УДК 343.9

Сукалина Юлия Антоновна
студент,
Институт юстиции,
Байкальский государственный университет,
г. Иркутск, Российская Федерация,
e-mail: yulya.sukalina05@mail.ru

Научный руководитель: Коломинов Вячеслав Валентинович
кандидат юридических наук, доцент,
кафедра уголовного процесса и криминалистики,
Институт юстиции,
Байкальский государственный университет,
г. Иркутск, Российская Федерация

КРИМИНАЛИСТИЧЕСКИЙ АНАЛИЗ ЦИФРОВЫХ СЛЕДОВ В СОЦИАЛЬНЫХ СЕТЯХ И МЕССЕНДЖЕРАХ

Аннотация. Криминалистический анализ цифровых следов в социальных сетях и мессенджерах занимает ключевое место в современном уголовном и гражданском судопроизводстве. В работе рассматриваются методы и инструменты извлечения, восстановления и верификации цифровых следов, а также юридические и этические аспекты их применения. Основное внимание уделяется характеру данных, сохраняющихся в профильных аккаунтах, переписке, медиафайлах и метаданных, а также их цепочке происхождения и целостности.

***Ключевые слова*:** криминалистическая наука, виртуальные следы, сетевые платформы, сервисы мгновенного обмена сообщениями, высокотехнологичные преступления, технологии искусственного интеллекта.

Yulia A. Sukalina
Student,
Institute of Justice,
Baikal State University,
Irkutsk, Russian Federation,
e-mail: yulya.sukalina05@mail.ru

Scientific Supervisor: Vyacheslav V. Kolominov
PhD in Law, Associate Professor,
Department of Criminal Procedure and Criminalistics,
Institute of Justice,
Baikal State University,
Irkutsk, Russian Federation

ISSN 2658-7823

CRIMINALISTIC ANALYSIS OF DIGITAL TRACES IN SOCIAL NETWORKS AND MESSENGERS

Abstract. Forensic analysis of digital traces in social networks and instant messengers occupies a key place in modern criminal and civil proceedings. The paper discusses methods and tools for extracting, restoring, and verifying digital traces, as well as the legal and ethical aspects of their application. The focus is on the nature of data stored in profile accounts, correspondence, media files, and metadata, as well as their chain of origin and integrity.

***Keywords*:** forensic science, virtual traces, online platforms, instant messaging services, high-tech crimes, artificial intelligence technologies.

Обоснование актуальности научной работы на тему «Криминалистический анализ цифровых следов в социальных сетях и мессенджерах» заключается в нескольких ключевых аспектах:

1. Стремительное увеличение числа правонарушений в виртуальном пространстве, реализуемых посредством IT-технологий. Сегодня электронно-цифровая следовая картина выступает главным источником доказательственной базы в ходе раскрытия как специфических киберпреступлений, так и классических общеуголовных деяний [1, с. 27].

2. Необходимость адаптации традиционных криминалистических методов и средств к условиям цифровой реальности. Компьютерная информация обладает специфическими свойствами: способностью к мгновенному тиражированию без потери качества, одновременным нахождением на разных носителях, а также уязвимостью к дистанционному изменению или полному уничтожению. Наличие временных меток и метаданных требует особых подходов для достоверной реконструкции хронологии расследуемого события [8, с. 142].

3. Трансформация тактических приемов ведения следственных действий под влиянием IT-технологий. Классические методики адаптируются к особенностям виртуального пространства и специфике поведения людей в социальных сетях. В частности, в процессе допроса следователь может эффективно использовать сведения из личных профилей, геолокационные маркеры и историю переписок для изобличения допрашиваемого во лжи или верификации его показаний [2, с. 193].

Ключевая цель исследования заключается в разработке эффективных методов анализа цифровых следов для установления обстоятельств преступления.

Виртуальная информация аккумулирует в себе сведения о поведении пользователя на веб-ресурсах, истории его посещений, а также об использованных программно-аппаратных средствах и иные криминалистически значимые данные [3, с. 84].

Методологически работа сочетает цифровую криминалистику, анализ больших данных (биг-дата), методы графового анализа сетей, машинное обучение для обнаружения аномалий и связей, а также подходы к воспроизведению

сценариев действий пользователей в рамках экспертиз. Практическая значимость заключается в повышении надёжности судебных экспертиз по цифровым следам в соцсетях и мессенджерах, снижении рисков фальсификаций, а также в выработке рекомендаций по политике конфиденциальности и защите информации. В рамках исследования обсуждаются ограничения методик, правовые риски и требования к компетенциям специалистов по цифровой криминалистике.

Объектами криминалистического анализа выступают:

Персональные аккаунты и учетные записи пользователей в социальных медиа;

Открытые публикации, комментарии, истории, записи на персональных страницах и иные виды публичного цифрового контента;

Приватные и коллективные диалоги в мессенджерах (VK, Telegram и др.);

Мультимедийные материалы: фотоснимки, аудиозаписи, видеоматериалы, а также голосовые сообщения;

Логи активности, сведения об авторизации, геолокационные отметки и метаданные документов;

Информация, извлеченная непосредственно из памяти портативных устройств (смартфонов, планшетных компьютеров) или стационарных ПК;

Резервные копии и архивы сетевых профилей и переписок [8, с. 165].

Специфика, структура и объём сохраняемой следовой картины напрямую обусловлены архитектурными особенностями конкретной социальной платформы или мессенджера.

Предмет криминалистического анализа — виртуальные следы, сформированные пользователями в интернет-пространстве.

Выделяют несколько базовых категорий таких следов:

Статические —формируются в результате функционирования электронного устройства (компьютера) без прямого участия человека. К ним относятся, например, сведения об IP-адресе используемого устройства и его перемещении в телекоммуникационной сети. Подобные сведения аккумулируются провайдером сетевых услуг (оператором связи) и предоставляются органам предварительного расследования в рамках установленных законом процедур [3, с. 112].

Динамические цифровые следы возникают тогда, когда пользователь совершает конкретные действия в сети. К ним относится информация, которая автоматически создается в процессе работы человека с приложением или сайтом. Например, это могут быть поисковые запросы, история переходов по ссылкам, отметки «мне нравится» (лайки), а также сведения о действиях пользователя в личном кабинете [7, с. 66].

Сетевые данные — это техническая информация, которая связана с передачей сообщений и файлов через интернет. К ней относятся, например:

уникальные сетевые адреса устройств (IP и MAC- адреса);

точное время подключения к сети и длительность сессии;

технические данные от операторов связи (например, сведения о том, к какой вышке сотовой связи подключался телефон);

сведения об интернет-провайдере, через которого осуществлялся доступ в социальную сеть;

А также международный идентификационный код мобильного девайса (IMEI) [3, с. 120; 7, с. 68].

Контентные — непосредственное содержание переписки, включая текстовые сообщения, голосовые и видеозвонки. Даже частично удаленные сообщения могут быть восстановлены при условии своевременного доступа к устройству [11, с. 107].

Метаданные — "данные о данных", включающие временные метки создания, редактирования и удаления сообщений, идентификаторы устройств, IP-адреса, сведения о типе и версии приложения. Именно анализ метаинформации зачастую позволяет верифицировать факт подделки или несанкционированного изменения контента [11, с. 109].

Файловые артефакты — медиафайлы (фото, видео, аудио), документы, стикеры и GIF-изображения, передаваемые через платформы. Важное значение имеют встроенные метаданные этих файлов (EXIF-данные), которые могут указывать время, место и устройство создания [7, с. 69].

Специфика виртуальных улик кроется в их формировании посредством сложной интеграции программных алгоритмов и аппаратных модулей, а также в ходе выполнения различных информационных процессов. Данное свойство предопределяет их уникальную природу и обуславливает необходимость задействования узкоспециализированных методик криминалистического анализа [8, с. 44].

В рамках научной дискуссии выделяют три ключевых проблемы работы с такими материалами:

1. Вопросы этики и права в ходе расследований. Сюда относится обязательное соблюдение конфиденциальности, защита личной жизни граждан и строгий контроль за сохранностью данных [1, с. 29].

2. Модернизация уголовно-процессуального законодательства. Эксперты указывают на необходимость нормативного закрепления определения «цифровой документ», а также на расширение перечня следственных действий, сфокусированных на фиксации и изъятии компьютерной информации [9, с. 115].

3. Профессиональная подготовка кадров. В условиях стремительного роста киберпреступности обучение узкопрофильных специалистов в области цифровой криминалистики становится приоритетной задачей для правоохранительной системы [9, с. 210].

Для выявления и изучения цифровых следов применяются различные методы и инструменты [3, с. 145]:

1. Анализ метаданных. Исследуются данные о времени создания и редактирования сообщений, используемых устройствах, геолокации. Например, в фотографиях могут содержаться EXIF-данные, а в сообщениях — информация о времени отправки и IP-адресах.

2. Изучение системных логов. Анализируются журналы действий пользователя: время входа в систему, запуск приложений, перемещение по файловой системе. Это помогает восстановить хронологию событий.

3. Поведенческий анализ. Выявляются повторяющиеся сценарии взаимодействия пользователя с системой или приложениями. Для этого часто используются алгоритмы машинного обучения и искусственный интеллект.

4. Анализ исходного кода страниц. В некоторых случаях требуется изучение исходного кода сайта или приложения для обнаружения скрытых ссылок или путей к данным.

5. Восстановление удалённых данных. Используются программы для извлечения информации из резервных копий, свободных кластеров диска или областей памяти, где данные могли сохраниться даже после удаления.

6. Визуализация связей. Применяются инструменты для построения графов связей между аккаунтами, анализа сетевых взаимодействий.

Сбор и анализ цифровых следов регулируются законодательством. В России ключевые нормативные акты:

А) Кодекс об административных правонарушениях (КоАП) и УК РФ — ответственность за утечку данных и незаконный сбор информации (ст. 13.11 КоАП, ст. 137, 272 УК РФ).

Б) Уголовно-процессуальный кодекс РФ (УПК РФ), в частности статья 81, которая определяет порядок фиксации и изъятия электронных носителей информации [10].

В) Федеральный закон №144-ФЗ «Об оперативно-розыскной деятельности» — регламентирует правовые основы осуществления оперативно-технических мероприятий в рамках информационных систем и сетей связи [4].

Г) Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации» — регулирует общие правоотношения в сфере обмена, распространения и технической защиты данных [5].

Д) Федеральный закон №152-ФЗ «О персональных данных», который требует защиты информации, позволяющей идентифицировать физическое лицо [6].

Для признания цифровых доказательств в суде важно соблюдать процессуальные нормы: правильно фиксировать следы, обеспечивать целостность данных и подтверждать их подлинность экспертным заключением.

При анализе цифровых следов возникают ряд сложностей:

Быстрота распространения информации затрудняет её своевременную фиксацию.

Возможность мгновенного удаления данных делает их недоступными для анализа.

Шифрование усложняет доступ к содержимому сообщений и требует времени на дешифрование. Данные, зашифрованные на устройстве отправителя и расшифрованные только на устройстве получателя, недоступны для анализа в

транзите. Эксперты вынуждены полагаться на артефакты, остающиеся на самих устройствах, что требует физического доступа к ним.

Доступ к серверной информации социальных сетей и мессенджеров часто ограничен для независимых экспертов. В таких случаях суд может направить запрос администрации платформы.

Необходимость междисциплинарного взаимодействия — требуется сотрудничество специалистов в области IT, криминалистики, права.

Недостаток унифицированных стандартов фиксации и обработки цифровых улик.

Различия в платформах. Один и тот же мессенджер на Android и iOS может хранить данные в разных структурах и с разной степенью доступности. iOS традиционно создает больше препятствий для физического извлечения данных, тогда как Android при наличии root-доступа предоставляет более широкие возможности.

Большие объемы данных. Социальные медиа генерируют терабайты данных ежедневно. Ручной анализ неэффективен, требуется применение автоматизированных инструментов и алгоритмов машинного обучения.

Динамический характер данных. Социальные сети позволяют редактировать и удалять сообщения, что создает риски утраты доказательств. Проблема усугубляется тем, что некоторые платформы (например, Snapchat) по умолчанию удаляют контент через короткое время.

Криминалистический анализ цифровых следов помогает в расследовании различных преступлений, например:

– вербовки в преступные группировки (анализ цепочек сообщений для выявления лидеров и каналов распространения идеологии);

– финансирования преступлений (отслеживание финансовых транзакций через цифровые следы);

– распространения запрещённого контента (порнография, экстремизм);

кибербуллинга, мошенничества, клеветы.

Таким образом, анализ цифровых следов в социальных сетях и мессенджерах — сложный многоуровневый процесс, требующий технических знаний, правовых компетенций и использования современных инструментов. Его эффективность зависит от соблюдения процедур, выбора методов анализа и взаимодействия между специалистами разных областей.

Интеграция сквозных цифровых технологий существенно расширяет потенциал криминалистической техники. Внедрение алгоритмов машинного обучения и нейросетевых моделей позволяет автоматизировать процесс идентификации лиц по материалам систем видеонаблюдения даже в условиях низкого разрешения кадра или частичной окклюзии (сокрытия) биометрических признаков. В области цифрового автороведения методы искусственного интеллекта обеспечивают верификацию создателей текстового контента. Изучение особенностей текста помогает определить автора сообщений в мессенджерах. Это позволяет узнать, кто именно скрывается за анонимными аккаунтами и группами, в кото-

рых нарушают закон. Параллельно с этим технологии работы с большими данными (Big Data) трансформируют подход к анализу массивов информации, извлекаемой из социальных сетей, детализаций телефонных соединений и банковских транзакций. Автоматизированная корреляция таких сведений позволяет оперативно реконструировать схемы взаимодействия между соучастниками преступных групп и устанавливать скрытые причинно-следственные связи [1, с. 31].

Социальные сети выступают ключевым источником криминалистически значимой информации, оптимизирующей процесс принятия тактических решений при расследовании киберпреступлений. Данная информационная совокупность включает в себя сведения о механизме образования как идеальных, так и материальных следов. Указанные данные, извлеченные из виртуального пространства с использованием специализированных программно-аппаратных средств, подлежат процессуальному закреплению для последующего доказывания обстоятельств уголовного дела [2, с. 197].

Заключение

Криминалистический анализ цифровых следов в социальных сетях и мессенджерах представляет собой динамично развивающуюся область на стыке юриспруденции, компьютерных наук и криминалистики. Цифровые следы — от текстовых массивов и метаданных до геолокационных отметок и сетевых логов — обладают значительным доказательственным потенциалом. Шифрование, различия платформ, трансграничный характер данных и динамическая природа социальных сетей создают существенные вызовы, требующие постоянного совершенствования методов анализа.

Перспективы развития связаны с внедрением технологий искусственного интеллекта, способных обрабатывать огромные массивы данных, выявлять скрытые закономерности и делать анализ более эффективным. При этом ключевым требованием остается объяснимость — способность системы предоставить понятную человеку и проверяемую цепочку рассуждений, ведущую к выводу. Только сочетание передовых технологий с соблюдением правовых норм и этических принципов позволит цифровым следам полноценно выполнять свою роль в отправлении правосудия. [9, с.340]

Список использованной литературы

1. Амирова М.Г. Криминалистические аспекты цифровых Технологий / М.Г. Амирова, А.Г.Таилова // Human Progress. — 2025. — Т. 11, вып. 6. — С. 27. — DOI: 10.46320/2073-4506-2025-6a-29.

2. Васютин С.В. Криминологический аспект использования информации из социальных сетей при расследовании интернет-преступлений / С.В. Васютин // Вестник науки. — 2024. — Т. 1, № 3 (72). — С. 191–198.

3. Колычева А.Н. Расследование преступлений с использованием компьютерной информации из сети Интернет : учебное пособие / А.Н. Колычева, В.Ф. Васюков ; под ред. А.Г. Волеводза. — Москва : Проспект, 2020. — 200 с.

4. Об оперативно-розыскной деятельности : Федеральный закон от 12.08.1995 № 144-ФЗ (послед. ред. от 01.04.2025).

5. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 №149-ФЗ (посл.ред. От 24.06.2025).

6. О персональных данных : Федеральный закон от 27.07.2006 № 152-ФЗ (посл. ред. от 08.07.2024) / Российская Федерация. Законы // Консультант Плюс. — URL: http://www.consultant.ru.

7. Иванов В.Ю. К вопросу о классификации электронно-цифровых следов / В.Ю. Иванов // Национальная безопасность / Nota bene. — 2020. — № 3. — С. 64–71.

8. Вехов В.Б. Компьютерная криминалистика : учебное пособие / В.Б. Вехов. — Москва : Юрлитинформ, 2020. — 416 с.

9. Воронин М.Ю. Криминалистические основы получения и использования компьютерной информации в доказывании по уголовным делам : дис. … д-ра юрид. наук / М.Ю. Воронин. — Саратов : СГЮА, 2021. — 398 с.

10. Уголовно-процессуальный кодекс Российской Федерации от 18 дек. 2001 г. № 174-ФЗ : (в ред. от 08.03.2026 г.) // Собрание законодательства РФ. — 2002. — № 1. — Ст. 81.

11. Рамалданов Х.Х. Проблемы использования и хранения цифровых доказательств в доказывании в уголовном процессе / Х.Х. Рамалданов // Вестник Казанского юридического института МВД России. — 2023. — Т. 14, № 2. — С. 105–111.