

3. О противодействии терроризму : федеральный закон № 35-ФЗ (принят Государственной Думой Российской Федерации от 6 марта 2006 г., в ред. от 28 февраля 2025 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

4. Романовский В. Г. Противодействие терроризму в странах ОДКБ : основные тенденции и перспективы // Электронный научный журнал «Наука. Общество. Государство». 2020. Т. 8, № 1 (29). С. 156–165.

5. Щеколдина Т. И. Контртеррористическая и антиэкстремистская деятельность ОДКБ // Постсоветские исследования. 2019. № 6. С. 1373–1384.

© Лисаускайте В. В., 2026

УДК 343.13

Маликова Н. В. – доцент кафедры уголовного процесса Уфимского юридического института МВД России, кандидат юридических наук, доцент (Россия, г. Уфа)

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ СРЕДИ МОЛОДЕЖИ

FEATURES OF INVESTIGATION OF EXTREMIST CRIMES AMONG YOUNG PEOPLE

Аннотация. В статье исследуются криминалистические и процессуальные особенности расследования преступлений экстремистского характера, совершаемые лицами в возрасте 14–35 лет¹. Анализируются современные способы вовлечения молодежи в экстремистскую деятельность, включая использование цифровых платформ и психологических технологий манипулирования. Выявлены ключевые проблемы доказывания: латентность преступлений, противодействие расследованию со стороны организаторов, высокая скорость удаления цифровых следов. Предложены пути совершенствования методики расследования: межведомственное взаимодействие, алгоритмизация работы с Big Data и внедрение социально-психологических экспертиз.

Ключевые слова: экстремизм, молодежная среда, расследование, цифровые следы, уголовный процесс, противодействие экстремизму.

¹ С 2020 г. согласно Федеральному закону от 30 декабря 2020 года № 489-ФЗ «О молодежной политике в Российской Федерации» под молодежью понимается категория граждан в возрасте от 14 до 35 лет.

Abstract. The article examines the forensic and procedural features of the investigation of extremist crimes committed by individuals aged 14–25. It analyzes modern methods of involving young people in extremist activities, including the use of digital platforms and psychological manipulation techniques. The article identifies key challenges in proving such crimes, such as the latency of crimes, the resistance of the organizers to investigation, and the rapid deletion of digital traces. The article proposes ways to improve the investigation methodology, including interagency cooperation, the use of Big Data algorithms, and the implementation of socio-psychological examinations.

Keywords: extremism, youth environment, investigation, digital traces, criminal proceedings, countering extremism.

Актуальность расследования экстремистских преступлений среди молодежи обусловлена тремя основными факторами.

Во-первых, глобальной тенденцией к омоложению субъектов экстремистской деятельности. По данным ГИАЦ МВД России, за последние пять лет доля лиц в возрасте 14–35 лет среди осужденных за преступления экстремистской направленности выросла на 37 % [1]. Молодежь рассматривается организаторами деструктивных сообществ как «расходный материал» ввиду низкой правовой социализации, импульсивности и стремления к самоутверждению.

Во-вторых, цифровой трансформацией способов совершения преступлений. Экстремистская пропаганда, призывы, вербовка и даже координация противоправных актов все чаще перемещаются в мессенджеры (Telegram, WhatsApp), закрытые группы в социальных сетях, даркнет-форумы и игровые платформы. Это создает новые, нетривиальные для традиционного уголовного процесса источники доказательств.

В-третьих, высокой общественной опасностью. Молодежный экстремизм часто сопряжен с совершением тяжких насильственных действий (нападения на учебные заведения, уличные погромы) и имеет ярко выраженный демонстративный характер, что вызывает широкий общественный резонанс и дестабилизирует социальную обстановку [2, с. 15–18].

Несмотря на повышенное внимание правоохранительных органов, расследование данной категории дел сталкивается с системными проблемами.

1. Латентность и трудности фиксации первичной информации.

Большинство экстремистских проявлений (посты, переписка, репосты) долгое время остаются в «серой зоне» – они не заявляются очевидцами, а выявляются оперативно-розыскным путем. Момент перехода от слов к действиям следователь часто пропускает, так как отсутствует четкий критерий, когда мониторинг должен перерасти в уголовное дело.

2. Проблема «цифрового расследования».

1. Быстрое уничтожение следов: участники групп экстремистской направленности используют самоуничтожающиеся сообщения, VPN, анонимные браузеры.

2. Большой объем информации: изъятие одного смартфона у подозреваемого может давать до 500 ГБ данных, среди которых нужно найти криминалистически значимые фрагменты.

3. Юридическая квалификация: суды не всегда принимают скриншоты как допустимые доказательства без судебной компьютерно-технической экспертизы, проведение которой требует времени, в течение которого контент может быть удален.

3. Противодействие расследованию со стороны взрослых кураторов.

Организаторы экстремистских сообществ действуют анонимно, используют подставные аккаунты, криптовалюту для оплаты «активистам» и инструктируют молодежь о том, как вести себя при задержании (отказ от дачи показаний, заведомо ложные алиби). Молодые исполнители нередко сами не знают личности кураторов, что обрывает цепочку доказывания на уровне рядового участника.

4. Психологическая специфика работы с подозреваемыми.

Несовершеннолетние и молодые экстремисты часто находятся в состоянии когнитивного диссонанса: они искренне верят в идеологию, либо, напротив, глубоко раскаиваются, но боятся мести сообщества [3, с. 180–189]. Стандартные допросы «по шаблону» неэффективны. Требуются специалисты-психологи, однако в штате следственных органов их остро не хватает.

Преодоление указанных проблем требует не только законодательных изменений, но и внедрения криминалистических и управленческих новаций.

1. Формирование специализированных следственно-оперативных групп (далее – СОГ) с цифровым профилем.

В состав СОГ по делам о молодежном экстремизме следует включать не только следователя и оперуполномоченного, но и специалиста по компьютерно-техническим экспертизам, аналитика социальных сетей и психолога. Это позволит проводить неотложные действия (осмотр места происшествия, выемку электронных устройств) с одновременным зеркалированием данных без их утраты.

2. Алгоритмизация работы с открытыми данными и Big Data.

Предлагается внедрение ведомственного программного обеспечения, которое в автоматическом режиме:

- выявляет в открытых пабликах и чатах экстремистские паттерны (использование специфической лексики, символики, командных фраз);
- фиксирует динамику роста аудитории деструктивных групп;
- составляет временные и коммуникативные сети участников.

Полученные результаты должны служить основанием для назначения лингвистической судебной экспертизы, а не только оперативной проверки.

3. Развитие института «цифрового понятого» и спецхранения.

Для преодоления проблемы допустимости доказательств предлагается законодательно закрепить возможность участия понятого [4, с. 129–130] в дистанционном осмотре интернет-страниц с помощью видео-конференц-связи. Также необходимо создать специализированные хранилища изъятых цифрового контента (серверы с повышенной защитой) с обязательной блокчейн-фиксацией каждого действия с файлом, чтобы исключить заявления защиты о фальсификации.

4. Межведомственный протокол «быстрого замораживания» данных.

Разработать и утвердить на уровне Генпрокуратуры, МВД, ФСБ и Роскомнадзора единый регламент, по которому при получении первичной информации о готовящемся преступлении экстремистской направленности правоохранительные органы в течение 1 часа направляют операторам связи и владельцам платформ требование о сохранении данных (прекращении автоматического удаления сообщений) на срок до 10 суток без судебного решения, с последующим уведомлением судьи в течение 24 часов.

5. Введение обязательной комплексной психолого-лингвистической экспертизы личности несовершеннолетнего подозреваемого.

Назначать такую экспертизу до предъявления обвинения, чтобы определить:

- степень внушаемости и наличие признаков идеологического манипулирования;
- наличие или отсутствие корыстного мотива;
- реальную возможность осознавать общественную опасность своих действий (с учетом возрастных психофизиологических особенностей).

Это позволит дифференцировать ответственность и строить тактику допроса не на конфликте, а на сотрудничестве, особенно в случаях, когда подросток сам стал жертвой вербовки.

Подводя итог, следует отметить, что расследование преступлений экстремистской направленности среди молодежи требует отхода от шаблонных методик. Ключевой вектор развития – переход от реактивного (расследование уже совершенного) к превентивно-расследовательному (выявление и блокировка на стадии приготовления) подходу на основе цифровой криминалистики и междисциплинарного взаимодействия. Реализация предложенных путей позволит не только повысить раскрываемость, но и минимизировать сам феномен вовлечения молодежи в экстремистскую деятельность.

Библиографический список

1. Состояние преступности в России за 2021-2025 годы // ГИАЦ МВД России. URL: <https://xn--b1aew.xn--p1ai/reports/> (дата обращения: 23.03.2026).

2. Мешев И. Х. Экстремизм в молодежной среде : причины возникновения и пути противодействия // Международный научный вестник. 2024. № 9. С. 15–18.

3. Шиповская В. В., Гуссейнов А. Ш. Психологические факторы риска экстремистской активности личности в молодежной среде // Научно-практический журнал «Гуманизация образования». 2019. № 5. С. 180–189.

4. Кузора С. А. Проблемы участия понятых при производстве следственных действий с электронными носителями информации // Закон и право. 2010. № 10. С. 129–130.

© Маликова Н. В., 2026

УДК 343.85: 343.34(470)

Миняшева Г. И. – доцент кафедры оперативно-разыскной деятельности органов внутренних дел Уфимского юридического института МВД России, кандидат юридических наук (Россия, г. Уфа)

НЕКОТОРЫЕ ОСОБЕННОСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ

SOME FEATURES OF COUNTERING EXTREMIST CRIMES

Аннотация. Интересы обеспечения национальной безопасности государства диктуют необходимость повышения эффективности противодействия экстремизму во всех проявлениях, видах и формах. Несмотря на то, что органами внутренних дел постоянно проводится работа по недопущению экстремистских проявлений, противодействию вербовке граждан Российской Федерации, экстремизм продолжает оставаться одной из самых сложных проблем современности.

Ключевые слова: экстремизм, информационная безопасность, противодействие экстремизму, информационные технологии, искусственный интеллект.

Abstract. The interests of ensuring the national security of the state dictate the need to increase the effectiveness of countering extremism in all its manifestations, types, and forms. Despite the fact that the internal affairs agencies are constantly working to prevent extremist manifestations and counter the recruitment of citizens of the Russian Federation, extremism remains one of the most complex problems of our time.

Keywords: extremism, information security, countering extremism, information technology, artificial intelligence.