УДК 343.3

Сущность выявления и раскрытия преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей

Екатерина Андреевна Мишкичева
Следственный комитет Российской Федерации по Ставропольскому краю, Ставрополь, Россия, emishkicheva@mail.ru

Аннотация. Рассматриваются основы деятельности оперативных подразделений по борьбе, выявлению и раскрытию преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей. Цифровое пространство обеспечивает радикальным группировкам анонимность, высокую скорость передачи данных и колоссальный охват аудитории, что превращает киберэкстремизм в одну из ключевых угроз национальной безопасности. Анализируется влияние информационно-телекоммуникационных сетей на динамику экстремистской преступности, выявление и раскрытие данных деяний как гарантии национальной безопасности и общественной стабильности.

Ключевые слова: экстремизм, информационно-телекоммуникационные сети, оперативные подразделения, выявление преступлений, раскрытие преступлений

Для цитирования: Мишкичева Е.А. Сущность выявления и раскрытия преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей // Правда и закон. 2026. № 2(36). С. 70–79.

Place of identification and disclosure of crimes of extremist nature, committed with the use of information and telecommunication networks

Ekaterina A. Mishkicheva
Investigative Committee of the Russian Federation in the Stavropol Territory, Stavropol, Russia, emishkicheva@mail.ru

Abstract. Examines the basics of the activities of operational units to combat extremist crimes, identify and solve crimes of this category committed using information and telecommunication networks. The digital space provides radical groups with anonymity, high-speed data transmission, and a huge audience reach, which turns cyber-extremism into one of the key threats to national security. The article analyzes the impact of information and telecommunication networks on the dynamics of extremist crime, the identification and disclosure of these acts, as a guarantee of national security and public stability.

Keywords: extremism, information and telecommunication networks, operational units, crime detection, crime solving

For citation: Mishkicheva E.A. Place of identification and disclosure of crimes of extremist nature, committed with the use of information and telecommunication networks // Truth and law. 2026. № 2(36). P. 70–79.

XXI в. – эпохальный период цифровой глобализации. Информационно-телекоммуникационные сети, ранее являвшиеся редкой роскошью для человечества, в настоящее время составляют неотъемлемую часть обыденной жизни каждого. Люди с трудом могут представить свою жизнь без смартфонов, интернета, стремительно набравшего популярность искусственного интеллекта и т.п. Однако, несмотря

© Мишкичева Е.А., 2026

на достижение успеха в технологическом направлении, не стоит забывать и об обратной стороне медали – минусах, ключевыми из которых выступает зависимость общества от инноваций и их использования в преступных целях.

Рассматривая аспекты противодействия экстремизму необходимо остановиться на понятии самого экстремизма, закрепленном в ст. 1 Федерального закона от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности»[1], согласно которому экстремизм представляет собой насильственное изменение основ конституционного строя и (или) нарушение территориальной целостности Российской Федерации; публичное оправдание терроризма и иную террористическую деятельность; возбуждение социальной, расовой, национальной или религиозной розни; воспрепятствование законной деятельности государственных органов, органов местного самоуправления, избирательных комиссий, общественных и религиозных объединений или иных организаций, соединенное с насилием либо угрозой его применения и т.д.

Целесообразно также отразить понятие терроризма, под которым согласно ст. 3 Федерального закона от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму»[2] понимается идеология насилия и практика воздействия на принятие решения органами государственной власти, органами публичной власти федеральных территорий, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий.

Экстремизм и терроризм представляют собой самостоятельные правовые категории, но которые находятся в тесной взаимосвязи: экстремистская идеология нередко служит основой для террористической деятельности, а сам терроризм рассматривается как наиболее радикальная форма проявления экстремизма.

В мае 2013 г. Генеральный секретарь Организации Объединенных Наций Пан Ги Мун в предисловии к выступлению на заседании рабочей группы по осуществлению контртеррористических мероприятий высказался о том, что «Интернет является наглядным примером того, как террористы могут действовать на транснациональной основе; в ответ государствам необходимо думать и действовать на столь же транснациональной основе»[3].

Всемирное распространение экстремизма – современная, актуальная и глобальная проблема. Обсуждение вопросов координации усилий государств по борьбе с терроризмом и экстремизмом в рамках международных объединений, таких как БРИКС, ШОС (Шанхайская организация сотрудничества) и других, в очередной раз подчеркивает важность и значимость роли выявления и раскрытия преступлений экстремистской направленности для мировой безопасности [1]. Сотрудничество государств, в частности их правоохранительных органов на международном уровне, со специализированными компаниями (Group IB, Cyberint, SOCRadar, RecordedFuture, CrowdStrike и другими) позволило бы повысить эффективность противодействия экстремизму.

Статистические данные свидетельствуют о том, что только за последние десять лет количественный показатель преступлений террористической и экстремистской направленности в Российской Федерации с каждым годом лишь набирает обороты. Так, в 2015 г. было зарегистрировано 1 538 преступлений террористической направленности и 1 308 – экстремистской, в 2016 г. – 2 227 (+30,9 %) / 1 450 (+9,9 %), в 2017 г. – 1 871 (–16 %) / 1 521 (+4,7 %), в 2018 г. – 1 679 (–11,4 %) / 1 265 (–20,24 %), в 2019 г. – 1 806 (+7,03 %) / 585 (–116,2 %), в 2020 г. – 2 342 (+22,9 %) /

[1] О противодействии экстремистской деятельности: Федер. закон от 25 июля 2002 г. № 114-ФЗ (в ред. от 27 окт. 2025 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

[2] О противодействии терроризму: Федер. закон от 6 марта 2006 г. № 35-ФЗ (в ред. от 28 февр. 2025 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

[3] Использование интернета в террористических целях. Нью-Йорк: Издание Организации Объединенных Наций, 2013. 89 с.

833 (+29,8 %), в 2021 г. – 2 136 (–9,6 %) / 1 057 (+21,2 %), в 2022 г. – 2 233 (+4,34 %) / 1 566 (+32,5 %), в 2023 г. – 2 383 (+6,29 %) / 1 340 (–16,9 %), в 2024 г. – 3 714 (+35,8 %) / 1 800 (+25,6 %), в 2025 г. – 6 000 (+38,1 %) / 2 200 (+18,2 %), соответственно[4].

Динамика террористических преступлений в России в 2015–2021 гг. характеризуется относительной стабильностью, однако с 2022 года наблюдается резкий рост, достигший максимума в 2025 г. В отличие от этого, экстремистские преступления демонстрируют более плавную и устойчивую восходящую динамику.

По данным Министерства внутренних дел Российской Федерации за 2015–2025 гг. также наблюдается устойчивая тенденция роста преступлений террористического характера при волнообразной, но в целом возрастающей динамике преступлений экстремистской направленности[5].

Таким образом, выявление и раскрытие преступлений исследуемой категории на современном этапе характеризуется ускоренной криминализацией террористической деятельности при умеренном росте проявлений экстремизма.

Для уяснения сущности выявления и пресечения преступлений исследуемой категории, совершенных с использованием информационно-телекоммуникационных сетей, необходимо обратиться к примечанию к ст. 282.1 Уголовного кодекса Российской Федерации (УК РФ), согласно которому под преступлениями экстремистской направленности понимаются преступления, совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды либо по мотивам ненависти или вражды в отношении какой-либо социальной группы, предусмотренные соответствующими статьями Особенной части УК РФ и п. «е» ч. 1 ст. 63 УК РФ[6].

Вместе с тем сущность самого понятия экстремизма не ограничивается формальными положениями УК РФ. Ввиду отсутствия в науке единого понятия экстремизма, исследователи обращают внимание на разные подходы к его понимаю. Так, А. Шмид связывает его с насилием и терроризмом [2], К. Мадде – с отрицанием демократии [3], П. Коулман – с особенностями мышления [4], а М. Седжвик подчеркивает политическую и оценочную природу самого термина [5].

Проанализировав многогранность подходов, для наиболее полного уяснения сущности выявления и пресечения преступлений исследуемой категории можно предложить понимать экстремизм как совокупность идеологий и форм деятельности, характеризующихся приверженностью крайним взглядам, отрицанием демократического порядка, склонностью к поляризованному мышлению и допускающих или оправдывающих использование насильственных и иных радикальных средств для достижения целей.

Сущность выявления и раскрытия преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей, по мнению исследователей, заключается в эффективном обнаружении и процессуальном закреплении противоправных деяний, посягающих на основы конституционного строя, межнациональное и межрелигиозное согласие, с использованием специальных средств и методов работы в цифровой среде [6, 7].

В этом направлении среди исследователей также не сформировалось единого мнения относительно сущности выявления и раскрытия преступлений данной категории.

[4] Федеральная служба государственной статистики. URL: https://rosstat.gov.ru (дата обращения: 06.04.2026).
[5] Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/dejatelnost/statistics (дата обращения: 15.04.2026).
[6] Уголовный кодекс Рос. Федерации от 13 июня 1996 г. № 63-ФЗ (в ред. от 9 апр. 2026 г.). Доступ из справ.-правовой системы «КонсультантПлюс».

Научные споры по вопросу выявления и раскрытия экстремистских преступлений в виртуальном мире связаны с определением границ вмешательства государства в цифровую среду, критериев экстремистского контента, соотношения профилактики и репрессии, а также проблемой допустимости цифровых доказательств и обеспечения баланса между безопасностью и правами человека.

Российские и зарубежные ученые по-разному оценивают баланс между обеспечением безопасности и защитой прав человека, а также степень допустимого вмешательства государства в цифровую среду.

Так, например, И.Л. Бачило критиковала тотальный контроль, указывая, что предпринимаемые государством меры должны иметь четкие законодательные границы, в противном случае это приведет к подавлению свобод граждан [8]. Аналогичной позиции, критикующей подобный контроль, придерживается Б. Шнайер, отмечающий, что «массовая слежка – это не компромисс, а потеря свободы» [9].

Вехов В.Б., наоборот, выступает сторонником глубокого цифрового мониторинга, отмечая необходимость осуществления мероприятий в строгом соответствии с нормами законодательства [10]. Керр О. сформулировал четкую позицию: автоматизированный анализ потоков данных допустим всегда, а вот раскрытие личности конкретного пользователя – только после получения санкции суда [11].

Среди множества противоположных мнений срединную (нейтральную) позицию занимает Т.А. Полякова, которая потребность в контроле признает вынужденной необходимостью, однако подчеркивает, что без хорошо проработанной законодательной регламентации правил фиксации цифровых доказательств любой контроль рискует превратиться из следственного действия в инструмент слежки [12].

В результате анализа научных позиций формируется мнение, что выявление и раскрытие экстремистских преступлений с использованием информационно-телекоммуникационных сетей должно основываться на балансе между обеспечением общественной безопасности и соблюдением прав и свобод человека, при обязательном использовании законных, технически обоснованных и процессуально закрепленных методов работы в цифровой среде.

Накопленный к настоящему времени опыт практической деятельности правоохранительных органов в сфере борьбы с экстремистскими преступлениями и теоретические изыскания указывают на то, что для эффективного пресечения фактов их проявления необходимо проведение оперативными подразделениями правоохранительных органов оперативно-розыскных мероприятий [13].

Полномочия по выявлению и пресечению преступлений исследуемой категории возлагаются на правоохранительные органы, деятельность которых традиционно характеризуется определенной степенью консервативности в силу ее специфики и в определенной мере закрытости, применяемых методов, сил и средств. Внедрение новых технологий в этой среде занимает довольно длительное время, поэтому их актуализация является ключевым аспектом в нормализации работы правоохранительных органов [14].

Представляется, что ключевым и необходимым фактором действий государств по контртеррористическому направлению должна являться деятельность оперативных подразделений правоохранительных органов, способных в той же мере, как экстремисты и террористы, активно использовать результаты цифровизации в борьбе с преступностью [15].

В России в соответствии с Указом Президента Российской Федерации от 28 декабря 2024 г. № 1124 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации» одной из задач государственной политики в сфере противодействия экстремизму является повышение эффективности

профилактики, выявления и пресечения преступлений экстремистской направленности[7].

Анализ результатов практической деятельности и регулярно публикуемых сообщений в средствах массовой информации по данной проблематике свидетельствует о модификации экстремизма, произошедшей за последнее десятилетие. Об этом свидетельствует переход экстремизма в цифровую среду, изменение форм вербовки, рост информационных проявлений, а также усложнение правовой квалификации. Социальные сети, компьютерные игры с возможностью мгновенного обмена анонимными сообщениями, технологии DeepFake, VPN, прокси-серверы, форумы DarkNet, мессенджеры с двойным сквозным шифрованием и многое другое – инструменты, которые активно используются радикальными группами, агитирующими отдельных членов общества к насильственным действиям, выступая против сложившихся устоев.

Анализируя статистику совершенных в Российской Федерации преступлений, вынуждены констатировать, что более 40 % из них совершается с применением информационно-телекоммуникационных сетей [16].

Нередкими стали случаи вовлечения в совершение подобного рода преступлений несовершеннолетних или еще не устоявшихся в обществе молодых людей, увлеченных получением заработка за совершение противоправных действий. Так, участились случаи совершения подростками поджогов базовых электростанций, путевых машин, зданий и автомобилей сотрудников правоохранительных органов [17]. Их вовлечение в совершение данных деяний стало возможно, в связи с использованием тех же информационных технологий, поскольку привлечение к совершению преступлений и дистанционное управление их действиями осуществлялось с использованием информационно-телекоммуникационной сети Интернет, распространенных мессенджеров и т.д.

Учитывая обстоятельства современных реалий, рост количества преступлений экстремистской направленности, а также снижение эффективности противодействия им, возникает необходимость детальной проработки оперативного выявления, качественного раскрытия преступлений указанной категории, а также разработки и реализации действенных мер по цифровому противодействию экстремизму.

Нарабатываемый в ходе осуществления практической деятельности механизм работы по выявлению и раскрытию преступлений экстремистской направленности, совершенных с использованием информационно-телекоммуникационных сетей, направлен на наиболее эффективное решение ряда задач, таких как пресечение вовлечения лиц в преступные действия, предотвращение совершения насилия, обеспечение безопасного информационного пространства, перекрытие финансовых потоков, питающих экстремизм [18].

Осуществление любой деятельности, в том числе преступной, невозможно без финансирования. В связи с этим представляется необходимым усовершенствовать работу по выявлению использования криптовалюты, электронных кошельков, краудфандинга для финансирования экстремистской деятельности, что приведет к своевременному перекрытию, истощению финансовых потоков экстремистских организаций.

В ходе выявления и последующего пресечения экстремистской деятельности целесообразно устанавливать схемы движения денежных средств лиц, причастных к совершению преступлений, каналы их поступления и способы распоряжения финансами. Важно установить конечных бенефициаров в получении нелегальных доходов от экстремистской и террористической деятельности, определить их долю дохода, место нахождения денежных средств и активов данных лиц.

[7] Об утверждении Стратегии противодействия экстремизму в Российской Федерации: Указ Президента Рос. Федерации от 28 дек. 2024 г. № 1124. Доступ из справ.-правовой системы «КонсультантПлюс».

Для демонстрации актуальности работы по блокированию финансирования экстремизма приведем статистические данные Росфинмониторинга за 2025 г.: в перечень физических и юридических лиц, внесенных в список причастных к терроризму и экстремизму, попало более 3,8 тыс. человек (свыше 2,6 тыс. подозреваемых в организации террористической деятельности и более 1,1 тыс. – в экстремистской) и свыше 190 организаций, что существенно превышает показатели аналогичных периодов прошлых лет (в 2020 г. более 3,2 тыс. граждан и свыше 40 организаций). Таким образом, количество новых субъектов ежегодно растет в сотни раз[8].

Работа в данном направлении подразумевает выявление лиц, выполняющих агитацию и вербовку в цифровом мире. Основным объектом информационного вовлечения в экстремизм выступает молодежь, зависимая от цифрового пространства и нацеленная на получение признания общества, заработка любым путем. Учитывая, что виртуальное пространство является главным плацдармом для вербовки, то своевременное ограничение доступа к этому пространству, путем блокировки или ограничения доступа, приведет к обеспечению безопасного информационного пространства и предотвращению насилия [19]. В связи с этим представляется необходимым рассмотреть вопрос о внедрении и развитии технологий фильтрации содержимого сети Интернет по аналогии с «Золотым щитом», представляющим систему интернет-цензуры и наблюдения в Китае.

В кризисных ситуациях безопасность информационного пространства может играть далеко не последнюю роль. Экстремизм, пропагандирующийся в информационно-телекоммуникационных сетях, деструктивно влияет на сознание людей. Благодаря информационно-телекоммуникационной сети Интернет радикальные группы могут беспрепятственно транслировать свои идеи неограниченному кругу лиц, тем самым дестабилизировать жизнь общества и государства. Предотвратить или, по крайней мере, минимизировать риск дестабилизации возможно путем своевременного обнаружения размещенных материалов.

Важным аспектом в выявлении преступлений экстремистской направленности является работа с сознательностью населения. Обществу необходимо транслировать разъяснительный контент о деятельности субъектов противодействия экстремизму, о трагических последствиях совершения исследуемых преступлений для формирования в обществе нетерпимого отношения к проявлениям экстремизма и терроризма, фактах привлечения лиц к ответственности за совершение с помощью электронных или информационно-телекоммуникационных сетей экстремистских преступлений с целью демонстрации правовой силы и неотвратимости наказания, развеивания иллюзий о возможности совершения преступлений анонимно [20].

Вместе с тем нельзя не отметить, что анонимный характер распространения экстремистских материалов, так же как и получение к ним доступа неограниченного круга лиц по всему миру, значительно затрудняет процесс раскрытия преступлений экстремистской направленности и фиксации цифровых следов.

Противодействие экстремизму, совершаемому в информационно-телекоммуникационной сети, включая сеть Интернет, требует соблюдения баланса между обеспечением безопасности государства и его граждан и соблюдением конституционных прав последних на свободу слова и тайну переписки. Поэтому сбор доказательств в информационной сфере имеет решающее значение для дальнейшей судебной перспективы уголовных дел [21].

Раскрытие совершенного преступления – это работа с последствиями. Правильная интерпретация и использование анализа уже имеющихся последствий служат основой для формирования стабильного, действенного алгоритма действий и практики расследования уголовных дел с судебной перспективой.

[8] Федеральная служба по финансовому мониторингу. URL: https://www.fedsfm.ru/ (дата обращения: 10.03.2026).

Для повышения качества работы оперативных подразделений правоохранительных органов по борьбе с преступлениями экстремистской направленности целесообразно применять современные информационные технологии. С использованием нейронных систем и комбинированных действий Timing поиск необходимой информации, производство анализа данных позволят минимизировать затраченное время, эффективно справиться с обнаружением экстремистской активности в информационной сети. Также необходимо координировать работу технологии искусственного интеллекта с учетом материалов ранее выявленных и раскрытых преступлений. Помимо обнаружения значимой информации (паролей, сайтов, log-файлов, метаданных, сведений оперативной памяти и т.п.), следует разработать алгоритм их фиксации.

Осуществление мониторинга интернет-пространства на непрерывной основе позволит достичь положительных результатов в подрыве экстремистской деятельности. В случае обнаружения запрещенной информации, должна следовать незамедлительная блокировка сайта, при установлении лиц, распространяющих подобную информацию, необходимо привлекать их к административной или уголовной ответственности в соответствии с действующим законодательством.

Для достижения наибольшей эффективности в деятельности по пресечению преступлений экстремистской направленности, совершенных с использованием информационного пространства, важно комплексно усовершенствовать действующее законодательство путем внесения поправок, направленных на более тщательную проверку и блокировку интернет-сайтов, содержащих информацию экстремистской направленности; ужесточение ответственности за преступления и правонарушения, связанные с распространением экстремистских и иных запрещенных материалов; осуществлять постоянный мониторинг интернет-пространства подразделениями по борьбе с преступлениями экстремистской направленности, с целью выявления действующих экстремистских организаций и/или отдельных лиц, пропагандирующих насилие.

Таким образом, в настоящее время экстремизм, представляющий опасность для конституционного и общественного строя, является одной из наиболее актуальных угроз мирового общества.

При выявлении и раскрытии экстремистских преступлений, совершаемых с использованием информационно-телекоммуникационных сетей, должен поддерживаться баланс между обеспечением общественной безопасности и соблюдением прав и свобод человека при использовании законных и современных методов работы в цифровой среде.

В современных условиях деятельность сотрудников правоохранительных органов Российской Федерации по выявлению и пресечению преступлений исследуемой категории имеет потенциал повышения своей результативности.

Ввиду развития преступности меры по противодействию экстремизму должны постоянно совершенствоваться, иметь комплексный, регулярный и наступательный характер. Эффективность проводимых оперативных мероприятий зависит от надлежащего уровня знаний оперативников и технической оснащенности оперативных подразделений по борьбе с преступлениями экстремистской направленности.

Выявление и раскрытие преступлений экстремистской направленности в информационном пространстве – это важная задача, способная сохранить социальную стабильность, что подчеркивает актуальность исследования вопросов повышения результативности ее решения. Значение выявления и раскрытия преступлений данной категории выходит далеко за рамки классической правоохранительной деятельности. Эффективность этой работы напрямую зависит от внедрения инновационных методов анализа и укрепления взаимодействия между государством и IT-сектором.

Список источников

1. Бычков В.В., Харченко С.В. К истории организационно-структурного обеспечения расследования преступлений экстремистской направленности // Создание и развитие модели органов предварительного расследования в Российской империи: материалы Всерос. науч.-практ. конф., посвящ. 160-летию учреждения должности судебного следователя и памяти выдающегося историка российской юриспруденции Дмитрия Олеговича Серова / под общ. ред. Д.Н. Кожухарика. М., 2020. С. 30–36.

2. Schmid A.P. The Routledge Handbook of Terrorism Research. London: Routledge, 2011. 718 p.

3. Mudde C. On Extremism and Democracy in Europe. London: Routledge, 2016. 196 p.

4. Coleman P.T. The Five Percent: Finding Solutions to Seemingly Impossible Conflicts. New York: PublicAffairs, 2011. 432 p.

5. Sedgwick M. Key Thinkers of the Radical Right: Behind the New Threat to Liberal Democracy. New York: Oxford University Press, 2019. 376 p.

6. Авдеев В.А., Авдеева О.А. Противодействие преступлениям экстремистской направленности в цифровом пространстве: новые вызовы и правовые решения // Российский судья. 2023. № 8. С. 22–27.

7. Гирько С.И., Харченко С.В., Бычков В.В. Некоторые вопросы деятельности правоохранительных органов в сфере противодействия информационной активности участников террористических и экстремистских действий // Военное право. 2021. № 3(67). С. 9–16.

8. Бачило И.Л. Информационное право. М.: Юрайт, 2011. 512 с.

9. Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company, 2015. 320 p.

10. Вехов В.Б. Основы оперативно-разыскной деятельности. Волгоград: ВА МВД России, 2016. 240 с.

11. Kerr O. Computer Crime Law. St. Paul: Thomson Reuters, 2019. P. 120–124.

12. Полякова Т.А. Проблемы правового регулирования электронных доказательств. М.: ИГП РАН, 2017. 180 с.

13. Бычков В.В., Харченко С.В. О некоторых проблемах использования результатов оперативно-розыскной деятельности в раскрытии и расследовании преступлений экстремистской направленности // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования. 2020. Т. 1. № 1(2). С. 49–57.

14. Бычков В.В., Харченко С.В. Понятие и формы использования специальных знаний при выявлении противодействия расследованию преступлений экстремистской направленности // Раскрытие и расследование преступлений: наука, практика, опыт: сб. науч. трудов. Тула: Изд-во ТулГУ, 2020. Ч. 2. С. 9–14.

15. Григорьев Д.А. Алгоритмизация поиска экстремистского контента с использованием нейросетевых технологий в 2024–2025 гг. // Право и цифровая экономика. 2025. № 2. С. 12–19.

16. Иванцов С.В. Криминологические показатели экстремизма в цифровой среде: тенденции 2024–2026 годов // Российский следователь. 2026. № 2. С. 55–61.

17. Харченко С.В. О факторах, влияющих на организацию оперативно-розыскной деятельности органов внутренних дел по борьбе с криминальным автобизнесом // Право и государство: теория и практика. 2015. № 4(124). С. 133–136.

18. Волеводз А.Г. Противодействие использованию информационно-телекоммуникационных сетей в экстремистских целях: международный, национальный аспекты // Международное право. 2023. № 4. С. 102–115.

19. Бахта А.С. Особенности раскрытия преступлений, совершенных с использованием ИТ-технологий: современные вызовы // Вестник криминалистики. 2024. Т. 12. № 1. С. 18–25.

20. Карпов Н.С. Методика раскрытия преступлений экстремистского характера, совершенных с применением средств анонимизации // Труды Академии управления МВД России. 2024. № 3(71). С. 88–96.

21. Оганесян С.С. Интернет и религиозный экстремизм // Уголовно-исполнительная система: право, экономика, управление. 2022. № 2. С. 32–36.

References

1. Bychkov V.V., Harchenko S.V. K istorii organizacionno-strukturnogo obespecheniya rassledovaniya prestuplenij ekstremistskoj napravlennosti // Sozdanie i razvitie modeli organov predvaritel'nogo rassledovaniya v Rossijskoj imperii: materialy Vseros. nauch.-prakt. konf., posvyashch. 160-letiyu uchrezhdeniya dolzhnosti sudebnogo sledovatelya i pamyati vydayushchegosya istorika rossijskoj yurisprudencii Dmitriya Olegovicha Serova / pod obshch. red. D.N. Kozhuharika. M., 2020. S. 30–36.

2. Schmid A.P. The Routledge Handbook of Terrorism Research. London: Routledge, 2011. 718 p.

3. Mudde C. On Extremism and Democracy in Europe. London: Routledge, 2016. 196 p.

4. Coleman P.T. The Five Percent: Finding Solutions to Seemingly Impossible Conflicts. New York: PublicAffairs, 2011. 432 p.

5. Sedgwick M. Key Thinkers of the Radical Right: Behind the New Threat to Liberal Democracy. New York: Oxford University Press, 2019. 376 p.

6. Avdeev V.A., Avdeeva O.A. Protivodejstvie prestupleniyam ekstremistskoj napravlennosti v cifrovom prostranstve: novye vyzovy i pravovye resheniya // Rossijskij sud'ya. 2023. № 8. S. 22–27.

7. Gir'ko S.I., Harchenko S.V., Bychkov V.V. Nekotorye voprosy deyatel'nosti pravoohranitel'nyh organov v sfere protivodejstviya informacionnoj aktivnosti uchastnikov terroristicheskih i ekstremistskih dejstvij // Voennoe pravo. 2021. № 3(67). S. 9–16.

8. Bachilo I.L. Informacionnoe pravo. M.: Yurajt, 2011. 512 s.

9. Schneier B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company, 2015. 320 p.

10. Vekhov V.B. Osnovy operativno-razysknoj deyatel'nosti. Volgograd: VA MVD Rossii, 2016. 240 s.

11. Kerr O. Computer Crime Law. St. Paul: Thomson Reuters, 2019. P. 120–124.

12. Polyakova T.A. Problemy pravovogo regulirovaniya elektronnyh dokazatel'stv. M.: IGP RAN, 2017. 180 s.

13. Bychkov V.V., Harchenko S.V. O nekotoryh problemah ispol'zovaniya rezul'tatov operativno-rozysknoj deyatel'nosti v raskrytii i rassledovanii prestuplenij ekstremistskoj napravlennosti // Sovremennoe ugolovno-processual'noe pravo – uroki istorii i problemy dal'nejshego reformirovaniya. 2020. T. 1. № 1(2). S. 49–57.

14. Bychkov V.V., Harchenko S.V. Ponyatie i formy ispol'zovaniya special'nyh znanij pri vyyavlenii protivodejstviya rassledovaniyu prestuplenij ekstremistskoj napravlennosti // Raskrytie i rassledovanie prestuplenij: nauka, praktika, opyt: sb. nauch. trudov. Tula: Izd-vo TulGU, 2020. Ch. 2. S. 9–14.

15. Grigor'ev D.A. Algoritmizaciya poiska ekstremistskogo kontenta s ispol'zovaniem nejrosetevyh tekhnologij v 2024–2025 gg. // Pravo i cifrovaya ekonomika. 2025. № 2. S. 12–19.

16. Ivancov S.V. Kriminologicheskie pokazateli ekstremizma v cifrovoj srede: tendencii 2024–2026 godov // Rossijskij sledovatel'. 2026. № 2. S. 55–61.

17. Harchenko S.V. O faktorah, vliyayushchih na organizaciyu operativno-rozysknoj deyatel'nosti organov vnutrennih del po bor'be s kriminal'nym avtobiznesom // Pravo i gosudarstvo: teoriya i praktika. 2015. № 4(124). S. 133–136.

18. Volevodz A.G. Protivodejstvie ispol'zovaniyu informacionno-telekommunikacionnyh setej v ekstremistskih celyah: mezhdunarodnyj, nacional'nyj aspekty // Mezhdunarodnoe pravo. 2023. № 4. S. 102–115.

19. Bahta A.S. Osobennosti raskrytiya prestuplenij, sovershennyh s ispol'zovaniem IT-tekhnologij: sovremennye vyzovy // Vestnik kriminalistiki. 2024. T. 12. № 1. S. 18–25.

20. Karpov N.S. Metodika raskrytiya prestuplenij ekstremistskogo haraktera, sovershennyh s primeneniem sredstv anonimizacii // Trudy Akademii upravleniya MVD Rossii. 2024. № 3(71). S. 88–96.

21. Oganesyan S.S. Internet i religioznyj ekstremizm // Ugolovno-ispolnitel'naya sistema: pravo, ekonomika, upravlenie. 2022. № 2. S. 32–36.

Статья поступила в редакцию 17.05.2026; одобрена после рецензирования 25.05.2026; принята к публикации 26.05.2026.
The article was submitted 17.05.2026; approved after reviewing 25.05.2026; accepted for publication 26.05.2026.

Информация об авторе
Е.А. Мишкичева – следователь первого контрольно-следственного отдела следственного управления Следственного комитета Российской Федерации по Ставропольскому краю (Россия, 355005, г. Ставрополь, ул. Абрамовой, 2).

Information about the author
E.A. Mishkicheva – investigator of the first control and investigative Department of the Investigative Department of the Investigative Committee of the Russian Federation for the Stavropol Territory (Russia, 355005, Stavropol, Abramova str., 2).