УДК 343.98.068

ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ЭКСТРЕМИСТСКИХ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ: ПРОБЛЕМЫ ПОДСЛЕДСТВЕННОСТИ И ВЗАИМОДЕЙСТВИЯ

Ярощук И.А.

И.о. заведующего кафедрой судебной экспертизы и криминалистики

Кандидат филологических наук, доцент

Белгородский государственный национальный исследовательский университет

Белгород, Россия

Митрофанова М.А.,

Студент Юридического института

Белгородский государственный национальный университет

Белгород, Россия

Степанченко С.П.

Студент Юридического института

Белгородский государственный национальный университет

Белгород, Россия

Аннотация

Исследуются сложности, которые формируются при использовании актуальных тактических приемов криминалистики в процессе раскрытия экстремистских преступлений, реализуемых посредством интернет-пространства.

Ключевые слова: криминалистика, тактика расследования, экстремизм, глобальная сеть Интернет, виртуальные следы.

ORGANIZATION OF INVESTIGATION OF EXTREMIST CRIMES COMMITTED USING THE INTERNET: PROBLEMS OF INHERENT RESPONSIBILITY AND INTERACTION

Yaroshchuk I.A.
Candidate of Philological Sciences, Associate Professor
Acting Head of the Department of Forensic Science and Criminalistics
Belgorod State National Research University
Belgorod, Russia

Mitrofanova M.A.,
Student at the Law Institute
Belgorod State National University
Belgorod, Russia

Stepanchenko S.P.
Student at the Law Institute
Belgorod State National University
Belgorod, Russia

Abstract
This article examines the challenges that arise when using current tactical methods of criminology in the process of solving extremist crimes committed via the Internet.
Keywords: criminology, investigative tactics, extremism, the global Internet, virtual traces.

Интеграция информационно-коммуникационных технологий в различные сегменты общественной жизни давно перестала восприниматься как инновация и прочно вошла в повседневный уклад. На протяжении длительного времени люди систематически обращаются к возможностям интернет-пространства,

активно используя социальные сети, которые выступают в роли ключевого инструмента для профессиональной деятельности, обмена сообщениями, поиска необходимых сведений и информации и решения большого количества задач.

Вместе с расширением цифрового взаимодействия нарастает и криминальная активность в интернет-среде. Все больше противоправных действий фиксируется в киберпространстве, а именно в мессенджерах, на различных интернет-площадках, а также иных сегментах глобальной сети. Сведения и данные, опубликованные на официальном ресурсе МВД РФ в настоящее время свидетельствуют о том, что порядка трети всех регистрируемых преступлений и правонарушений совершается с задействованием информационно-телекоммуникационных технологий [7]. В данный массив входят и противоправные деяния экстремистской направленности – они органично вписываются в общую негативную динамику.

На основании прим. 2 ст. 282.1 Уголовного кодекса Российской Федерации, к экстремистским преступлениям относятся деяния, которые обусловлены мотивами политической, идеологической, расовой, национальной или религиозной вражды, а также неприязнью по отношению к отдельной социальной группе [8]. Необходимо отметить, что при этом составы данных преступлений закреплены в действующем уголовном законодательстве российского государства. Объективная сторона указанных деяний заключает в себе обширный набор действий, и в настоящее время значительная их часть реализуется именно при помощи интернет-пространства, то есть цифровые каналы становятся ключевой площадкой для воплощения идентичных противоправных схем.

В рамках данного исследования необходимо подчеркнуть, что методика расследования экстремистских преступлений, совершенных с использованием сети Интернет сопровождается рядом проблем, которые на данный момент не находят должного решения. Как отмечают некоторые отечественные авторы, «препятствиями к эффективному расследованию соответствующих категорий

преступлений в заданных условиях являются факторы отсутствия у сети Интернет определенного собственника, предоставление каждому лицу неограниченного доступа к материалам, размещенным в ней, мировые масштабы охватов интернет-пользователей, а также возможности анонимного размещения экстремистских материалов в сети» [2, с. 74, 4, с. 390].

По справедливому замечанию профессоров Ю.В. Гаврилина и А.В. Шмонина, «экстремистские преступления, дистанционно совершаемые в сети Интернет, отображают следовую картину, исследование которой требует применения особых криминалистических технологий поиска, фиксации, хранения и использования виртуальных следов» [3, с. 108].

При расследовании преступлений экстремистской направленности, совершенных в глобальной сети Интернет, особое значение приобретает проведение лингвистических экспертиз, выступающих в качестве дополнительного доказательства по делу, а в некоторых случаях становящихся прямым аргументом квалификации содеянного как преступления. Как отмечается отечественными авторами, «их проведение наиболее эффективно в случаях использования среднего и мягкого языка вражды, не сопровождающегося прямым выражением ненависти. На основании этого практика применения лингвистической экспертизы при расследовании преступлений экстремисткой направленности отличается особой результативностью. Кроме того, как показывает судебная практика, наряду с производством лингвистических экспертиз при расследовании данной категории преступлений следователи нередко обращаются экспертной оценке материалов с психологической точки зрения – назначают производство психологических экспертиз» [3, С. 19].

Основополагающим условием результативного раскрытия экстремистских преступлений в интернет-пространстве выступает опора на базовые положения криминалистической техники. Стоит отметить, что освоение цифрового пространства трансформирует ключевые составляющие криминалистической

науки, это отражается не только на ее теоретических и методологических основаниях, но и напрямую воздействует на механизмы поиска и идентификации, в частности, на работу со следовой информацией, которая классически выступает в роли краеугольного камня любого расследования. В фокусе настоящего исследования – виртуальные следы, которые формируются в результате противоправной деятельности экстремистского характера.

Наиболее актуальным сдерживающим фактором для результативности следственной работы до настоящего времени остается отсутствие нормативно закрепленного подхода к категории виртуальных следов. В профессиональной среде трактовка данного феномена пока не унифицирована. В доктрине встречаются разного рода интерпретации природы такого феномена, хотя на практике соответствующие данные активно задействуются. Исследование актуальных юридических публикаций позволяет заключить, что в настоящее время назрела потребность в формировании отдельного направления в рамках криминалистической техники, либо самостоятельного учения о виртуальных следах. Его ключевая задача состоит в легализации понятия, систематизировании разновидности виртуальных следов, а также вписания их в сложившуюся следовую концепцию криминалистики. Четкое правовое регулирование данной категории способно в значительной степени усилить результативность раскрытия преступлений, которые совершаются с применением информационно-телекоммуникационных технологий, включая деяния экстремистской направленности.

Вместе с пробелами в теоретической части и законодательстве, расследованию препятствуют и прикладные сложности, которые характеризуются техническими и организационными особенностями цифровых платформ.

В современных условиях цифровые платформы выступают не только основополагающим каналом коммуникативных отношений, но и пространством распространения деструктивного контента, к примеру, идеологии

экстремистских объединений. Среди наиболее актуальных и активных площадок в российском сегменте выделяются такие мессенджеры, как «ВКонтакте» и Telegram. В настоящее время, как показывает динамика работы приложений, аудитория «ВКонтакте» достигает практически 75 миллиона пользователей ежемесячно, тогда как глобальная база Telegram превышает 500 миллионов человек [5, с. 276]. Стоит отметить, что ключевую долю активных участников данных онлайн-платформ формирует молодое поколение, которое отличается высокой степенью вовлеченности в цифровое взаимодействие и в то же время повышенной восприимчивостью к манипулятивным нарративам. Именно данная специфика делает вышеуказанные социальные сети приоритетными векторами для агитационной и вербовочной работы радикальных групп.

Правоохранительные органы и другие государственный структуры систематически реализуют комплекс мероприятий, направленных на мониторинг цифрового пространства, уделяя детальное внимание публичным блогам, сообществам и официальным Интернет-ресурсам. Для эффективного раскрытия экстремистских преступлений критически значимо получение доступа к релевантным электронным данным, а именно публикациям, переписка, материалам закрытых групп. Стоит сказать, что в данном аспекте правоприменительная практика говорит о существенных различиях в возможностях взаимодействия с различными платформами. К примеру, в отношении социальной сети «ВКонтакте» механизмы предоставления сведений о пользователях нормативно и технически проработаны, а обеспечение идентичного доступа к данным Telegram – остается нерешенной проблемой.

Дополнительным барьером выступает повсеместное внедрение технологий защиты пользовательской информации. Необходимо понимать, что, начиная с 2017 года, ведущие интернет-сервисы активно интегрируют протокол оконченного шифрования, который исключает возможность передачи ключей дешифрации третьим лицам, в частности уполномоченным органам государственной власти [9]. В результате технические ограничения платформ

фактически нивелируют потенциал правоохранительных структур по оперативному сбору доказательств, что существенно снижает эффективность выявления и расследования экстремистских преступлений в онлайн-среде.

Подводя итог, можно констатировать устойчивый рост количества экстремистских преступлений, реализуемых в цифровой среде. Виртуальное пространство создаёт удобные условия для тиражирования радикальных воззрений, одновременно формируя серьёзные барьеры для правоохранительной деятельности: ограничения в доступе к персональным и иным цифровым данным существенно осложняют идентификацию правонарушителей и формирование доказательственной базы по уголовным делам.

Библиографический список

1. Агибалов В. Ю. Виртуальные следы в криминалистике и уголовном процессе: дисс. канд. юрид. наук. М., 2012. 198 с.

2. 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. С. 70–80.

3. Болвачев М. А. Особенности производства лингвистических судебных экспертиз по делам о преступлениях экстремисткой направленности в социальных сетях // Криминалистика: вчера, сегодня, завтра. 2022. № 2. С. 17–24.

4. Гаврилин Ю. В., Шмонин А. В. Использование информации, полученной из сети «Интернет», в расследовании преступлений экстремистской направленности // Труды Академии управления МВД России. 2019. № 1 (49). С. 105–111.

5. Герасименко Н. И. Особенности использования сети Интернет в расследовании преступлений экстремисткой направленности // Пенитенциарная наука. 2020. № 3. С. 388–393.

6. Дубовик Н. Г. Криминологический анализ экстремистских проявления в социальных сетях // Вестник Воронежского института МВД России. 2019. № 2. С. 275–279.

7. Краткая характеристика состояния преступности в Российской Федерации за январь-март 2023 // [Интернет-ресурс] URL: https://мвд.рф/reports/item/37377025/ (дата обращения 30.10.2026).

8. Уголовный кодекс Российской Федерации от 13 июня 1996 года № 63-ФЗ (ред. от 14.03.2026) // Собрание законодательства РФ. 17.06.1996. № 25. Ст. 2954.

9. Решение Таганского районного суда г. Москвы от 13 апреля 2018 года по делу № 2-1779/2018 // [Интернет-ресурс «Официальный портал судов общей юрисдикции города Москвы»] URL: https://mos-gorsud.ru/rs/taganskij/services/cases/civil/details/2cc72aea-39e7-4f8e-adc9-37d170966efa (дата обращения 29.10.2026).