

МЕТОДИКА РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ, СОВЕРШЕННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

Сайгачева Ирина Александровна*

магистр

ira.saigacheva@mail.ru

* Национальный исследовательский
Мордовский государственный университет им. Н.П. Огарева,
г. Саранск, Россия

Аннотация:

В статье автором рассматриваются основные элементы методики расследования преступлений экстремистской направленности. Рассмотрены особенности проверки сообщений о преступлении. Представлены основные рекомендации производства следственных действий, направленные на повышение эффективности сбора криминалистически значимой информации на первоначальном и последующем этапах расследования преступлений данной категории.

Ключевые слова:

криминалистическая методика расследования преступлений, преступление экстремистской направленности, экстремизм, компьютерные технологии

УДК 347.77

DOI: 10.24411/2658-6932-2025-12-24-32

Для цитирования: Сайгачева И. А. Методика расследования преступлений экстремистской направленности, совершенных в компьютерных сетях / И. А. Сайгачева // Контентус. – 2025. – № 12. – С. 24 – 32.

Согласно данным официальной статистики, в Российской Федерации отмечается поступательный рост количества преступлений экстремистской направленности [10]. Высокодинамичное развитие компьютерных и информационных технологий оказало влияние на все сферы жизни общества, однако, нередкими являются и случаи, когда

достижения научно-технического прогресса используются не на благо человечества, так расширение информационного пространства и включение в него значительной социально-активной части населения повлекло существенное изменение характера и структуры преступности. Не исключением является и категория преступлений террористической и экстремистской направленности. Рост данной категории преступлений не в последнюю очередь обусловлен облегченностью их совершения при активном использовании компьютерных технологий в противоправной деятельности, а также ощущением безнаказанности, вызванной крайне латентным характером данных преступлений, связанным анонимизацией преступников. Однако в силу высокой общественной опасности экстремистских преступлений, подрывающих основы конституционного строя, дестабилизирующих и без того напряженную социальную обстановку, проблема выявления, раскрытия и расследования таких преступлений становится в числе первоочередных задач правоохранительных органов на современном этапе. Вместе с тем, в настоящее время практика расследования преступлений, совершаемых с применением компьютерных технологий, демонстрирует крайне неудовлетворительное состояние, что обуславливается, с одной стороны, сложностью преодоления консервативного отношения представителей традиционного уголовного розыска к современным вызовам, а с другой стороны, значительным отставанием отечественной криминалистической науки и инструментария правоохранительных органов от скоротечно изменяющегося и развивающегося преступного мира, в существенной доле перешедшего в информационное пространство [7, с. 284]. В связи с этим, совершенствование методических знаний в сфере расследования преступлений указанной категории продолжает сохранять свою актуальность. В настоящем исследовании нами предпринята попытка обзорного обобщения основных наработок и последних достижений криминалистической науки, противопоставляемой государством неуклонно нарастающей экстремистской угрозе общественной безопасности с акцентом на ее цифровую трансформацию.

Ключевое значение рассматриваемой категории преступлений состоит в использовании сети Интернет как многоаспектного способа совершения экстремистского преступления, применяемого для установления и поддержания коммуникации между членами экстремистских сообществ и организаций (поскольку большинство преступлений данной категории носят групповой характер); распространения запрещенной идеологии, культурно-религиозной пропаганды радикального толка, поиска и вербовки новых членов и последователей, организации финансирования экстремистских групп и организаций, совершаемых ею противоправных акций: сбора,

накопления и систематизации сведений об объектах, на которые направлено воздействие организаций [4, с. 390].

Основным поводом для проведения оперативно-розыскных мероприятий в рамках проверки сообщения о преступлении экстремистского характера выступают обращения граждан и организаций, самостоятельно обнаруживших информацию, которая, по их мнению, носит характер экстремистских материалов, а также результаты регулярного мониторинга сети Интернет, в частности, информации, размещенной средствами массовой информации, осуществляемой сотрудниками правоохранительных органов. Основной целью первоначальных оперативно-розыскных мероприятий является подтверждение поступивших данных, а также сбор необходимого объема сведений об обстоятельствах совершенного деяния и лицах, к нему причастных. На данном этапе к числу задач, стоящих перед сотрудниками правоохранительных органов, относятся: установление места выхода в сеть, содержание размещенной в сети информации, особенности программно-технических средств, используемых для размещения и распространения потенциально экстремистских сведений, идентификация индивидуальных номеров устройств, подключенных к сети и работающих по протоколу IP [3, с. 59].

В целях наиболее полной и всесторонней проверки поступившего сообщения о преступлении следователю рекомендуется выполнить ряд обязательных действий и мероприятий, в том числе:

- Во-первых, назначить судебно-лингвистическую экспертизу, направленную на установление наличия или отсутствия в исследуемой информации сведений, выражений, носящих экстремистский характер, то есть имеющих цель разжигания ненависти или вражды в отношении определенных социальных групп;

- Во-вторых, произвести детальный осмотр интернет-ресурса (веб-страницы, форума, аккаунта в социальной сети), на котором был обнаружен и размещен противоправный контент, с фиксацией его технических и визуальных характеристик;

- В-третьих, провести опрос сотрудников оперативных подразделений, осуществлявших документирование факта размещения материалов в рамках оперативно-розыскных мероприятий, а также понятых, присутствовавших при данных действиях;

- В-четвертых, направить адресный запрос администрации или подразделению безопасности соответствующего интернет-ресурса с целью получения идентификационных и регистрационных данных пользователя, включая историю IP-адресов, использовавшихся для доступа к аккаунту в периоды, значимые для расследования;

- В-пятых, истребовать у провайдера интернет-услуг и оператора связи документально подтвержденные сведения об абоненте, за

которым закреплен установленный IP-адрес, а также копию действующего договора на оказание услуг связи;

– В-шестых, на основании полученных данных установить точный физический адрес (местонахождение), с которого осуществлялся выход в сеть для публикации запрещенной информации, и собрать характеризующие данные на лицо, за которым это место закреплено;

– В-седьмых, в установленном законом порядке изъять все сетевое оборудование и технические устройства, потенциально использовавшиеся для доступа в сеть «Интернет» по указанному адресу;

– В-восьмых, провести допрос лица, в отношении которого имеются подозрения, а также совместно проживающих с ним лиц для выяснения порядка общего и индивидуального пользования техническими средствами, особенностей доступа к сети и парольной политики [5, с. 53].

Эффективность и сроки расследования во многом зависят от профессиональной компетенции следователя. Она должна проявляться в умении формулировать детальные и технически грамотные вопросы при допросе подозреваемых и обвиняемых, при назначении экспертного исследования, а также в методически правильном производстве таких действий, как осмотр места происшествия и вещественных доказательств (документов), изъятых в ходе следствия.

На начальном этапе расследования, непосредственно после его возбуждения, следователь обязан оперативно реализовать ряд первоначальных следственных действий. К ним относится, прежде всего, осмотр места, связанного с событием преступления.

Параллельно возникает необходимость допроса лиц, проживающих совместно с подозреваемым (обвиняемым), для сбора сведений, характеризующих его личность, особенности семейных отношений, а также для выявления возможных фактов необычного поведения в общении с третьими лицами или специфических увлечений. При подтверждении данных о нахождении вещественных доказательств в определенном месте проводится обыск.

Важнейшим направлением работы является сбор и процессуальная фиксация цифровых следов. Для этого у провайдера сетевых услуг истребуется информация о сетевой активности фигуранта, а у операторов сотовой связи – детализированные данные о его телефонных соединениях. Администрации крупнейших интернет-платформ и социальных сетей запрашиваются на предмет предоставления регистрационных данных и истории переписки. Все полученные в результате электронные носители информации и распечатки подлежат осмотру с участием специалиста в строгом соответствии со положениями уголовно-процессуального закона. Необходимость производства иных следственных действий вытекает из конкретной следственной ситуации.

Допрос фигурантов (подозреваемых или обвиняемых) и свидетелей в рамках данной категории дел требует особого методического подхода, обусловленного цифровой средой совершения преступлений. Его проведение направлено на установление ключевых элементов состава преступления и выявление механизма противоправной деятельности [2, с. 100].

Основное внимание уделяется выяснению обстоятельств, связывающих лицо с цифровыми сведениями и экстремистской деятельностью. Ключевыми темами для проведения допроса являются:

- цифровая идентификация и деятельность – установление используемых аккаунтов в социальных сетях и мессенджерах (имена, цели регистрации, предоставленная о себе информация), характера и содержания онлайн-коммуникации. Особое значение имеет выяснение фактов обсуждения экстремистских идей и круга соответствующих собеседников;

- техническая и инфраструктурная составляющая – определение применяемых для доступа в сеть технических средств (их происхождение и круг пользователей), поставщика интернет-услуг. Важным блоком является оценка уровня цифровой грамотности лица;

- происхождение и распространение противоправного контента – выяснение обстоятельств получения, хранения и возможной рассылки материалов экстремистской направленности, а также их публикации на ресурсах открытого доступа;

- причастность к экстремистским структурам и мотивация – установление факта членства или участия в деятельности запрещенного сообщества (название, структура, цели), роли в нем фигуранта, мотивов его действий, а также обстоятельств вовлечения в эту деятельность иных лиц [6, с. 82].

Для эффективного преодоления возможного технического противодействия или непонимания специальной терминологии к допросу целесообразно привлекать специалиста в сфере информационных технологий.

Круг свидетелей по таким делам широк и может включать как лиц из ближайшего окружения фигуранта (родственники, друзья), так и случайных интернет-пользователей, администраторов онлайн-платформ, а также экспертов (лингвистов, религиоведов). Основные цели их допроса состоят в необходимости установления характера взаимоотношений с фигурантом и получение его характеризующих данных (личные качества, круг интересов, особенности общения); в фиксации обстоятельств знакомства с исследуемой информацией, источников и условий его получения, а также субъективного восприятия этой информации; в выяснении порядка коллективного или индивидуального использования компьютерной техники и доступа к

сети, что может иметь значение для установления взаимосвязи между противоправными действиями и конкретным лицом.

Таким образом, допрос в данных делах выступает как комплексное действие, синтезирующее традиционные приемы получения показаний со специальными познаниями в области информационных технологий и экспертных оценок. Его содержание строго детерминировано необходимостью доказать умысел, установить способ совершения преступления и документально зафиксировать цифровую цепочку от ее исполнителя до конечного адресата. Далее рассмотрим особенности осмотра места происшествия по данной категории дел.

Ключевой особенностью является его распределенный (нетопологический) характер. Локации, подлежащие осмотру, зачастую географически разобщены, поскольку этапы создания, хранения, распространения и использования противоправного контента могут быть территориально разделены. Это требует проведения осмотров в нескольких пунктах [9, с. 60].

Высокая сложность данного следственного действия обусловлена необходимостью сохранения целостности цифровых доказательств. В связи с этим, подготовка к осмотру должна включать в себя: привлечение специалистов (IT-эксперта, криминалиста), инструктаж всех участников (включая понятых) о порядке действий; обеспечение специальным оборудованием и программной средой для копирования данных на месте без их изменения.

К изымаемым и исследуемым объектам относятся: аппаратные средства (системные блоки, ноутбуки, мобильные устройства, SIM-карты, модемы); цифровые носители (оптические диски, флеш-накопители), программные среды и объекты (интернет-браузеры с историей, аккаунты в социальных сетях, отдельные файлы – изображения, видео, тексты) [8, с. 185].

Осмотр требует детального протоколирования всех манипуляций с устройствами (включение, поиск данных, выключение). Фиксация результатов следственного осмотра должна включать в себя: текстовую часть протокола – полное описание действий и обнаруженных предметов; визуальную фиксацию – обязательное применение скриншотов (снимков экрана) с их последующей распечаткой и/или сохранением на прилагаемом диске. Скриншоты должны отображать контекст и всю ключевую информацию, а также реквизиты ресурса (адресную строку браузера, дату и время системы). Особое внимание уделяется осмотру профилей в социальных сетях, где необходимо зафиксировать все данные: время создания, указанные анкетные сведения, список контактов, визуальный контент, переписку.

Помимо основного места, проводится осмотр локаций, указанных фигурантом в показаниях (например, точек доступа в сеть, где велась

противоправная деятельность). Такой осмотр предпочтительно проводить с участием самого подозреваемого (обвиняемого) и в обязательном порядке фиксировать на видео или фото.

Доказательственную силу результаты осмотра приобретают только при неукоснительном соблюдении норм уголовно-процессуального закона, регламентирующих порядок его производства и оформления. Каждое действие должно находить точное отражение в протоколе, а изъятые цифровые носители – быть надлежаще упакованы и опечатаны для исключения возможности признания важнейших результатов следственных мероприятий недопустимыми доказательствами.

Таким образом, расследование преступлений экстремистской направленности, совершаемых с использованием информационно-телекоммуникационных сетей, характеризуется ярко выраженной спецификой, требующей адаптации традиционных следственных действий к особенностям поиска, обнаружения, фиксации и изъятия криминалистически значимой информации в цифровой среде. Ключевыми особенностями являются нетопологический характер места происшествия, необходимость специальных технико-криминалистических знаний для работы с цифровыми доказательствами и обязательное комплексное применение традиционных и специализированных методик. Эффективность расследования напрямую зависит от способности следователя организовывать междисциплинарное взаимодействие и скрупулезно соблюдать процессуальный порядок фиксации электронной информации, обеспечивая её допустимость и достоверность в качестве доказательств.

Список использованных источников

1. **1. Баранов В. В.** Некоторые проблемы расследования и противодействия расследованию экстремистских преступлений, совершаемых с использованием сферы телекоммуникаций и компьютерной информации // Труды Академии управления МВД России. – 2022. – № 1 (61). – С. 70-80.
2. **Болвачев М. А.** О следственных действиях по делам о преступлениях экстремистской направленности в социальных сетях // Известия ТулГУ. – 2022. – № 2. – С. 98-105.
3. **Вершицкая Г. В.** Некоторые криминалистические аспекты расследования преступлений экстремистской направленности // Вестник ПАГС. – 2020. – № 1. – С. 57-63.
4. **Герасименко Н. И.** Особенности использования сети интернет в расследовании преступлений экстремистской направленности // Пенитенциарная наука. – 2020. – № 3. – С. 388-393.
5. **Иващенко М. А.** Интернет-экстремизм: алгоритм действий следователя // Уголовный процесс. – 2020. – № 12(192). – С. 49-57.
6. **Иващенко М. А.** Расследование преступлений экстремистской направленности, совершенных с использованием сети Интернет: учебно-методическое пособие. – М.: Московская академия СК России, 2019. – 146 с.
7. **Ковылина П. С.** Актуальные проблемы тактики и методики расследования экстремистских преступлений, совершаемых в глобальной сети Интернет // Молодой ученый. – 2023. – № 21 (468). – С. 284-286.
8. **Ложис З. З.** Применение специальных знаний при расследовании преступлений экстремистской направленности, совершенных в сети Интернет, а также преступлений террористического характера в практике Следственного комитета Российской Федерации // Актуальные проблемы российского права. – 2021. – № 6 (127). – С. 178-193.
9. **Францифоров Ю. В.** Расследование преступлений экстремистской направленности // Legal Concept. 2020. №2. – С. 57-63.
10. Число осужденных за терроризм и экстремизм возросло в первом полугодии 2025 года // Коммерсантъ. – URL: <https://www.kommersant.ru/doc/8138991> (дата обращения: 25.11.2025).

INVESTIGATION METHODOLOGY FOR EXTREMIST CRIMES COMMITTED ON COMPUTER NETWORKS

Saigacheva Irina Aleksandrovna **

Master's student

ira.saigacheva@mail.ru

** National Research Mordovian State University,
Saransk, Russia

Abstract:

This article examines the key elements of investigation methods for extremist crimes. The author discusses the specifics of verifying crime reports. Key recommendations for investigative actions aimed at increasing the efficiency of collecting forensically relevant information at the initial and subsequent stages of investigating this category of crime are presented.

Keywords:

forensic investigation methods, extremist crime, extremism, computer technology.