УДК 343.98:004.9

Колотовкина А.А.
магистрант 3 курса
Красноярский государственный аграрный университет
(г. Красноярск, Россия)

ОСОБЕННОСТИ ПОЛУЧЕНИЯ, ФИКСАЦИИ И ИССЛЕДОВАНИЯ ЦИФРОВЫХ СЛЕДОВ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Аннотация: *в статье исследуются криминалистические и процессуальные особенности получения информации из социальных сетей при расследовании преступлений экстремистской направленности. Рассматриваются возможности OSINT и SOCMINT, этапы обнаружения, фиксации, сохранения и последующего анализа цифровых объектов. Анализируются ограничения скриншотов и автоматизированного сбора, значение метаданных, контрольных значений и документирования истории обращения с цифровыми материалами. Обосновывается необходимость разграничивать открытые сведения, персональные данные и информацию, охраняемую тайной сообщений, а также привлекать специалистов на раннем этапе расследования.*

Ключевые слова: *цифровой след, социальная сеть, OSINT-анализ, SOCMINT-мониторинг, фиксация информации, электронное доказательство, метаданные, компьютерно-техническая экспертиза.*

Использование социальных сетей в расследовании преступлений сопровождается необходимостью работать с информацией, которая может быть быстро изменена, удалена или скрыта настройками доступа. В отличие от традиционного документа, цифровой объект существует в определенной технологической среде, зависит от программного обеспечения и может сохраняться в нескольких версиях или на различных устройствах. Поэтому его обнаружение и копирование не исчерпывают задачу следствия: требуется

установить происхождение материала, обстоятельства получения, целостность и возможность последующей проверки.

При расследовании преступлений экстремистской направленности сведения социальных сетей могут включать публикации, комментарии, переписку, фотографии, видеозаписи, данные учетных записей, метаданные и сведения о сетевых взаимодействиях. Неполная фиксация контекста или нарушение порядка доступа способны повлиять на достоверность и процессуальную пригодность собранных материалов. Цель статьи — обобщить последовательность криминалистической работы с цифровыми следами социальных сетей и сформулировать требования к их фиксации и исследованию.

На первоначальном этапе значительная часть ориентирующей информации может быть получена из открытых источников. В научной литературе для обозначения сбора, обработки и анализа общедоступных сведений используется понятие OSINT. Применительно к социальным платформам употребляется также термин SOCMINT, акцентирующий внимание на информации из профилей, публикаций, комментариев и сообществ. Эти подходы имеют не только поисковую, но и аналитическую составляющую: обнаруженную страницу необходимо соотнести с конкретной задачей, проверить источник и определить, какие обстоятельства требуют дополнительного подтверждения [1, с. 66–71, 2, с. 79–86].

Применение OSINT не следует смешивать с получением доступа к закрытым разделам учетной записи. Открытая публикация, информация, доступная только после авторизации, частная переписка и сведения, находящиеся у администрации платформы, различаются по режиму доступа. Само по себе наличие технической возможности открыть страницу не заменяет правового основания для сбора и использования информации. При планировании работы необходимо определить конкретный объект, необходимый временной период, предполагаемый способ получения сведений и правовые ограничения.

Автоматизированный сбор может осуществляться с помощью поисковых инструментов, программных интерфейсов платформ, средств сохранения веб-страниц и парсеров, извлекающих заданные элементы: текст, идентификатор учетной записи, ссылку, время публикации, комментарии и число реакций. Однако структура интернет-страниц, программные интерфейсы и правила доступа изменяются. Поэтому программный инструмент может получить неполный набор полей или неверно интерпретировать отдельные данные. Результат автоматизированного извлечения нуждается в проверке и не должен приниматься за исчерпывающее отражение цифровой среды [1, с. 68–71].

При поиске открытых сведений важно сохранять поисковый контекст. Следует отражать, по каким идентификаторам и запросам обнаружен материал, на каком ресурсе он размещен, когда осуществлялся доступ и какие элементы были доступны наблюдателю. Такая фиксация облегчает повторную проверку и позволяет отличить первоначально обнаруженный объект от его копии, позднейшей публикации или пересказа. Подходы к использованию открытых источников в оперативно-розыскной и следственной деятельности подчеркивают необходимость аналитической проверки, а не механического накопления ссылок [1, 2].

Криминалистическую работу с цифровыми следами целесообразно выстраивать как последовательный процесс, включающий определение источника, законное получение доступа, обнаружение объекта, фиксацию его видимого содержания и технических характеристик, копирование, сохранение, анализ и документирование результатов. Этапы взаимосвязаны: если при обнаружении не зафиксированы адрес страницы и идентификатор публикации, позднее может оказаться затруднительно установить конкретный объект, если не сохранен исходный файл, возможности технического исследования могут быть ограничены.

При осмотре интернет-страницы необходимо описывать адрес ресурса и конкретной страницы, дату и время доступа, часовой пояс при его установлении, сведения об учетной записи, идентификатор публикации, видимость материала,

полный текст, вложения, комментарии и иные элементы, имеющие значение для контекста. Следует указывать, какие действия выполнялись при осмотре и какие средства использовались. Если содержание страницы изменяется в процессе просмотра, это обстоятельство целесообразно отдельно отразить в протоколе и приложениях. Тактические особенности осмотра интернет-страниц рассматриваются в криминалистической литературе как самостоятельная задача, требующая точного описания объекта и условий его восприятия [6, с. 246–253].

Скриншот полезен для визуального отражения того, что наблюдалось на экране, но он не всегда содержит сведения, достаточные для установления происхождения материала. Снимок экрана может не показывать полный адрес, идентификатор публикации, скрытые элементы интерфейса, историю изменений и технические параметры. Кроме того, изображение экрана может быть отредактировано. Поэтому при наличии технической возможности визуальную фиксацию следует дополнять сохранением страницы, исходных файлов, видеозаписью последовательности действий и получением данных из иных источников. Каждый способ фиксации имеет собственные ограничения, которые необходимо учитывать при последующей оценке.

При работе с файлами и электронными носителями существенное значение имеет сохранение неизменности исходных данных. Рекомендуется по возможности создавать рабочую копию и ограничивать операции, способные изменить исходный объект. Для контроля целостности могут использоваться криптографические хеш-функции. Рассчитанное контрольное значение позволяет сопоставить файл до и после копирования и установить, совпадают ли сравниваемые наборы данных. Вместе с тем хеширование подтверждает неизменность сравниваемого файла, но само по себе не доказывает, кем и когда он был создан, а также достоверность содержащейся в нем информации [3, с. 142–148].

История обращения с цифровым объектом должна быть прослеживаемой. В документации целесообразно указывать, кто и когда обнаружил материал, каким способом он получен, где и в каком виде сохранен, какие копии

создавались, какие операции проводились и кому объект передавался. Если данные конвертировались, распаковывались, декодировались или подвергались иной технической обработке, необходимо отразить соответствующие действия. Такой подход позволяет оценивать сохранность объекта и воспроизводить ход исследования. В научной литературе подчеркивается, что надежность электронных доказательств зависит не только от содержания, но и от соблюдения процедуры их получения и проверки [4, с. 170–173].

При исследовании смартфона или компьютера следует учитывать риск изменения информации при включении устройства, подключении к сети, открытии приложений и запуске файлов. До начала действий необходимо определить предполагаемые источники данных: мобильные устройства, рабочие станции, резервные копии, облачные хранилища, корпоративную почту и иные используемые сервисы. Объем копирования должен быть соразмерен задачам расследования. Необоснованное копирование всей цифровой инфраструктуры, когда возможно выделить относящиеся к делу данные, создает риск затронуть информацию третьих лиц и затрудняет последующий анализ.

При исследовании цифровых объектов следует сопоставлять их между собой и с информацией, полученной из независимых источников. Например, время публикации может проверяться по истории операций, переписке, данным устройства и сведениям платформы, авторство — по сочетанию данных об учетной записи, технических характеристик и иных обстоятельств, содержание файла — по метаданным, признакам изменения и связанным объектам. Такой подход уменьшает вероятность того, что отдельная техническая отметка будет истолкована вне контекста.

При работе с социальными сетями необходимо разграничивать открытый контент, персональные данные и сведения, охраняемые тайной переписки и иных сообщений. Открытая доступность страницы не устраняет требований законодательства о персональных данных и не предоставляет права на несанкционированный доступ к закрытой переписке. Получение сведений из закрытых источников должно осуществляться при наличии предусмотренных

законом оснований и с соблюдением соответствующей процедуры. В числе нормативных ориентиров можно назвать Конституция Российской Федерации, УПК РФ, федеральные законы об оперативно-розыскной деятельности, противодействии экстремистской деятельности, информации и персональных данных [7–12].

Важно также отделять ориентирующую информацию, полученную в ходе анализа открытых источников, от результатов процессуального доказывания. Сведения OSINT могут помочь сформировать версию, определить учетную запись или обнаружить источник цифровых следов. Однако для использования соответствующих материалов в уголовном деле требуется соблюдение процессуального порядка получения и закрепления. Аналитическая справка, подборка ссылок или результат программной выгрузки не должны подменять надлежащее оформление осмотра, выемки, экспертного исследования либо другого предусмотренного законом действия.

Особого внимания требует взаимодействие с администрацией социальной платформы. В обращении целесообразно индивидуализировать учетную запись или публикацию, указать временной интервал, цель и правовое основание запроса. Следует разграничивать сохранение данных и их предоставление: необходимость предотвратить удаление определенного объекта не означает автоматического права получить весь объем информации о пользователе. Объем запрашиваемых сведений должен соответствовать задаче, а обмен материалами — осуществляться по официальным и защищенным каналам. Такой подход одновременно способствует сохранению следов и снижает риск чрезмерного вмешательства в частную жизнь.

Результаты фиксации должны позволять другим участникам процесса понять, какой именно цифровой объект исследовался, откуда он получен и какие операции с ним проводились. В этой связи целесообразно использовать унифицированную карточку цифрового объекта, включающую идентификатор, источник, дату и время получения, способ доступа, описание содержимого, перечень файлов, контрольные значения, место хранения и историю

преобразований. Единообразное документирование облегчает сопоставление объектов, повторную проверку и передачу материалов между подразделениями.

Техническая сложность цифровой среды обусловливает необходимость привлекать специалиста на раннем этапе, когда требуется определить порядок осмотра, выбрать способ копирования и предупредить изменение исходных данных. Компьютерно-технические знания необходимы для исследования устройства, файловой системы, приложений, метаданных и признаков вмешательства. При этом технический специалист не подменяет следователя в определении процессуальных задач и не дает правовую оценку действиям пользователя.

В зависимости от содержания материала могут потребоваться знания в области лингвистики, психологии, религиоведения и иных дисциплин. Лингвистический анализ помогает исследовать смысловую структуру текста, употребление выражений, контекст и коммуникативную направленность. Исследование изображения или видеозаписи может требовать специальных знаний для установления признаков монтажа или цифровой обработки. Вопросы экспертам должны формулироваться с учетом природы объекта и не сводиться к требованию дать окончательную уголовно-правовую квалификацию. Заключение специалиста и заключение эксперта имеют самостоятельное процессуальное значение и различаются по основаниям и порядку получения.

Для обеспечения проверяемости исследования в материалах следует отражать исходные данные, использованные программы и их версии, последовательность операций, параметры обработки и ограничения метода. Если эксперт исследовал не оригинал, а копию или распечатку, необходимо учитывать, какие свойства исходного цифрового объекта при этом были утрачены. В научной литературе обращается внимание на необходимость комплексного информационно-компьютерного обеспечения криминалистической деятельности и сохранения возможности проверить полученный результат [14, с. 77–81, 13, с. 250–262].

Получение и исследование информации из социальных сетей должно строиться как последовательный криминалистический процесс: от определения источника и правового основания доступа до фиксации, сохранения, анализа и документирования истории обращения с цифровым объектом. Использование OSINT и SOCMINT расширяет возможности обнаружения первоначальных сведений, но результаты автоматизированного поиска требуют проверки и не заменяют процессуального закрепления доказательств.

Для повышения надежности цифровых материалов предлагается дополнять визуальную фиксацию сведениями об адресе страницы, идентификаторе объекта, времени доступа, контексте, вложениях и использованных средствах, сохранять исходные файлы и историю операций, применять контрольные значения как способ контроля неизменности, не приписывая им доказательственного значения сверх их технической функции, обеспечивать соразмерность копирования и запросов к платформам.

Соблюдение правовых пределов доступа и привлечение специалистов на ранних этапах позволяет повысить качество цифровых материалов, сократить риск утраты данных и обеспечить возможность последующей проверки их происхождения и целостности.

СПИСОК ЛИТЕРАТУРЫ:

1. Батоев В.Б. О технологии поиска по открытым источникам «OSINT» в оперативно-розыскной деятельности // Вестник Уфимского юридического института МВД России. 2023. № 2 (100). С. 66–71
2. Васюков В.Ф., Афанасьев А.Ю. К вопросу о получении оперативно значимой информации из открытых источников информации сети «Интернет» // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2024. № 1 (65). С. 79–86 https://doi.org/10.36511/2078-5356-2024-1-79-86
3. Демидченко Ю.В. Обеспечение целостности электронных доказательств в уголовном процессе: возможности криптографического хеширования // Право и практика. 2026. № 2. С. 142–148

4. Пастухов П.С. Средства проверки надежности «электронных» доказательств в ходе производства по уголовному делу // Пробелы в российском законодательстве. 2015. № 3. С. 170–173

5. Россинская Е.Р., Семикаленова А.И., Рядовский И.А., Сааков Т.А. Теория информационно-компьютерного обеспечения криминалистической деятельности: монография. Москва: Проспект, 2023. 256 с.

6. Смушкин А.Б. Криминалистическое исследование страницы в социальных сетях // Вестник Томского государственного университета. 2024. № 505. С. 246–253 https://doi.org/10.17223/15617793/505/27

7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства РФ. 24.12.2001. № 52

8. Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» // Российская газета. 18.08.1995. № 160

9. Федеральный закон от 31.05.2001 № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации» // Российская газета. 05.06.2001. № 106

10. Федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности» // Собрание законодательства РФ. 29.07.2002. № 30. Ст. 3031

11. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 29.07.2006. № 165

12. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Российская газета. 29.07.2006. № 165

13. Чич Ю.А., Романов А.В. Процессуальные особенности собирания электронных доказательств в социальных сетях // Эпомен. 2026. № 113. С. 250–262

14. Шубина К.С. Актуальные проблемы собирания цифровых следов преступлений из социальных сетей и мессенджеров // Современные проблемы уголовного судопроизводства, криминалистики и судебной экспертизы: материалы XII Всероссийской научно-практической конференции. Саратов, 2024. С. 77–81

Kolotovkina A.A.
master's degree student of 3rd year
Krasnoyarsk State Agrarian University
(Krasnoyarsk, Russia)

FEATURES OF COLLECTING, DOCUMENTING AND EXAMINING DIGITAL TRACES FROM SOCIAL NETWORKS IN CRIMINAL INVESTIGATIONS

Abstract: *this article examines forensic and procedural aspects of obtaining information from social networks during investigations of extremist crimes. It explores OSINT and SOCMINT capabilities and the stages of identifying, documenting, preserving and subsequently analyzing digital objects. It analyzes the limitations of screenshots and automated collection, as well as the importance of metadata, hash values and documenting the chain of custody for digital materials. It argues for distinguishing publicly available information from personal data and information protected by the confidentiality of communications, and for involving specialists at an early stage of investigation.*

Keywords: *digital trace, social network, OSINT analysis, SOCMINT monitoring, information documentation, electronic evidence, metadata, computer forensic examination.*