемых данных;

– захватывать видео с рабочего стола пользователя и с вебкамеры;

– предоставлять доступ к протоколам.

Базовый подход предполагает использование трехзвенной архитектуры «клиент-сервер», состоящей из следующих модулей:

– общая библиотека компонентов, реализующая функции шифрования для клиентской и серверной частей программного обеспечения системы;

– сервер, отвечающий за передачу информации между клиентами;

– «клиент», осуществляющий захват видео и звука, распознавание лиц и их ретуширование, передачу аудио- и видеопотоков и файлов на сервер.

К инфраструктуре сети видео-конференц-связи относится совокупность аппаратно-программных средств администрирования (управления) с использованием различного оконечного оборудования и программного обеспечения – сервера многоточечной видеоконференц-связи (Multipoint Control Unit), системы управления видеоконференциями (учет, управление конфигурацией, безопасностью, производительностью и ошибками узлов, линий и оконечного

оборудования видео-конференц-связи), системы распределения нагрузки распределенных серверов, шлюзы для прохождения трафика через межсетевые экраны, шлюзы с мобильными сетями и абонентами H.320[1].

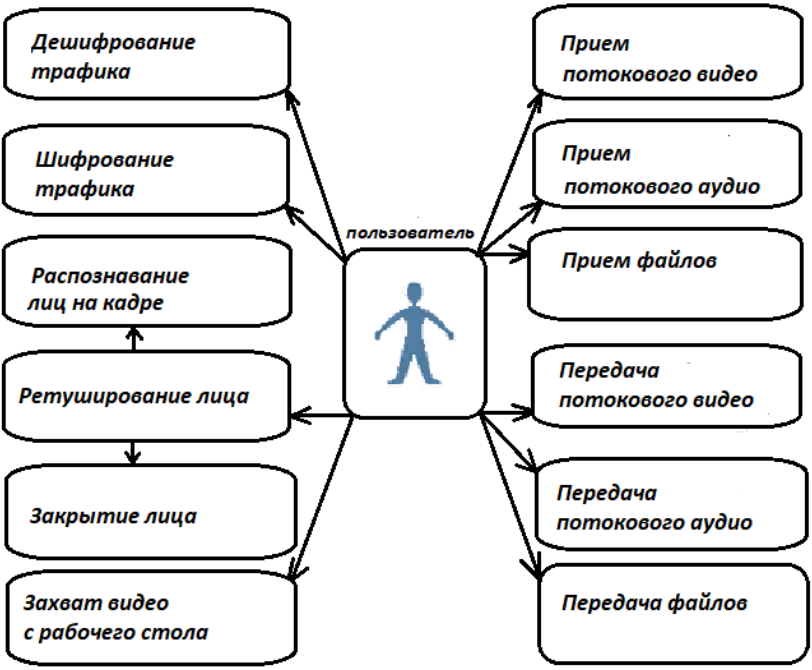


Рис. 20. Функции программного обеспечения для следственных действий в режиме ВКС

Программные средства устанавливаются на персональный компьютер, ноутбук или мобильное устройство. В качестве периферии для захвата и воспроизведения видео и звука могут использоваться

[1] В число стандартов видеоконференций входит известный H.320 на базе ISDN, а также более новые H.323 (сетевой) и H.324 (модемный) – по данным интернет-ресурса Системы конференций для предприятия // On-line библиотека: офиц. сайт. URL: http://www.xserver.ru/computer/nets/internet/87/ (дата обращения: 23.05.2025).

разные устройства – как встроенные (камера, микрофон или динамик), так и внешние (веб-камера, головная гарнитура или спикерфон).

Система управления сетями действует для повышения безопасности сетей видеоконференции и отказоустойчивости, обеспечения их надежности. Система управления сетями видеоконференций должна выполнять следующие функции:

– анализ и обработку ошибок – определение причин отказов и сбоев терминальных и сетевых устройств, обеспечение необходимыми инструментами для обнаружения проблем, выполнение функции по восстановлению работоспособности;

– управление конфигурацией сетевого аппаратно-программного обеспечения (настройка и отслеживание конфигурации);

– учет (детектирование сетевых ресурсов на предмет использования и доступности);

– менеджмент продуктивности (исследование производительности сети, сбор и анализ сведений о функционировании сети для ее эксплуатации на стандартном уровне как для планирования развития сети, так и для оперативного управления ею);

– алармирование (контроль доступа (с обязательным ведением журналов) к сетевым ресурсам и оборудованию для своевременного предотвращения несанкционированного доступа, его обнаружения и пресечения)[1].

Существуют службы, которые находят конкретные уязвимости в корпоративных сетях. Ведутся активные исследования в области программного обеспечения и сервисов операционных систем для обнаружения «угроз нулевого дня» – уязвимостей в программном обеспечении, приводящих к расширению привилегий пользователей, о которых не знают даже разработчики. «Угроза нулевого дня» предоставляет новые возможности для распространения вредоносного кода, которые киберпреступники активно используют для создания эффективных механизмов заражения программного обеспечения. Эти уязвимости используются с помощью так называемых

[1] См.: Фрактальная компетентностная архитектура корпоративных систем дистанционного образования / А. С. Гуртяков, А. Г. Кравец, Д. В. Юдин [и др.] // Современные проблемы науки и образования. 2012. № 3. С. 124–127.

наборов эксплойтов, которые позволяют получить удаленный доступ к операционной системе и осуществить последующую загрузку вредоносного ПО.

Значительная часть «угроз нулевого дня» – это критические уязвимости, иными словами – отсутствие доступных программных патчей и антивирусных сигнатур. Это позволяет злоумышленнику полностью контролировать систему с помощью стандартного хакерского эксплойта. Информационная безопасность становится особенно сложной, когда пользователи игнорируют необходимость установки патчей, даже если они уже выпущены, особенно для программного обеспечения, не являющегося частью операционной системы.

Борьба с эксплуатацией информационных сетей преступными группами, специализирующимися на вымогательстве, мошенничестве, кражах и киберпреступности, а также защита критически важных информационных инфраструктур от кибератак имеют решающее значение для ведомственной информационно-коммуникационной системы[1].

Подготовка (технический сеанс, заявка). Технические характеристики применяемых средств обусловливают необходимость детально продумать пространственное расположение участников следственного действия. Естественно, все они по возможности должны находиться в поле зрения, в объективе видеокамеры. Программное обеспечение должно реализовывать функцию одновременного нахождения в картинке изображений из обоих пунктов соединения, чтобы при воспроизведении действия участников не выглядели разрозненно.

Рекомендуется проведение предварительного технического сеанса связи между помещениями, в которых будет производиться следственное действие. Он позволит отрегулировать проблемные вопросы заблаговременно, продумать все упомянутые обстоятельства и пресеты.

Возникает необходимость заведения в следственных подразделениях журналов приема заявок на производство следственных действий в режиме ВКС. Заявка должна содержать сведения об ини-

[1] См.: Кравец Е. Г. Информационно-коммуникационные технологии как элемент технико-криминалистического обеспечения расследования преступлений: дис. … канд. юрид. наук: 12.00.12. Волгоград, 2016. С. 37.

циаторе, уголовном деле или материале процессуальной проверки, по которому проводится мероприятие, виде планируемого следственного действия, времени и прогнозируемой продолжительности его производства, удаленном объекте, количестве участников. Естественно, и заявка, и журнал должны существовать и пополняться в электронном виде.

Необходимость выработки единых технических правил производства следственных действий с использованием систем видеоконференц-связи обусловлена незначительной практикой их применения при расследовании уголовных дел. Отсутствие единого подхода при реализации возможностей ВКС влечет за собой принятие правоприменителями различных технических решений.

С учетом сказанного в практике расследования возникают следующие сложности технического характера:

– дополнительная потребность в лимитах бюджетных средств на создание в изоляторах временного содержания территориальных органов МВД России на районном уровне телекоммуникационной инфраструктуры;

– организация каналов передачи данных для подключения соответствующего оборудования к подсистеме ВКС государственной автоматизированной системы «Правосудие».

Выемка. При необходимости изъятия предметов и документов, имеющих значение для дела, у потерпевшего нужно произвести выемку мобильного телефона, на который поступил звонок, и документов, содержащих сведения о совершенном преступлении.

При описании изъятого мобильного телефона в протоколе обязательно указываются:

– индивидуальные признаки устройства (размер, цвет, материал, идентифицирующие признаки: царапины, сколы, потертости, трещины и их расположение);

– точное наименование устройства (марка, модель, год выпуска);

– IMEI-код мобильного телефона (при этом устанавливается, имеет ли телефон несколько кодов IMEI);

– абонентский номер, который использовался в телефоне, информация о том, на кого он зарегистрирован, какому мобильному оператору принадлежит, номер сим-карты;

– наличие или отсутствие защитного пароля. Если пароль имеется, то отразить, какой именно (ПИН-код, буквенно-цифровой пароль, графический ключ, Face ID, сканер отпечатков пальцев).

При необходимости отключается защита.

Специалист, участвующий в следственном действии, может применять специализированные программные комплексы с использованием алгоритма искусственного интеллекта (например, «Мобильный криминалист»). Работа с программным комплексом позволяет извлекать информацию в полном объеме, даже восстанавливать удаленные файлы. Если этого требуют условия расследования, устанавливаются графы взаимосвязей, геолокационные данные, временные метки.

Заслуживают особого внимания особенности порядка изъятия и упаковки мобильных телефонов (смартфонов), поскольку мобильный телефон является ценным источником криминалистически значимой информации. После осмотра на телефоне следует установить «авиарежим», чтобы исключить удаленный доступ к его содержимому.

Интересна специфика обнаружения и изъятия объектов при расследовании криптовалютных преступлений. С каждым годом количество преступлений, совершенных в сфере криптовалют и цифровых активов, только возрастает. Прогрессирующая популярность криптовалют (таких, например, как биткоин и эфириум) делает их привлекательными для мошенников, хакеров и других преступников. В большинстве случаев преступления, связанные с реализацией криптовалюты, направлены на кражу цифровых активов, обман инвесторов или получение возможности уклонения от налогов и отмывания денег.

Данные международных отчетов свидетельствуют о том, что около 60 % всех случаев финансовых преступлений с использованием криптовалют связаны с мошенничеством и хищением средств. Возрастает число «схем Понци» (здесь криптовалюта используется для создания «финансовых пирамид»). Эти преступления охватывают не только местные, но и трансграничные операции, что усложняет их расследование. Поскольку трансграничный характер действий вызывает сложности в работе следствия, мошенничество с использованием криптовалюты преследуется по закону в различных странах, юрисдикциях.

Криптовалюты анонимны и неотслеживаемы. Криптовалютная система децентрализована, то есть центрального сервера, администратора или менеджера нет. Она основана на сети, распределенной в большом количестве компьютеров, пользователи которых выполняют транзакции через приложения на смартфонах или компьютерах. Поэтому для того, чтобы правоохранительные органы могли заморозить и конфисковать криптовалюту, им необходимо получить контроль над криптовалютным кошельком пользователя и перевести преступные доходы на кошелек, принадлежащий правоохранительным органам.

Национальные меры реагирования на криптовалютные риски должны включать следующие компоненты:

– понимание (повышение уровня знаний политиков, правоохранительных и надзорных органов в области криптовалюты, достижение ими высокого уровня осведомленности о том, как эти средства работают);

– расследование (создание потенциала правоохранительных органов для отслеживания движения криптовалюты);

– изъятие и конфискацию;

– регулирование и надзор;

Отслеживание, изъятие, конфискация и регулирование криптовалют основаны на этих компонентах.

Экономическое преступление, совершенное с использованием криптовалюты, включает широкий спектр действий, таких как хищение активов, схемы «финансовых пирамид» и отмывание денег. Несмотря на то что многие страны до сих пор работают над нормативной регуляцией криптовалютного рынка, законодательство их уже предусматривает уголовную ответственность за подобные действия.

Во многих странах криптовалюта признается имуществом, значит, полиция может возбуждать уголовные дела о кражах криптоактивов.

Криптовалютные преступления децентрализованны и глобальны. Эти средства не привязаны к государственным институтам и могут быть перемещены по всему миру в течение считанных минут, чем обусловлена сложность работы правоохранительных органов, вынужденных координировать свои действия с международными партнерами.

Расследование рассматриваемого вида преступлений часто включает в себя работу не только с блокчейн-данными. Если доказана причастность к мошенничеству, отмыванию денег или финансированию терроризма с использованием криптовалют, то обвиняемому грозит наказание.

Примеры недавних дел показывают, что суды все чаще выносят реальные сроки за экономические преступления с криптовалютами. Новостные сводки во всем мире в последнее время пестрят заголовками о суде над криптомошенниками.

Законодательство о криптовалютах развивается стремительно. Иллюстрируют это, в основном, примеры из зарубежного опыта. Так, в 2023 г. шесть фигурантов дела о мошеннической схеме AirBit Club были осуждены в США за создание глобальной криптовалютной пирамиды, действовавшей с 2015 г. Организаторы AirBit Club обещали своим участникам пассивный доход от инвестиций в криптовалюты, однако никакие реальные операции с криптовалютой не осуществлялись. В общей сложности жертвами схемы стали тысячи людей во всем мире, потерявшие более $ 100 млн. Ключевые фигуранты дела – Пабло Родригес и Гутемарас Гарса – были признаны виновными в мошенничестве с использованием электронных средств связи и отмывании денег. В апреле 2023 г. суд вынес им приговоры – до 12 лет лишения свободы, а также наложил на них обязательство вернуть средства пострадавшим инвесторам.

Едва ли не самым громким криптовалютным скандалом последних лет стало дело FTX – одной из крупнейших криптовалютных бирж, основанной Сэмом Бэнкманом-Фридом. В 2022 г. биржа внезапно объявила о банкротстве, а затем выяснилось, что руководство FTX использовало средства клиентов для поддержания связанных компаний, таких как Alameda Research. По оценкам, ущерб составил более $ 10 млрд, что привело к массовым потерям средств инвесторами. В 2023 г. Сэм Бэнкман-Фрид был арестован и обвинен в мошенничестве с ценными бумагами, отмывании денег и незаконном использовании средств клиентов. В октябре 2023 г. суд признал его виновным по нескольким статьям, фигуранту грозило наказание – до 115 лет лишения свободы. Это дело потрясло криптовалютное сообщество и поставило под сомнение возможность регулирования деятельности криптовалютных бирж.

Главное следственное управление по Москве расследует уголовное дело в отношении создателей анонимной платежной системы UAPS и криптовалютной биржи Cryptex. В сентябре 2024 г. следователи задержали уже 96 фигурантов. Сейчас их доставляют в Москву для проведения следственных действий, а после, как ожидается, районный суд будет рассматривать ходатайства следствия об избрании им мер пресечения.

По версии следствия, преступное сообщество было создано еще в 2013 г. фигурантами с целью личного обогащения. Как установили следователи, соучастники разработали инфраструктуру в виде анонимной платежной системы UAPS, криптовалютной биржи Cryptex и 33 онлайн-сервисов. Основными клиентами последних являлись киберпреступники и хакеры, которые пользовались услугами упомянутых сервисов для легализации своего преступного дохода. Только за 2023 г., как оценили в СК, оборот поступивших денежных средств в сервисы преступного сообщества составил более 112 млрд руб., а преступный доход фигурантов – 3,7 млрд руб.

В рамках расследования оперативники провели 148 обысков в местах, где жили и осуществляли преступную деятельность организаторы и участники ОПС. Cryptex («Криптекс») позиционирует себя как «выгодная биржа криптовалют», где можно «безопасно купить (продать) криптовалюту». Компания зарегистрирована на Карибских островах. В сентябре минфин США ввел санкции против сервиса.

Бывший следователь, адвокат Александр Бурчук, отметил, что криптовалюты как средства платежа в настоящее время не легализованы и вся деятельность по их обороту в серой зоне, пока не разработаны и не введены четкие правила контроля со стороны ЦБ. «Все нормативные акты, направленные на это, еще не предполагают активного законного использования криптовалюты как средства платежа и механизмов исполнения 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» от 2001 г.

Адвокат указал, что пока правоприменители привлекают только за использование криптовалюты в противозаконных целях – телефонное мошенничество, уклонение от уплаты налогов и легализацию. Но, судя по трендам, рассуждает юрист, в ЕС и США уже происходит радикальное ужесточение контроля уголовно-правовыми

методами криптобирж и обменников. «Это одно из первых таких дел в России, но далеко не последнее», – убежден он.

Бурчук напомнил также, что спецкомитет ООН по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях представил странам-участницам на голосование вторую редакцию такой конвенции.

Практика расследования подобных дел по ст. 172 УК сейчас сложная: трудно посчитать все безналичные переводы на карту и выяснить точную сумму, извлеченную фигурантами в криптовалюте.

Действительно, подобные дела в России пока возбуждаются не часто. Но это не первое. Например, в 2022 г. ФСБ России начала расследовать дело по запросу США в отношении ряда участников группировки REvil. Тогда задержанным фигурантам было предъявлено обвинение только в неправомерном обороте средств платежей (ч. 2 ст. 187 УК).

Криптовалютные транзакции анонимны, однако, несмотря на это, способы отследить транзакции существуют. Следователям необходимо выяснить путь транзакции (монеты) до «привратника» (обменного пункта или дилера), запросить информацию о личности клиентов «привратника», а затем отследить цепочку транзакций.

Чтобы эффективно отслеживать действия с криптовалютой, государственным органам необходимо:

1. Иметь специализированное программное обеспечение, позволяющее осуществлять мониторинг движения потоков криптовалют.

2. Обучать следователей навыкам по отслеживанию потоков криптовалюты.

В большинстве случаев единственным способом изъятия и конфискации криптовалютных монет является установка пароля (известного как «личный ключ») и перевод монет на криптовалютный кошелек правоохранительных органов.

Для этого сотрудники полиции должны искать «артефакты криптовалюты», материальные носители, содержащие тайные ключи, например, двенадцать слов, которые составляют «фразу восстановления». Чаще всего эти артефакты находят при обыске автомобилей и помещений или при задержании подозреваемых.

Интересен региональный опыт в этой сфере. Согласно п. 1.10 распоряжения МВД России от 29 сентября 2023 г. №1/11584 расследование уголовных дел о преступлениях, связанных с «финансовыми пирамидами», находится на особом контроле.

ГСУ ГУ МВД России по Волгоградской области проведен анализ результатов расследования уголовных дел о преступлениях анализируемой категории за 2023 г.

В качестве положительного примера можно привести уголовное дело № 11901780018000120, находившееся в производстве СЧ ГСУ ГУ МВД России по Волгоградской области, по обвинению участников организованной преступной группы в совершении тяжкого преступления, предусмотренного ч. 4 ст. 159 УК РФ, расследованное по факту осуществления организованной преступной группой хищений на территории Волгоградской, Ярославской, Ивановской, Московской, Самарской, Саратовской областей денежных средств граждан на общую сумму более 326 млн руб. под видом деятельности иностранной финансово-инвестиционной компании E-Z Finance Group.

Особую сложность в процессе расследования по уголовному делу представляли необходимость юридической оценки действий участников преступной группы, совершивших преступление, носящее межрегиональный характер, в течение длительного периода – с 2014 по 2019 г., доказывание их умысла на совершение преступления в условиях использования межотраслевого (уголовного, гражданского, финансового, страхового) законодательства, объем уголовного дела, составляющий более 300 томов, проведение по уголовному делу значительного количества следственных и процессуальных действий, направленных на сбор и закрепление доказательств виновности участников преступной группы, на значительном отдалении от места их производства (на территории Волгоградской, Ярославской, Московской, Саратовской, Самарской, Ивановской областей проведено более 7 000 различных следственных и процессуальных действий, среди которых допросы потерпевших, свидетелей, обвиняемых, подозреваемых, выемки, обыски, осмотры, запросы, компьютерные судебные экспертизы и иные), а также сбор и анализ документации и финансово-хозяйственных операций по деятельности преступной группы, количеством в несколько тысяч.

Расследование уголовного дела имело большую общественную значимость, поскольку участниками организованной группы был причинен материальный ущерб более чем 700 потерпевшим на общую сумму, превышающую 326 млн руб. 21 июля 2023 г. прокуратурой Волгоградской области было утверждено обвинительное заключение в отношении указанных участников организованной группы, после чего уголовное дело было направлено в суд г. Волгограда для рассмотрения по существу[1].

Вместе с тем в последние годы отмечается трансформация такого способа совершения преступлений, как «финансовая пирамида»: традиционные формы преступлений сменяются дистанционным привлечением денежных средств, криптовалюты, цифровой валюты в форме инвестиционных интернет-проектов.

Наряду с достижением положительных результатов в работе по преступлениям анализируемой категории необходимо отметить наличие объективных проблем.

Так, неэффективность организации работы следственных подразделений нашла выражение в факте необоснованного приостановления предварительного следствия без проведения необходимых следственных действий. Имеется и такая проблема в расследовании уголовных дел: в кредитных кооперативах ведется двойная бухгалтерия, денежные средства, поступающие в кассу, не проводятся по расчетным счетам, а распределяются наличным способом. Подобная ситуация значительно осложняет проведение документальной проверки финансово-хозяйственной деятельности предприятий и не позволяет не только установить в полном объеме общий оборот финансов кооператива, но и определить конечное движение денежных средств.

Значительно осложняет выявление и документирование преступной деятельности «финансовых пирамид» и тот факт, что данный вид преступлений относится к категории преступлений частного обвинения, и законодательно невозможно доказать противоправную деятельность организаторов «финансовых пирамид» до тех пор, пока не появится хотя бы одно заявление от вкладчиков –

[1] См.: Обзор ГСУ ГУ МВД России по Волгоградской области «О результатах расследования уголовных дел о преступлениях, связанных с «финансовыми пирамидами» за 12 месяцев 2023 года» (по материалам уголовных дел).

потерпевшей стороны. При этом преступный замысел будет весьма очевиден, но проведение каких-либо следственных мероприятий – невозможно.

Весьма значимым в пресечении данного вида преступлений является активное участие средств массовой информации. Однако в настоящее время работа СМИ, связанная с профилактической деятельностью, позволяющей упреждать случаи участия населения в «финансовых пирамидах», незначительна. Очень немногие информационные компании (в основном, специализированные издания «Высота 102» и др.) публикуют информацию об участившихся фактах преступной деятельности кредитных кооперативов и призывают население проявлять бдительность и не участвовать в сомнительных финансовых операциях.

Важное значение в расследовании преступлений в условиях цифровизации имеет производство следственного действия.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами. В случаях осуществления звонков с использованием программ по подмене номера с целью установления лиц, совершивших преступление, необходимо получить протоколы соединений абонентского номера потерпевшего онлайн через личный кабинет потерпевшего либо по постановлению суда – у оператора сотовой связи. В последнем случае необходимо направить в суд ходатайство о разрешении получения у оператора связи сведений о соединениях между абонентами и абонентскими устройствами.

После получения информации можно установить абонентский номер, использованный мошенником для совершения звонка, определить дату, время, продолжительность соединения. Указанная информация требуется для направления запросов операторам связи.

Ходатайство в суд о разрешении на получение у оператора связи сведений о соединениях между абонентами и абонентскими устройствами по номерам телефонов, использованным мошенником для совершения преступления, должно также содержать возможность получения у оператора связи информации об IMEI-кодах устройства, а также использованных с данным IMEI-кодом сим-картах, информации о способах оплаты за услуги связи (номера счетов, электронных кошельков, с которых она поступила).

Необходимо своевременно направить *запросы* в различные организации (рис. 21).

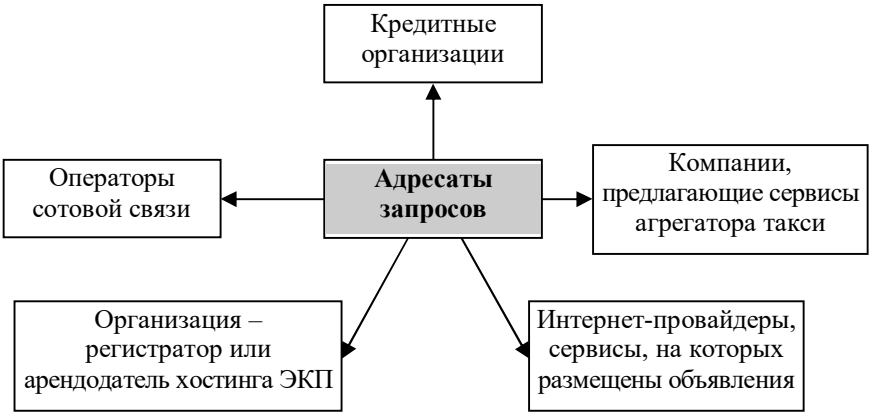


Рис. 21. Схема направления запросов в организации

В целях получения криминалистически значимой информации от учреждений финансово-кредитной системы, интернет-провайдеров, операторов сотовой связи и интернет-сервисов при расследовании уголовных дел о преступлениях, совершенных с использованием информационно-телекоммуникационных технологий, организовано взаимодействие следственных органов посредством электронного документооборота с различными коммерческими организациями.

Так, в рамках электронного взаимодействия не позднее дня направления электронного запроса (в среднем, в течение одного часа) направляются ответы операторами сотовой связи АО «Мегафон» и ООО «Т2 Мобайл», учреждениями финансово-кредитной системы ПАО «Сбербанк», АО «Альфа-Банк», ПАО «ВТБ», ООО НКО «ЮMoney» (Яндекс. Деньги).

В запросе оператору сотовой связи, которому принадлежит номер телефона потерпевшего, целесообразно отразить необходимость предоставления информации о том, откуда поступил вызов (интернет-провайдер либо компания, предоставляющая услуги в сфере IP-телефонии). В запросе обязательно указать номер телефона потерпевшего, номер телефона, с которого поступил звонок, дату, время и продолжительность телефонного соединения.

После этого в организацию, название которой сообщено в ответе, направляется запрос о предоставлении регистрационных данных абонента, использовавшего номер телефона, с которого поступил звонок потерпевшему (указываются дата телефонного соединения, время поступления звонка, длительность разговора), номера использованного оборудования, IP-адреса, шлюза, номера trunk, данных об использованном программном обеспечении, виртуальной АТС, МГТС, АТС, направлении соединения, адреса интернет-ресурса. Среди прочих можно получить и сведения о способах оплаты за использование интернет-трафика.

При поступлении ответа, в котором указана иная организация, направляется соответствующий запрос о получении аналогичных сведений. Запросы следует направлять до тех пор, пока не будет получен конечный ответ из организации, подтверждающей, что при осуществлении указанных соединений использовались их оборудование, учетные записи и IP-адреса.

Отметим, что факт использования подменного номера устанавливается при направлении запроса оператору связи, владеющему абонентским номером, использованным мошенником. Необходимо запросить сведения о том, поступал ли с данного абонентского номера звонок потерпевшему в ту дату и в то время, когда ему звонил мошенник. Если оператор связи сообщает о том, что с указанного в запросе абонентского номера звонок потерпевшему не осуществлялся или номер телефона никому не выделялся, есть все основания полагать, что номер телефона мошенником подменен.

Самыми популярными сайтами у мошенников являются Avito.ru, «Юла», «Яндекс.Такси», а также социальные сети «ВКонтакте», Instagram и мессенджеры WhatsApp* и Telegram. Сбербанк-онлайн, Qiwi Wallet и ФК «Открытие» – наиболее часто используемые для преступной деятельности приложения.

При получении сведений об IP-адресе требуется направить запрос в компанию-провайдер, которой выделен данный адрес, для получения информации о лице, которому он предоставлен. При этом важно указать дату и время его использования, адресата (сайт или иной интернет-ресурс). Следует помнить, что возможность уста-

* Социальная сеть Instagram и мессенджер WhatsApp принадлежат компании Meta, которая признана экстремистской и запрещена в РФ.

новления принадлежности динамического IP-адреса (например, оператора связи) зависит от точности указанного в запросе периода его использования мошенником (то есть необходимо указывать в запросе дату и время с точностью до секунд).

Для определения провайдера IP-адреса следует проверить его по специальному Whois-сервису для проверки доменов, позволяющему установить организацию, которой принадлежит IP-адрес, и даже информацию о хостинг-площадке, предоставляемой сайту[1].

Использование подсистемы ИБД-Ф «Дистанционное мошенничество».

Своевременное внесение информации о возбуждении уголовного дела и сведений, полученных на первоначальном этапе расследования, позволяет в кратчайшие сроки выявлять преступления, совершенные одними и теми же лицами, «серийность». Это дает основание соединять в одном производстве уголовные дела, возбужденные в различных регионах Российской Федерации.

Вместе с тем следует акцентировать внимание на тактических особенностях производства отдельных следственных действий, направленных на сбор и закрепление «цифровых» следов преступления, в том числе размещенных на электронных носителях информации, в сети Интернет (включая облачные хранилища) и других социальных сетях.

Именно высокотехнологичность способа совершения преступлений предопределяет особенности производства отдельных следственных действий. Отметим, что данная характеристика указывает на необходимость повсеместного применения знаний специалистов – не только системы МВД, но и иных учреждений, в том числе относящихся к негосударственной сфере.

Представленный алгоритм носит общий характер, но с учетом конкретных обстоятельств расследуемого уголовного дела может быть использован в качестве рекомендации при расследовании преступлений, совершенных с использованием информационно-телекоммуникационных технологий.

В связи со всем вышесказанным особую актуальность приобретает вопрос о необходимости специализации следователей и возни-

[1] См.: Whois-сервис для проверки доменов. URL: http://www.whois-service.ru (дата обращения: 11.06.2025).

кают многочисленные дискуссии о целесообразности появления IT-следователя, киберследователя. Указанное направление требует отдельного научного осмысления.

Полагаем, что применение на практике рассмотренной программы расследования будет в целом способствовать повышению эффективности организации и методики расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий. Мы видим огромный потенциал в применении современных технологий для раскрытия и расследования преступлений, а также при проведении отдельных следственных действий, но это направление требует дальнейшего научного изучения.

Таким образом, в настоящее время возникает объективная необходимость исследования проблем использования современных цифровых технологий для эффективного расследования преступлений и разработки тактических рекомендаций по производству отдельных следственных действий с учетом интеграции цифровых технологий, что подчеркивает актуальность обращения к избранной теме.

ЗАКЛЮЧЕНИЕ

Проведенное исследование актуальных проблем организационно-тактического обеспечения расследования преступлений в условиях цифровизации позволяет констатировать наличие достигнутых результатов, сформулировать определенные выводы и предложения.

Раскрыто понятие цифровой криминалистики, выявлены предпосылки ее возникновения, проанализированы существующие точки зрения на содержание этого понятия, предложено авторское определение.

Рассмотрены вопросы технико-криминалистического обеспечения расследования преступлений, имеющего особое значение для обнаружения, изъятия и фиксации цифровых доказательств в целях эффективного расследования современных преступлений, подчеркнута важность использования технологии искусственного интеллекта.

Проведен анализ тактических особенностей производства отдельных следственных действий и использования специальных знаний при расследовании преступлений в условиях цифровизации.

На монографическом уровне рассмотрены проблемы уголовно-процессуальной регламентации и криминалистического обеспечения расследования в условиях цифровизации. Предложено определение понятия цифровизации; сформулированы задачи расследования преступлений; разработана классификация современных цифровых технологий применительно к деятельности по расследованию преступлений; охарактеризована специфика регламентации цифровых доказательств в уголовном судопроизводстве; проанализировано правовое регулирование собирания (обнаружения, фиксации, изъятия) цифровых доказательств; исследованы понятие и перспективы цифровой криминалистики; определены особенности организационно-тактического обеспечения расследования преступлений, тактики проведения отдельных следственных действий с учетом интеграции цифровых технологий, а также использования специальных знаний.

Реализация возможностей цифровой криминалистики позволит эффективно выявлять, раскрывать и расследовать различные преступления: совершенные с использованием информационно-телекоммуникационных технологий, традиционные, неочевидные преступления прошлых лет. Цифровая криминалистика, постепенно

занимающая лидирующие позиции, может произвести революцию в расследовании преступлений, поскольку способствует переосмыслению существующих традиционных методик расследования различных видов и групп преступлений и разработке новых – действенных, эффективных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Нормативные правовые акты

1. Конституция Российской Федерации, принята всенародным голосованием 12 декабря 1993 г. с изм., одобренными в ходе общероссийского голосования 1 июля 2020 г. // КонсультантПлюс : справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_28399 (дата обращения: 17.06.2025).

2. Уголовно-процессуальный кодекс Российской Федерации : федер. закон от 18 декабря 2001 г. № 174-ФЗ // КонсультантПлюс : справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_34481 (дата обращения: 17.06.2025).

3. Уголовный кодекс Российской Федерации : федер. закон от 13 июня 1996 г. № 63-ФЗ // КонсультантПлюс : справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 17.06.2025).

4. Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 149-ФЗ // КонсультантПлюс : справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 17.06.2025).

5. О полиции : федер. закон от 7 февраля 2011 г. № 3-ФЗ // КонсультантПлюс : справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 17.06.2025).

6. Национальная стратегия развития искусственного интеллекта на период до 2030 года, утв. Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации». – URL : https://a-ai.ru/wp-content/uploads/2024/03/Национальная_стратегия_развития_ИИ_2024.pdf?ysclid=mcy7k7yv46402130895 (дата обращения: 17.06.2025).

7. О национальных целях развития Российской Федерации на период до 2030 года : указ Президента РФ от 21 июля 2020 г. № 474 // КонсультантПлюс: справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_357927/ (дата обращения: 17.06.2025).

8. О Стратегии национальной безопасности Российской Федерации : указ Президента Российской Федерации от 2 июля 2021 г. № 400 // КонсультантПлюс : справ.-правовая сист. – URL :

https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 17.06.2025).

Научная, учебная и учебно-методическая литература

9. Актуальные вопросы криминалистической тактики : науч.-практ. пособие / под общ. ред. проф. И. М. Комарова. – Москва : Юрлитинформ, 2018. – 176 с. – ISBN 978-5-4396-1649-7.

10. Алгоритмизация следственной деятельности : монография / под ред. Е. П. Ищенко. – Москва : Юрлитинформ, 2010. – 304 с. – ISBN 978-5-93295-723-3.

11. Бахтеев, Д. В. Искусственный интеллект. Этико-правовые основы : монография / Д. В. Бахтеев. – Москва : Проспект, 2021. – 176 с. – ISBN 978-0-01-688249-4.

12. Белкин, Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы современной криминалистики / Р. С. Белкин. – Москва : НОРМА : ИНФРА-М, 2001. – 240 с. – ISBN 5-89123-493-9.

13. Белкин, Р. С. Курс криминалистики : учебник для вузов / Р. С. Белкин. – 3-е изд., доп. – Москва : ЮНИТИ-ДАНА : Закон и право, 2001. – 835 с. – ISBN 5-238-00198-3.

14. Бессонов, А. А. Искусственный интеллект и математическая статистика в криминалистическом изучении преступлений : монография / А. А. Бессонов. – Москва : Проспект, 2021. – 816 с. – ISBN 978-5-392-34143-6.

15. Использование искусственного интеллекта при выявлении, раскрытии, расследовании преступлений и рассмотрении уголовных дел в суде : монография / под ред. С. В. Зуева, Д. В. Бахтеева. – Москва : Юрлитинформ, 2022. – 214 с. – ISBN 978-5-4396-2315-0.

16. Криминалистика : учебник / О. В. Челышева, К. И. Сотников, Г. Ю. Лутошкин [и др.] ; под общ. ред. О. В. Челышевой. – Санкт-Петербург : Р-КОПИ, 2017. – 580 с. – ISBN 978-5-9500351-5-9.

17. Криминалистика. Словарь терминов и определений / сост. А. В. Бачиева, А. Н. Виноградова. – Санкт-Петербург : Санкт-Петербургский университет МВД России, 2015. – 40 с.

18. Максуров, А. А. Обеспечение информационной безопасности в сети Интернет : монография / А. А. Максуров. – Москва : ИНФРА-М, 2023. – 226 с. – ISBN 978-5-16-018251-3.

19. Подобных, А. В. Цифровая криминалистика распределенных реестров : учеб.-метод. пособие / А. В. Подобных, Н. В. Мануйлова. – Санкт-Петербург : Самиздат (ЛитРес). – 2024. – 82 с. – ISBN 978-5-04-625144-9.

20. Тактика применения средств видеофиксации при производстве следственных действий : учеб.-метод. пособие / Э. Д. Нугаева, З. И. Харисова, С. А. Рябчиков [и др.]. – Уфа : Уфимский ЮИ МВД России, 2024. – 80 с.

21. Тактика следственного осмотра и исследования цифровой информации средств телекоммуникации и интернета : учеб.-практ. пособие / А. Р. Акиев, К. И. Сотников. – Санкт-Петербург : СПбУ МВД России, 2023. – 68 с. – ISBN 978-5-91837-716-1.

22. Тьюринг, А. М. Может ли машина мыслить? / А. М. Тьюринг ; пер. с англ. Ю. А. Данилова ; под ред. и с предисл. С. А. Яновской. – Москва : УРСС : ЛЕНАНД, 2016. – 110 с. – ISBN 978-5-9710-2758-4.

23. Цифровая криминалистика : учебник для вузов / под ред. В. Б. Вехова, С. В. Зуева. – 2-е изд., перераб и доп. – Москва : Юрайт, 2024. – 490 с. – ISBN 978-5-534-17464-9.

24. Цифровые следы преступлений : монография / А. М. Багмет, В. В. Бычков, С. Ю. Скобелин, Н. Н. Ильин. – Москва : Проспект, 2021. – 168 с. – ISBN 978-5-392-32868-0.

25. Цифровые технологии и право : сб. науч. тр. II Междунар. науч.-практ. конф. (г. Казань, 22 сентября 2023 г.). В 6 т. / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило [и др.]. – Казань : Изд-во «Познание» Казанского инновационного университета, 2023. – Т. 2. – 316 с. – ISBN 978-5-8399-0767-6.

Научные статьи

26. Арутюнян, Д. А. Цифровизация процессуальных действий: путь к ускорению и удешевлению производства по уголовному делу / Д. А. Арутюнян, О. Е. Головкин // Вестник Санкт-Петербургского университета МВД России. – 2022. – № 2 (94). – С. 89–94.

27. Баранов, А. М. Правила производства следственных действий или способов собирания доказательств / А. М. Баранов // 25 лет на службе Отечеству : сб. науч. тр., посвященный деятельности научных школ Санкт-Петербургского университета МВД России и приуроченный к 25-летию со дня его образования / сост.: О. И. Городо-

вая, О. С. Кравченко, А. А. Жаворонкова. – Санкт-Петербург : Санкт-Петербургский университет МВД России, 2023. – С. 325–330.

28. Батоев, В. Б. Использование технологии Deepfake в преступной деятельности: проблемы противодействия и пути их решения / В. Б. Батоев, А. В. Пучнин // Вестник Воронежского института МВД России. – 2023. – № 1. – С. 165–169.

29. Бахтеев, Д. В. Векторы цифрового развития криминалистики / Д. В. Бахтеев // Технологии XXI века в юриспруденции : материалы Шестой всерос. науч.-практ. конф., Екатеринбург, 24 мая 2024 г. – Екатеринбург, 2024. – С. 13–17.

30. Бахтеев, Д. В. Искусственный интеллект в криминалистике: состояние и перспективы использования / Д. В. Бахтеев // Российское право: образование, практика, наука. – 2018. – № 2 (104). – С. 43–49.

31. Бахтеев, Д. В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц / Д. В. Бахтеев // Российское право: образование, практика, наука. 2016. – № 3 (93). – С. 24–26.

32. Бессонов, А. А. К вопросу о цифровизации уголовного судопроизводства в Российской Федерации / А. А. Бессонов // Уголовный процесс и криминалистика: правовые основы, теория, практика, дидактика (к 75-летию со дня рождения профессора Б. Я. Гаврилова) : сб. науч. ст. по материалам междунар. науч.-практ. конф., Академия управления МВД России, 3 ноября 2023 г. – Москва : Академия управления МВД России, 2023. – С. 26–32.

33. Бессонов, А. А. О некоторых возможностях современной криминалистики в работе с электронными следами / А. А. Бессонов // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2019. – № 3 (55). – С. 46–52.

34. Бормотова, Л. В. Искусственный интеллект в производстве по уголовным делам / Л. В. Бормотова // Цифровые технологии и право : сб. науч. тр. II Междунар. науч.-практ. конф. (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило [и др.]. В 6 т. Т. 2. – Казань : Изд-во «Познание» Казанского инновационного университета, 2023. – С. 51–58.

35. Буглаева, Е. А. Перспективы применения технологий искусственного интеллекта в сфере судопроизводства / Е. А. Буглаева // Вестник ЮУрГУ. Серия «Право». – 2024. – Т. 24, № 1. – С. 10–15.

36. Бычков, В. В. Электронное следообразование преступной деятельности в сети Интернет / В. В. Бычков, В. Б. Вехов // Расследование преступлений: проблемы и пути их решения. – 2020. – № 1 (27). – С. 106–111.

37. Вехов, В. Б. Формирование стратегий расследования преступлений на основе положений электронной криминалистики / В. Б. Вехов, П. С. Пастухов // Ex jure. – 2019. – № 4. – С. 129–141.

38. Воробьева, И. Б. Применение больших данных (big data) при прогнозировании и расследовании преступлений / И. Б. Воробьева // Вестник Саратовской государственной юридической академии. – 2021. – № 3 (140). – С. 195–202.

39. Гаврилин, Ю. В. Цифровая форма фиксации доказательственной информации по делам о преступлениях экономической направленности / Ю. В. Гаврилин, П. В. Севастьянов // Криминалистическое обеспечение безопасности Российской Федерации в финансовой сфере (65-е ежегодные Криминалистические чтения) : сб. науч. ст. по материалам междунар. науч.-практ. конф. В 2 ч., Москва, 24 мая 2024 г. – Москва : Академия управления МВД России, 2024. – С. 16–22.

40. Гладышева, О. В. Искусственный интеллект и цифровые (электронные) доказательства в уголовном судопроизводстве / О. В. Гладышева, В. А. Семенцов, Я. В. Лошкобанова // Юридический вестник Кубанского государственного университета. – 2024. – № 1. – С. 89–99.

41. Головин, А. Ю. Криминалистическое мышление и цифровое будущее / А. Ю. Головин // Криминалистика – наука без границ: традиции и новации : материалы междунар. науч.-практ. конф., Санкт-Петербург, 30 ноября 2023 г. – Санкт-Петербург : Санкт-Петербургский университет МВД России, 2024. – С. 100–108.

42. Головин, А. Ю. Технологии искусственного интеллекта в криминалистике: задачи, которые необходимо решить / А. Ю. Головин // Сибирские уголовно-процессуальные и криминалистические чтения. – 2024. – № 2. – С. 25–33.

43. Гуртяков, А. С. Фрактальная компетентностная архитектура корпоративных систем дистанционного образования / А. С. Гуртяков, А. Г. Кравец, Д. В. Юдин [и др.] // Современные проблемы науки и образования. – 2012. – № 3. – С. 124–127.

44. Дмитриева, Т. Ф. О соотношении понятий «Технико-криминалистические средства» и «Научно-технические средства» / Т. Ф. Дмитриева // Вестник Полоцкого государственного университета. Серия D. Экономические и юридические науки. – 2013. – № 5. – С. 191–197.

45. Ефремова, М. А. Уголовно-правовые средства противодействия преступности в условиях цифровизации / М. А. Ефремова // Вестник Южно-Уральского государственного университета. Серия: Право. – 2024. – Т. 24, № 2. – С. 21–26.

46. Зайцев, О. А. Цифровой профиль лица как элемент информационно-технологической стратегии расследования преступлений / О. А. Зайцев, П. С. Пастухов // Вестник Пермского университета. Юридические науки. – 2022. – Вып. 56. – С. 281–308.

47. Зуев, С. В. IT-следователь в цифровой среде уголовного судопроизводства / С. В. Зуев, А. И. Зазулин // Правопорядок: история, теория, практика. – 2024. – № 2 (41). – С. 48–54.

48. Ищенко, Е. П. У истоков цифровой криминалистики / Е. П. Ищенко // Вестник Университета имени О. Е. Кутафина (МГЮА). – 2019. – № 3 (55). – С. 15–28.

49. Ким, Е. П. О криминалистической характеристике преступлений, совершаемых с использованием современных информационных и телекоммуникационных технологий / Е. П. Ким, Е. А. Киселев, О. Н. Каравянская // Научный компонент. – 2020. – № 3 (7). – С. 201–207.

50. Кирилюк, М. А. Характеристика способов дистанционных хищений денежных средств как этап ситуационного анализа / М. А. Кирилюк, А. Н. Литвиненко // Вестник экономической безопасности. – 2023. – № 1. – С. 219–225.

51. Климова, Я. А. Искусственный интеллект и цифровые доказательства в расследовании преступлений, совершенных с использованием современных информационно-коммуникационных технологий / Я. А. Климова // Вестник Волгоградской академии МВД России. – 2023. – № 1 (64). – С. 81–88.

52. Климова, Я. А. Цифровая криминалистика: перспективы развития / Я. А. Климова // Вестник Волгоградской академии МВД России. – 2020. – № 4 (55). – С. 128–133.

53. Клюев, Д. С. Анализ возможностей искусственного интеллекта для расследования мошенничества / Д. С. Клюев, А. Б. Смуш-

кин, Ю. В. Соколова [и др.] // Физика волновых процессов и радиотехнические системы. – 2023. – Т. 26, № 3. – С. 116–122.

54. Козодаева, О. Н. Способы совершения мошенничества с использованием банковских карт / О. Н. Козодаева, А. С. Обыденнова // Ученые записки Тамбовского отделения РоСМУ. – 2019. – № 13. – С. 52–58.

55. Ларина, Е. С. Криминальная жизнь дипфейков / Е. С. Ларина, В. С. Овчинский // Информационные войны. – 2022. – № 3 (63). – С. 69–73.

56. Латыпов, В. С. Перспективы применения инновационных технологий в деятельности следственных органов / В. С. Латыпов, А. Б. Гуськова // Евразийский юридический журнал. – 2024. – № 3 (190). – С. 356–357.

57. Лемайкина, С. В. Актуальные вопросы противодействия использованию технологии дипфейков / С. В. Лемайкина // Юристъ-Правоведъ. – 2022. – № 3 (102). – С. 175–178.

58. Лозинский, О. И. Цифровая экосистема как новый виток эволюции в области эффективного и результативного раскрытия и расследования преступлений в эпоху цифровой трансформации / О. И. Лозинский // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2024. – № 1 (164). – С. 126–131.

59. Лозовский, Д. Н. Использование беспилотных летательных аппаратов в процессе расследования преступлений: вопросы теории и практики / Д. Н. Лозовский, Н. Н. Лозовская, И. Р. Ульянова // Юристъ-Правоведъ. – 2021. – № 3 (98). – С. 162–165.

60. Лужинская, Е. Л. Особенности исследования изображений внешнего облика человека, измененного при помощи программных средств / Е. Л. Лужинская, В. А. Чванкин // Вопросы криминологии, криминалистики и судебной экспертизы. – 2022. – № 2 (52). – С. 116–121.

61. Малышева, О. А. Применение следователем информационно-коммуникационных технологий при производстве следственных действий: риски и пути их преодоления / О. А. Малышева, П. А. Самсонов // Журнал российского права. – 2024. – Т. 28, № 2. – С. 66–78.

62. Медведев, И. В. Компьютерная криминалистика «Форензика» и киберпреступность в России / И. В. Медведев // Пролог: журнал о праве. – 2013. – № 3. – С. 66–69.

63. Моругина, Н. А. Оценка допустимости распространения опыта цифровизации в уголовном судопроизводстве России / Н. А. Моругина, О. Л. Кузьмина // Современные проблемы уголовного процесса: пути решения (приуроченная к 160-летию Устава уголовного судопроизводства) : сб. материалов V Междунар. конф., Уфа, 4–5 апреля 2024 г. – Уфа : Уфимский юридический институт МВД России, 2024. – С. 190–194.

64. Мухутдинова, Л. М. Использование технологии Big Data в криминалистике / Л. М. Мухутдинова, М. А. Яворский // Актуальные проблемы правоведения. – 2023. – № 1 (77). – С. 30–35.

65. Пастухов, П. С. О необходимости развития компьютерной криминалистики / П. С. Пастухов // Пермский юридический альманах. – 2018. – № 1. – С. 450–460.

66. Пастухов, П. С. Оптимизация предварительного расследования с использованием электронной информации / П. С. Пастухов // Вестник экономической безопасности. – 2023. – № 2. – С. 154–158.

67. Пастухов, П. С. Унификация уголовно-процессуальной и технико-криминалистической деятельности при собирании цифровых следов преступлений / П. С. Пастухов // Пенитенциарная система и общество: опыт взаимодействия : сб. материалов X Междунар. науч.-практ. конф., Пермь, 5–7 апреля 2023 г. Т. 2. – Пермь : Пермский институт Федеральной службы исполнения наказаний, 2023. – С. 217–221.

68. Плахота, К. С. Особенности оформления результатов следственных действий, осуществляемых дистанционно / К. С. Плахота // Вестник Дальневосточного юридического института МВД России. – 2023. – № 4 (65). – С. 106–111.

69. Плахота, К. С. Перспективы использования электронных средств связи при производстве следственного осмотра / К. С. Плахота // Материалы криминалистических чтений : сб. материалов, Барнаул, 23 ноября 2023 г. – Барнаул : Барнаульский юридический институт МВД России, 2023. – С. 55–57.

70. Подобных, А. В. Биткойн-криминалистика для деанонимизации криптомиксеров и транзакций CoinJoin / А. В. Подобных // Информационная безопасность. – 2022. – № 5. – С. 44–45.

71. Поляков, В. В. Источники и принципы формирования частной методики расследования высокотехнологичных преступлений / В. В. Поляков // Lex russica (Русский закон). – 2022. – № 75 (6). – С. 85–96.

72. Расторопова, О. В. Противодействие использованию искусственного интеллекта в преступных целях / О. В. Расторопова // Вестник Университета прокуратуры Российской Федерации. – 2021. – № 4 (84). – С. 52–58.

73. Романенко, М. А. Новый подход к содержанию системы криминалистической техники / М. А. Романенко // Вестник Пермского университета. Серия «Юрид. науки». – 2008. – №. 2. – С. 116–119.

74. Россинская, Е. Р. К вопросу об инновационном развитии криминалистической науки в эпоху цифровизации / Е. Р. Россинская // Юридический вестник Самарского университета. – 2019. – № 4. – С. 144–151.

75. Россинская, Е. Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности / Е. Р. Россинская // Вестник Восточно-Сибирского института МВД России. – 2019. – № 2 (89). – С. 193–202.

76. Рябова, О. В. Роль электронных доказательств в расследовании отдельных категорий преступлений / О. В. Рябова // Вопросы российского и международного права. – 2023. – Т. 13, № 6–1. – С. 382–391.

77. Рябчиков, С. А. Использование систем видеоконференцсвязи и электронного документооборота при производстве следственных и иных процессуальных действий / С. А. Рябчиков // Криминалистика – наука без границ: традиции и новации : материалы междунар. науч.-практ. конф., Санкт-Петербург, 30 ноября – 1 декабря 2023 г. – Санкт-Петербург : Санкт-Петербургский университет МВД России, 2024. – С. 320–324.

78. Смушкин, А. Б. Об экосистеме предварительного расследования / А. Б. Смушкин // Вестник Томского государственного университета. – 2023. – № 488. – С. 242–247.

79. Смушкин, А. Б. О природе электронной цифровой криминалистики / А. Б. Смушкин // Lex russica. – 2020. – № 6 (163). – С. 110–121.

80. Смушкин, А. Б. Цели, задачи и функции электронной цифровой криминалистики / А. Б. Смушкин // Криминалистика: вчера, сегодня, завтра. – 2020. – № 1 (13). – С. 103–107.

81. Смушкин, А. Б. Электронная цифровая информация как центральный объект электронной цифровой криминалистики / А. Б. Смушкин // Криминалистика: вчера, сегодня, завтра. – 2022. – № 1 (21). – С. 142–154.

82. Сотников, К. И. Парадигма цифровизации криминалистики: частный взгляд на содержание и перспективы / К. И. Сотников // Санкт-Петербургский международный криминалистический форум : материалы междунар. науч.-практ. конф., Санкт-Петербург, 10–11 июня 2024 г. – Санкт-Петербург : Санкт-Петербургский университет МВД России, 2024. – С. 487–491.

83. Спектор, Л. А. Цифровая криминалистика в условиях компьютеризации современного общества / Л. А. Спектор, А. Д. Малютин // Вестник Алтайской академии экономики и права. – 2022. – № 9–1. – С. 159–164.

84. Табак, И. С. Мошенничество с банковскими картами / И. С. Табак // Современные инновации. – 2018. – № 4 (26). – С. 37–40.

85. Тисен, О. Н. Методика обнаружения, фиксации и изъятия электронно-цифровых следов по делам о преступлениях, совершенных с использованием криптовалют / О. Н. Тисен // Уголовное право. – 2024. – № 3 (163). – С. 69–80.

86. Химичева, О. В. Следственные действия: о цифровой трансформации их производства / О. В. Химичева // Криминологический журнал. – 2023. – № 2. – С. 170–174.

87. Четвергов, М. А. Компетентность эксперта-баллиста при исследовании объектов, изготовленных с применением современных технологий / М. А. Четвергов // Криминологический журнал. – 2024. – № 1. – С. 186–192.

88. Шапошников, А. Ю. Применение современных технологий фиксации информации и беспилотных систем при производстве осмотра места происшествия / А. Ю. Шапошников, Д. Н. Овакимян // Судебная власть и уголовный процесс. – 2021. – № 1. – С. 142–153.

89. Шухова, Н. В. О роли форензики в криминалистическом обеспечении расследования преступлений / Н. В. Шухова, А. Л. Снигирев // Информатизация и информационная безопасность правоохранительных органов : сб. тр. XX Междунар. науч. конф., Москва, 24–25 мая 2011 г. – Москва : Академия управления МВД России, 2011. – С. 331–333.

90. Яровенко, В. В. Применение цифровых технологий в дактилоскопии (переход на создание, хранение и исследование материалов в электронном формате) / В. В. Яровенко, О. В. Пяткова, А. В. Чередниченко // Юридические исследования. – 2022. – № 2. – С. 51–62.

Диссертации и авторефераты диссертаций

91. Бахтеев, Д. В. Концептуальные основы теории криминалистического мышления и использования систем искусственного интеллекта в расследовании преступлений : автореф. дис. … д-ра юрид. наук : 5.1.4 / Бахтеев Дмитрий Валерьевич. – Екатеринбург, 2022. – 504 с.

92. Коляманов, Р. А. Теоретические и организационно-тактические основы применения методов технико-криминалистической экспертизы документов : дис. ... канд. юрид. наук : 12.00.12 / Коляманов Руслан Александрович. – Москва, 2020. – 185 с.

93. Кравец, Е. Г. Информационно-коммуникационные технологии как элемент технико-криминалистического обеспечения расследования преступлений : дис. … канд. юрид. наук : 12.00.12 / Кравец Евгений Григорьевич. – Волгоград, 2016. – 208 с.

94. Куемжиева, С. А. Концептуальные основы групповой методики расследования преступлений против семьи и несовершеннолетних : дис. ... д-ра юрид. наук : 12.00.12 / Куемжиева Светлана Александровна. – Краснодар, 2020. – 496 с.

95. Литвин, И. И. Современные технические средства и проблемы их применения в доказывании на досудебных стадиях уголовного судопроизводства : автореф дис. … канд. юрид. наук : 12.00.09 / Литвин Илья Ильич. – Екатеринбург, 2018. – 31 с.

96. Мохат, П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы : дис. ... д-ра юрид. наук : 12.00.03 / Мохат Петр Мечиславович. – Москва, 2018. – 420 с.

97. Рамалданов, Х. Х. Процесс доказывания по уголовным делам в условиях тотальной цифровизации общественных отношений : дис. ... канд. юрид. наук : 5.1.4 / Рамалданов Ханбулат Хизриевич. – Москва, 2024. – 244 с.

Материалы судебной и следственной практики

98. Обзор результатов работы по профилактике, раскрытию и расследованию преступлений в сфере информационно-телекоммуникационных технологий в Волгоградской области за 2023 г. (на основании материалов уголовных дел) // Консультант Плюс : справ.-правовая сист. – Режим доступа : для зарегистрир. пользователей.

99. Обзор судебной практики Верховного Суда Российской Федерации № 1 (2020), утв. Президиумом Верховного Суда РФ 10.06.2020 // КонсультантПлюс : справ.-правовая сист. – Режим доступа : для зарегистрир. пользователей.

100. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» : постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 // КонсультантПлюс: справ.-правовая система. – URL : https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения: 17.06.2025).

101. О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности : постановление Пленума Верховного Суда РФ от 9 февраля 2012 г. № 1 // КонсультантПлюс : справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_125957/ (дата обращения: 25.06.2025).

102. О практике назначения судами Российской Федерации уголовного наказания : постановление Пленума Верховного Суда РФ от 22 декабря 2015 г. № 58 // КонсультантПлюс : справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_190932/ (дата обращения: 25.05.2025).

103. О практике применения судами законодательства об ответственности за бандитизм : постановление Пленума Верховного Суда РФ от 17 января 1997 г. № 1 // КонсультантПлюс : справ.-правовая сист. – URL: https://www.consultant.ru/document/cons_doc_LAW_13102/ (дата обращения: 25.05.2025).

104. О результатах расследования уголовных дел о преступлениях, связанных с «финансовыми пирамидами» за 12 месяцев 2023 года : обзор ГСУ ГУ МВД России по Волгоградской области (по материалам уголовных дел).

105. О судебной практике по делам о краже, грабеже и разбое : постановление Пленума Верховного Суда РФ от 27 декабря 2002 г. № 29 // КонсультантПлюс : справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_40412/ (дата обращения: 25.05.2025).

106. О судебном приговоре : постановление Пленума Верховного Суда РФ от 29 ноября 2016 г. № 55 // КонсультантПлюс : справ.-правовая сист. – URL : https://www.consultant.ru/document/cons_doc_LAW_207874/ (дата обращения: 25.05.2025).

107. Приговор Самарского областного суда № 02-34/2024 2-34/2024 от 29 октября 2024 г. по делу № 02-34/2024. – URL : https://sudact.ru/regular/doc/spLKUQAD2CrM/?regular-txt=228&regular-case_doc=&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=1000&regular-court=Самарский+областной+суд+%28Самарская+область%29&regular-judge=&_=1752213330839&snippet_pos=20236#snippet (дата обращения: 29.05.2025).

108. Приговор Шпаковского районного суда Ставропольского края от 9 февраля 2022 г. № 1-467/2021. – URL : http//www.sudact.ru/regular/doc/MLht2ESs1yrT/ (дата обращения: 29.05.2025).

109. Проект Федерального закона «О внесении изменения в статью 6 Федерального закона «Об оперативно-розыскной деятельности» от 14 августа 2023 г. // Федеральный портал проектов нормативных правовых актов. – URL : https://regulation.gov.ru/Regulation/Npa/PublicView?npaID=140881 (дата обращения: 28.04.2025).

110. Статистические данные по организации производства компьютерно-технической экспертизы в ЭКЦ ГУ МВД России по Волгоградской области (на основании материалов уголовных дел) за 2020–2025 гг.

Интернет-ресурсы

111. В Госдуме работают над законопроектом о запрете дипфейков. – URL : https://pravo.ru/news/251111/ (дата обращения: 09.05.2025).

112. Владимир Колокольцев провел заседание Правительственной комиссии по профилактике правонарушений. – URL : https://mvdmedia.ru/news/official/vladimir-kolokoltsev-provel-zasedfanie-pravitelstvennoy-komissii-po-profilaktike-pravonarusheniy (дата обращения: 06.05.2025).

113. Впервые полиция начала расследование в метавселенной. – URL : https://xn--80aafkca5bdpa3bj2p.xn--p1ai/ (дата обращения: 17.05.2025).

114. В РФ разработали систему идентификации пользователя по клавиатурному почерку. – URL : https://www.m24.ru/news/nauka/15032024/674543?utm_source=CopyBuf (дата обращения: 09.05.2025).

115. В Томске вынесен приговор участникам организованной преступной группы. – URL : https://epp.genproc.gov.ru/ru/web/proc_sibfo/mass-media/news/news-regional?item=99301354 (дата обращения: 01.06.2025).

116. Генеральная прокуратура : офиц. сайт. – URL : https://genproc.gov.ru/smi/news/genproc/news1828306/ (дата обращения: 25.03.2025).

117. Главное управление внутренних дел Мингорисполкома : офиц. сайт. – URL : https://minsk.mvd.gov.by/ru/news/10744 (дата обращения: 31.05.2025).

118. Государственная автоматизированная система Российской Федерации «Правосудие» : офиц. сайт. – URL : https://sudrf.ru (дата обращения: 25.05.2025).

119. Дипфейк // Большая российская энциклопедия : офиц. сайт. – URL : http://bigenc.ru/c/dipfeik-f9f89b (дата обращения: 03.05.2025).

120. Заседание дискуссионного клуба «Валдай». – URL : http://kremlin.ru/events/president/news/75521 (дата обращения: 07.04.2025).

121. Интервью руководителя Главного управления криминалистики Следственного комитета Российской Федерации З. З. Ложиса. – URL : https://sledcom.ru/search?q=+crimeserieslinkage (дата обращения: 29.05.2025).

122. Искусственный интеллект привлекут для расследования нераскрытых преступлений. – URL : https://euronus.com/news-tech/1442-iskusstvennyj-intellekt-privlekut-dlya-rassledovaniya-neraskrytykh-prestuplenij.html (дата обращения: 04.06.2025).

123. Итоги года с Владимиром Путиным – 2023. – URL : https://www.pnp.ru/story/itogi-goda-s-vladimirom-putinym-2023 (дата обращения: 29.04.2025).

124. Картину Уорхола продали по частям на первом криптовалютном аукционе. – URL : https://style.rbc.ru/repost/5b321d3d9a79472e748915c7 (дата обращения: 23.05.2025).

125. Комсомольская правда. Казахстан : офиц. сайт. – URL : https://www.kp.kz/daily/27453/4656857 (дата обращения: 17.05.2025).

126. Международная конференция по искусственному интеллекту и машинному обучению «Artificial Intelligence Journey 2023». – URL : http://kremlin.ru/events/president/news/72811 (дата обращения: 06.06.2025).

127. Министерство внутренних дел Российской Федерации : офиц. сайт. – URL : https://мвд.рф/dejatelnost/statistics (дата обращения: 24.06.2025).

128. Мониторинг глобальных трендов цифровизации за 2022 год // Ростелеком. 2023. – URL : https://www.company.rt.ru/upload/iblock/109/rostelekom_monitoring_2022.pdf (дата обращения: 16.06.2025).

129. Оборудование ВКС для переговорных комнат. – URL : http://pcnews.ru/blogs/oborudovanie_vks_dla_peregovornyh_komnat-708118.html (дата обращения: 20.06.2025).

130. Он не спал: фитнес-приложение раскрыло убийство. – URL : https://www.gazeta.ru/tech/2021/02/10/13473764/criminal_apps.shtml?updated (дата обращения: 27.05.2025).

131. Опрос на тему: «Искусственный интеллект: помощник или конкурент?». – URL : https://docs.google.com/forms/d/e/1FAIpQLSduMvdom9bGnU_AvT3q5fuoMLwTmiRrK8dbNbzF1A0EtW_PuQ/viewform?usp=sf_link (дата обращения: 01.04.2025).

132. Отчет о мошенничестве с личными данными, 2024 г. Onfido : офиц. сайт. – URL : https://onfido.com/landing/identity-fraud-report (дата обращения: 07.05.2025).

133. Портал правовой статистики. – URL : http://crimestat.ru/analytics (дата обращения: 12.04.2025).

134. Путин отметил рост числа преступлений в IT-сфере. – URL : https://ria.ru/20210303/prestupleniya-1599747056.html (дата обращения: 29.05.2025).

135. Путин призвал обеспечить массовое внедрение искусственного интеллекта. – URL : https://ria.ru/20221124/intellekt-1833975245.html (дата обращения: 24.03.2025).

136. Расширенное заседание коллегии МВД России в 2022 году. – URL : http://kremlin.ru/events/president/news/67795 (дата обращения: 02.06.2025).

137. Сбер создал одну из лучших в мире технологий распознавания дипфейков. – URL : https://www.ferra.ru/news/techlife/sber-sozdal-odnu-iz-luchshikh-v-mire-tekhnologii-raspoznavaniya-dipfeikov-09-02-2023.htm (дата обращения: 29.04.2025).

138. Системы конференций для предприятия // On-line библиотека : офиц. сайт. – URL : http://www.xserver.ru/computer/nets/internet/87/ (дата обращения: 23.05.2025).

139. Создателей искусственного интеллекта призвали остановить разработки // Газета «Известия» : офиц. сайт. – URL : https://iz.ru/1490348/2023-03-29/sozdatelei-iskusstvennogo-intellekta-prizvali-ostanovit-razrabotki (дата обращения: 24.05.2025).

140. Состояние преступности в России за 2023 год. – URL : file:///C:/Users/HOME/Downloads/Sbornik_23_12.pdf (дата обращения: 02.06.2025).

141. Состояние преступности в России за январь – октябрь 2024 года. – URL : file:///C:/Users/HOME/Downloads/Sbornik_2410_UOS.pdf (дата обращения: 03.05.2025).

142. Судебные и нормативные акты РФ. – URL : https://sudact.ru (дата обращения: 18.04.2025).

143. Умные браслеты. – URL : https://www.oxygensoftware.ru/ru/news/articles/141-fitnes-kriminalistika-kak-umnye-braslety-pomogayut-raskryvat-prestupleniya (дата обращения: 25.05.2025).

144. Федеральный институт промышленной собственности (ФИПС) : офиц. сайт. – URL : https://new.fips.ru/registers-web/action?acName=clickTree&nodeId=1977&maxLevel=1 (дата обращения: 29.05.2025).

145. Фейковая реклама казино от имени стендап-комика Нурлана Сабурова распространяется в Сети. – URL : https://stopfake.kz/ru/archives/21066 (дата обращения: 30.04.2025).

146. ФСБ завела на жителя Владимирской области дело об оправдании терроризма. – URL : https://rg.ru/2024/07/11/reg-cfo/fsb-zavela-na-zhitelia-vladimirskoj-oblasti-delo-ob-opravdanii-terrorizma.html (дата обращения: 11.06.2025).

147. ЦБТ изучает возможность идентификации по сетчатке глаза. – URL : https://ria.ru/20231109/identifikatsiya-1908290911.html (дата обращения: 07.05.2025).

148. Что юристу нужно знать о LegalTech. – URL : https://www.law.ru/article/27878-chto-yuristu-nujno-znat-o-legaltech-produkty-primery-obuchenie (дата обращения: 21.05. 2025).

149. Эксперты посоветовали силовикам РФ внедрять в работу искусственный интеллект // Информагентство «Интерфакс» : офиц. сайт. – URL : https://www.interfax.ru/russia/797839 (дата обращения: 18.06.2025).

150. NFT для предметов искусства и коллекционирования. – URL : https://vc.ru/crypto/476920-nft-dlya-predmetov-iskusstva-i-kollekcionirovaniya-osnovy-istoriya-i-perspektivy (дата обращения: 23.05.2025).

151. South China Morning Post. – URL : https://www.scmp.com/news/china/society/article/3023964/chinese-murder-suspect-caught-ai-software-spotted-dead-persons (дата обращения: 09.06.2025).

152. Statista – международная глобальная платформа данных с обширной коллекцией статистических данных, отчетов и аналитической информации. – URL : https://www.statista.com/aboutus (дата обращения: 02.06.2025).

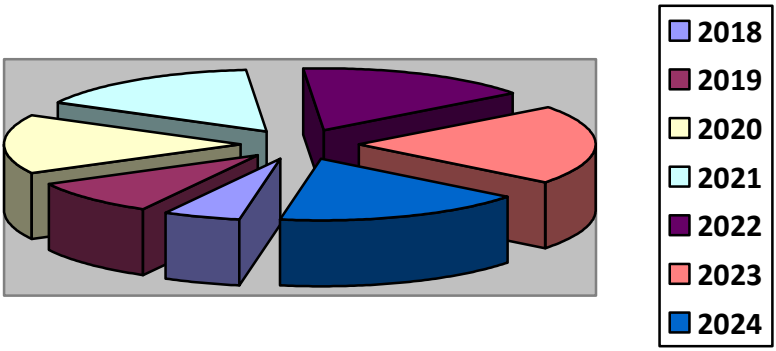
153. Turkey using AI software ASENA in fight against drugs. – URL : https://www.hurriyetdailynews.com/turkey-using-ai-software-asena-in-fight-against-drugs-173912 (дата обращения: 15.06.2025).

154. Whois-сервис для проверки доменов. – URL : http://www.whois-service.ru (дата обращения: 11.06.2025).

ПРИЛОЖЕНИЯ

Приложение 1

Статистические данные правоохранительных органов Российской Федерации о количестве преступлений, совершенных с использованием информационно-телекоммуникационных технологий за 2018–2024 гг.



Приложение 2

ПРОЕКТ
ФЕДЕРАЛЬНОГО ЗАКОНА
«О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации (о цифровых доказательствах)»

Статья 1

Внести в Уголовно-процессуальный кодекс Российской Федерации следующие изменения:

1) статью 5 дополнить пунктом: «58.1) цифровые доказательства – любые сведения в электронном виде, устанавливающие наличие или отсутствие обстоятельств, имеющих значение для уголовного дела, зафиксированные на носителях электронной информации либо хранящиеся или передаваемые с использованием информационно-телекоммуникационных технологий;».

2) часть 2 статьи 74 дополнить пунктом: «4.1) цифровые доказательства;».

Приложение 3

ПРОЕКТ
ФЕДЕРАЛЬНОГО ЗАКОНА
«О внесении изменений в Федеральный закон
от 27 июля 2006 г. № 149-ФЗ
„Об информации, информационных технологиях
и о защите информации“»

Статья 1

Внести в Федеральный закон Российской Федерации следующие изменения:

статью 2 дополнить пунктом: «4.1) искусственный интеллект – комплекс технологических решений, включающий информационно-коммуникационную инфраструктуру и программное обеспечение, воспроизводящий когнитивные возможности мозга человека для решения конкретных задач по обработке большого массива данных и поиска оптимальных решений согласно заданному алгоритму;».

ДЛЯ ЗАМЕТОК

Научное издание

Климова *Яна Александровна*

ОРГАНИЗАЦИОННО-ТАКТИЧЕСКОЕ ОБЕСПЕЧЕНИЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Монография

Редактор *А. Н. Гайворонская-Кантомирова*
Компьютерная верстка *Ю. В. Сиволапова*
Дизайн обложки *Н. А. Доненко*

Волгоградская академия МВД России.
400075, Волгоград, ул. Историческая, 130.

Редакционно-издательский отдел.
400005, Волгоград, ул. Коммунистическая, 36.

Подписано в печать 03.09.2025. Формат 60×84/16. Бумага офсетная.
Гарнитура Times New Roman. Физ. печ. л. 8. Усл. печ. л. 7,44.
Тираж 30 экз. Заказ 40.

ОПиОП РИО ВА МВД России. 400005, Волгоград, ул. Коммунистическая, 36.