Научная статья
УДК 343.85:343.326:004.738.5
https://doi.org/10.33874/2072-9936-2025-0-3-124–141

ОПЕРАТИВНО-РАЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ ОВД В БОРЬБЕ С ЭКСТРЕМИЗМОМ В СЕТИ ИНТЕРНЕТ: ОРГАНИЗАЦИОННО-УПРАВЛЕНЧЕСКИЕ, ПРАВОВЫЕ И ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ

Владимир Владимирович Баранов[1]

Вадим Михайлович Пашин[2]

[1] Академия управления МВД России, 125993, Россия, г. Москва, ул. 3ои и Александра Космодемьянских, д. 8

[2] Всероссийский государственный университет юстиции (РПА Минюста России), 117638, Россия, г. Москва, ул. Азовская, д. 2, корп. 1

[1] de_la_sergio@mail.ru

[2] paschin@mail.ru

Аннотация

Актуальность обусловлена активизацией экстремистской деятельности в сети Интернет и ее растущей угрозой для безопасности общества. Оперативно-разыскная деятельность органов внутренних дел в сфере противодействия интернет-экстремизму сталкивается с комплексом проблем, требующих системного анализа и разработки мер по их преодолению. Цель исследования – выявление организационно-управленческих, правовых и технологических проблем оперативно-разыскной деятельности ОВД в контексте борьбы с экстремизмом в сети Интернет, а также разработка предложений по их преодолению. В работе использованы методы анализа и синтеза, сравнительно-правовой анализ, эмпирическое исследование практики правоохранительных органов и анализ нормативно-правовых актов. Предложены конкретные рекомендации по совершенствованию организационно-управленческих механизмов, правовой инфраструктуры и технологического компонента. Сформулирован вывод о необходимости интеграции новых технологий, улучшения координации с международными партнерами и совершенствования образовательных программ для сотрудников правоохранительных органов.

Ключевые слова: экстремизм; Интернет; оперативно-разыскная деятельность; органы внутренних дел; мониторинг; искусственный интеллект; правовое регулирование; информационная безопасность.

Для цитирования: *Баранов В. В., Пашин В.М.* Оперативно-разыскная деятельность ОВД в борьбе с экстремизмом в сети Интернет: организационно-управленческие, правовые и технологические аспекты // Вестник Российской правовой академии. 2025. № 3. С. 124–141. https://doi.org/10.33874/2072-9936-2025-0-3-124-141

Research Article

OPERATIONAL SEARCH ACTIVITIES OF THE DEPARTMENT OF INTERNAL AFFAIRS IN THE FIGHT AGAINST EXTREMISM ON THE INTERNET: ORGANIZATIONAL, MANAGERIAL, LEGAL AND TECHNOLOGICAL ASPECTS

Vladimir V. Baranov[1]

Vadim M. Pashin[2]

[1] Academy of the Ministry of Internal Affairs of Russia, 8 Zoya and Alexander Kosmodemianskikh St., Moscow, 125993, Russia

[2] All-Russian State University of Justice, 2, Bldg. 1 Azovskaia St., Moscow, 117638, Russia

[1] de_la_sergio@mail.ru

[2] paschin@mail.ru

Abstract

The relevance is due to the increased extremist activity on the Internet and its growing threat to the security of society. The operational investigative activities of the Department of Internal Affairs in the field of countering Internet extremism face a set of problems that require a systematic analysis and the development of measures to overcome them. The aim is to identify organizational, managerial, legal and technological problems of the Department of Internal Affairs in the context of combating extremism on the Internet, and to develop proposals to overcome them. The methods of analysis and synthesis, comparative legal analysis, empirical research of law enforcement practice, and analysis of regulatory legal acts were used. Specific recommendations are proposed for improving organizational and managerial mechanisms, legal infrastructure, and the technological component. The conclusion is formulated that it is necessary to

integrate new technologies, improve coordination with international partners, and improve educational programs for employees of law enforcement agencies.

Keywords: extremism; Internet; operational and investigative activities; internal affairs bodies; monitoring; artificial intelligence; legal regulation; information security.

For citation: *Baranov V. V., Pashin V. M.* Operational Search Activities of the Department of Internal Affairs in the Fight Against Extremism on the Internet: Organizational, Managerial, Legal and Technological Aspects. *Herald of the Russian Law Academy*, 2025, no. 3, pp. 124–141. (In Russ.) https://doi.org/10.33874/2072-9936-2025-0-3-124-141

Введение

В последние годы экстремизм в сети Интернет стал не только деструктивным фактором онлайн-среды, но и одним из наиболее серьезных вызовов для безопасности и стабильности общества в целом, поскольку деструктивные идеи, возникающие при цифровом взаимодействии, нередко выходят за рамки цифровых платформ [1, с. 30–36]. В России последних лет зафиксирован рекордный рост числа зарегистрированных преступлений экстремистской направленности.

Согласно данным Генпрокуратуры в 2022 г. было зафиксировано 1566 таких преступлений, что на 48,2% превышает показатели 2021 г. и является наивысшим значением за пять лет; в 2023 г. данный показатель, хотя и несколько снизился – до 1340, представляет не менее острую проблему [2]. Основная часть этих деяний – призывы к насилию и распространение идеологий ненависти, особенно после начала специальной военной операции России на территории Украины, – совершается через Интернет. В контексте противодействия главную роль играют правоохранительные органы, органы внутренних дел (ОВД), которые осуществляют работу по выявлению и пресечению онлайн-преступлений.

В 2020 г. из 833 преступлений экстремистской направленности 500 были раскрыты сотрудниками МВД [3]. Однако рост числа дел свидетельствует не только об усилении активности экстремистов, но и о совершенствовании механизмов их обнаружения. В связи с этим целью данного исследования является анализ оперативно-разыскной деятельности (ОРД) органов внутренних дел в контексте борьбы с экстремизмом в сети Интернет, выявление организационно-управленческих, правовых и технологических проблем, а также предложений по их преодолению.

Для достижения этой цели поставлены следующие задачи:

– рассмотреть особенности взаимодействия различных государственных структур в борьбе с интернет-экстремизмом;

– проанализировать правовую базу, регулирующую оперативно-разыскную деятельность в данной области;

– оценить используемые технологии в мониторинге и пресечении экстремистской деятельности в Интернете;

– определить перспективы развития этой деятельности в условиях глобальных вызовов.

1. Организационно-управленческие аспекты оперативно-разыскной деятельности

В самом начале нашего исследования нами были определены организационно-управленческие аспекты ОРД ОВД в борьбе с экстремизмом в сети Интернет. В общем случае под оперативно-разыскной деятельностью понимается система мероприятий, направленных на выявление, предупреждение и пресечение преступлений, сбор доказательств для их расследования и предоставление материалов для судебного разбирательства [4, с. 33–37]. По мнению Н. В. Дудулиной, важной характеристикой такой системы является ее «юридическая», или регламентированная законом ориентация – иначе говоря, деятельность специальных уполномоченных органов в рамках «специального законодательства» [5, с. 54]. В отношении феномена интернет-экстремизма ОРД включает в себя действия правоохранительных органов по выявлению и пресечению преступных действий в сети, среди которых можно выделить распространение экстремистских материалов, участие в террористических организациях и другие формы деструктивной деятельности.

Экстремизм в Интернете в свою очередь включает в себя любые формы идеологической деятельности, направленные на подрыв существующего общественного порядка, нарушение прав и свобод граждан, создание угроз национальной безопасности посредством распространения информации, материалов и идей через интернет-ресурсы.

В последние десятилетия ОРД ОВД в России претерпела значительные изменения, связанные с развитием цифровых технологий [6, с. 154–163]. Проблемы экстремизма в сети Интернет требуют от правоохранительных органов применения новых подходов и методов работы, что влияет на организационную структуру и внутреннюю координацию в системе ОВД. В частности, при Главном управлении по противодействию экстремизму (ГУПЭ) МВД России и Центре по противодействию экстремизму (ЦПЭ) созданы специализированные подразделения для мониторинга и борьбы с экстремизмом в сети Интернет, где используются различные аналитические системы онлайн-дозора (Крибрум, система «Онлайн-дозор») и др.

Эти подразделения обеспечивают координацию взаимодействия между различными оперативными подразделениями органов внутренних дел и ведомствами, включая ФСБ России, Роскомнадзор и другие государственные органы.

Роль ОВД в контексте борьбы с экстремизмом заключается не только в выявлении и расследовании фактов экстремистской деятельности, но и в организации профилактической работы, направленной на предотвращение распространения радикальных идей в глобальной сети Интернет.

В компетенцию органов внутренних дел на любом уровне входит взаимодействие с населением, организация просветительской деятельности и работа с подрастающим поколением.

Для результативной нейтрализации экстремистской активности в онлайн-пространстве необходимо слаженное взаимодействие между различными отделами ОВД и другими государственными ведомствами, включая ФСБ России, прокуратуру и суды. В частности, оперативные сотрудники, следственные органы и аналитики должны объединять усилия для проведения всестороннего анализа и определения индикаторов экстремистской деятельности. Помимо этого координация

усилий важна и на международном уровне посредством сотрудничества с правоохранительными органами зарубежных государств, учитывая транснациональную природу экстремистских материалов.

В качестве примера эффективного взаимодействия можно привести практику блокировки сайтов экстремистской направленности, осуществляемую Роскомнадзором. Данное ведомство тесно сотрудничает с Министерством внутренних дел РФ для быстрого реагирования на возникающие риски в онлайн-среде. Важно подчеркнуть, что трудности в координации нередко обусловлены расхождениями в стратегиях и недостаточным объемом информации, которой располагают различные государственные органы, что способно замедлять процесс реагирования на потенциальные опасности.

Особое значение в борьбе с интернет-экстремизмом имеет взаимодействие правоохранительных органов с различными частными компаниями, занимающимися информационной безопасностью и предоставлением интернет-услуг [7, с. 77–82]. Компании, управляющие крупными интернет-платформами – например, социальными сетями, поисковыми системами, хостинг-платформами и интернет-магазинами, – играют важную роль в мониторинге экстремистского контента, поскольку в некоторых случаях они сотрудничают с правоохранительными органами, предоставляя данные о нарушителях с целью предотвращения распространения экстремистских материалов. Тем не менее на текущем этапе развития правоохранительной системы в РФ это взаимодействие является фрагментарным и не представляет собой закономерного тренда.

Нам представляется важным осветить вопрос наличия специфических проблем в организации взаимодействия между государственными органами.

Одной из основных проблем является отсутствие четкой регламентации в вопросах оперативного взаимодействия различных структур, что приводит к избыточной бюрократии и задержкам в принятии решений. Еще одной проблемой является нехватка профессионалов, способных эффективно работать в сфере кибербезопасности и борьбы с экстремизмом в Интернете. По критическому замечанию И. Н. Архипцева, «современная картина проблем в области противодействия киберпреступлениям свидетельствует об острой необходимости «выращивания» в правоохранительных органах грамотных специалистов в сфере высоких технологий» [6, с. 156], в связи с чем представляется необходимым повышать квалификацию сотрудников правоохранительных органов в сфере цифровых технологий и анализа данных для эффективной борьбы с онлайн-угрозами.

Для повышения результативности деятельности ОВД в противодействии экстремистской активности в интернет-пространстве целесообразно реализовать комплекс мер, включающий:

– формирование унифицированной базы данных, доступной для всех правоохранительных структур, что обеспечит своевременный обмен сведениями об обнаруженных рисках и опасностях;

– активизацию взаимодействия с коммерческими *IT*-организациями и специалистами по кибербезопасности с целью разработки и внедрения современных средств контроля и анализа сетевой активности;

– совершенствование профессиональной подготовки и повышение квалификации сотрудников ОВД в сфере обработки цифровой информации и расследования преступлений, совершаемых с использованием информационных технологий.

2. Правовые аспекты оперативно-разыскной деятельности ОВД

Переходя к вопросу правовых аспектов ОРД ОВД в борьбе с экстремизмом в интернет-пространстве, прежде всего еще раз отметим, что экстремизм в сети включает в себя самые разнообразные формы преступной деятельности. Он является многовидовым: распространение экстремистских материалов, призывы к насилию, вербовка в террористические организации и прочие действия, направленные на разжигание социальной ненависти и вражды.

С точки зрения российского законодательства экстремизм включает в себя действия, описанные в ст. 280 «Публичные призывы к осуществлению экстремистской деятельности», ст. 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства» и в ст. 205.2 «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма» УК РФ [8]. Анализ статистических данных правоохранительных органов позволяет оценить динамику выявления и расследования преступлений, совершенных с использованием информационно-телекоммуникационных технологий в России за период 2019–2024 гг. [9].

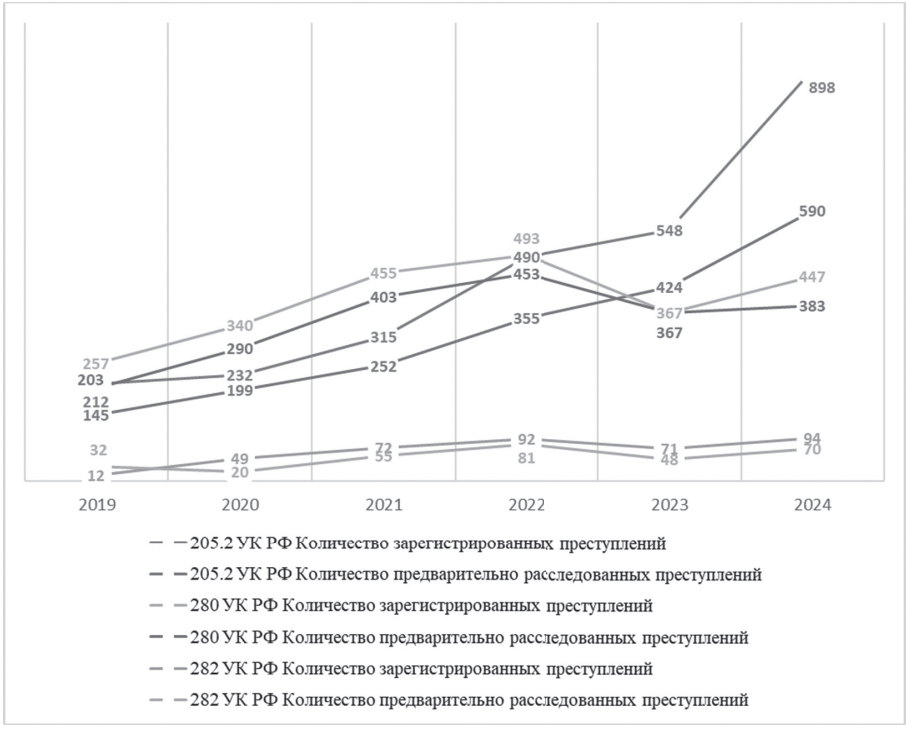

Рис. 1. Количество зарегистрированных и предварительно расследованных преступлений, совершенных с использованием ИТТ в целом по России за 2019–2024 гг.

Значительную часть работы ОВД составляет мониторинг интернет-пространства для выявления и пресечения экстремистских действий [10, с. 319–322].

Важно, что современные технологии позволяют быстро распространять и скрывать экстремистские материалы, что создает дополнительные трудности для правозащитников и правоохранительных органов. В таких условиях стремительного развития цифровых технологий и расширения интернет-пространства международное сообщество осознало необходимость создания цельной правовой базы и регламентации в ее рамках механизмов по борьбе с экстремизмом в сети.

Важнейшим актом международного формата в этой области стал документ о борьбе с терроризмом, принятый ООН в 2006 г. [11], который направлен на пресечение террористической деятельности, в том числе ее пропаганды через Интернет. Государства-участники обязуются принимать законодательные и практические меры для выявления, предотвращения и пресечения распространения экстремистских идей в цифровой среде.

В свою очередь, в рекомендации Европейской комиссии 2018/334 от 1 марта 2018 г. о мерах по эффективной борьбе с нелегальным онлайн-контентом [12] подчеркивается, что необходимо ввести определенные меры по контролю за интернет-платформами и обязать их к проактивному мониторингу пользовательского контента; в ее рамках также предложены принципы, направленные на баланс между свободой слова и необходимостью защиты общества от экстремизма. Среди них прозрачность модерации контента, обязательства платформ по удалению запрещенного материала и создание механизмов общественного контроля за деятельностью цифровых сервисов.

Российская Федерация, вбирая правовые регламентации международного уровня, уделяет значительное внимание обеспечению национальной безопасности в киберпространстве. Борьба с экстремистским контентом в Интернете регулируется рядом законодательных актов, обеспечивающих защиту граждан от деструктивного влияния цифровой информации [13]. Так, Конституция РФ 1993 г. закрепляет принципы защиты прав граждан, включая информационную безопасность.

В рамках борьбы с экстремизмом государство имеет право вводить ограничения на распространение информации, угрожающей основам конституционного строя и безопасности страны.

Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [14] включает запрет на распространение среди несовершеннолетних сведений, содержащих сцены насилия, пропаганду экстремистской деятельности и терроризма. В Интернете создаются системы возрастных ограничений и механизмы блокировки вредоносного контента.

Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»» прямо запрещает распространение в Интернете информации, содержащей пропаганду экстремистской и террористической деятельности [15]. В частности, он предусматривает:

– запрет на материалы, призывающие к экстремистской или террористической деятельности, включая тексты, изображения, видео и аудиозаписи;

– ограничение доступа к сайтам, распространяющим экстремистскую идеологию, в том числе пропагандирующим насилие, национальную или религиозную вражду;

– обязанность интернет-провайдеров и владельцев сайтов блокировать подобный контент после получения уведомления от Роскомнадзора или других уполномоченных органов;

– возможность внесудебной блокировки ресурсов, содержащих призывы к терроризму и экстремизму, по требованию Генеральной прокуратуры.

Эти меры направлены на предотвращение распространения радикальных взглядов и защиту детей от вредоносной информации.

Порядок ограничения доступа к интернет-ресурсу, содержащему информацию, распространение которой запрещено на территории Российской Федерации, определен ч. 1 ст. 15.3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в целях ограничения доступа к сайтам в сети Интернет [16].

На сегодняшний день в России создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (далее – Единый реестр, eais.rkn.gov.ru). Органы власти имеют право оперативно вносить сайты в реестр запрещенных, а интернет-провайдеры обязаны обеспечивать их недоступность для пользователей. Ниже, к примеру, представлены данные о количестве сайтов в Едином реестре по ведомствам на 1 марта 2025 г. (Рис. 2) [17].

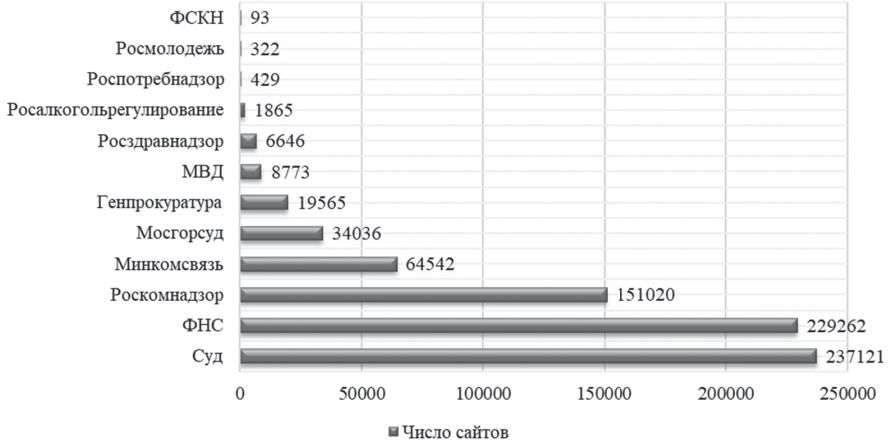

Рис. 2. Результаты внесения сайтов в Единый реестр по ведомствам на 1 марта 2025 г.

Наибольшее количество сайтов в Единый реестр внесено по решениям судебных органов – 237 121, что составляет примерно 31% от общего числа. На втором

месте находится ФНС России с 229 262 сайтами (около 30%). Роскомнадзор замыкает тройку лидеров с 151 020 сайтами (около 20%). Всего в реестре находится более 750 тыс. сайтов, что демонстрирует масштабность системы контроля за информацией в российском сегменте сети Интернет.

Кроме того, Роскомнадзор разработал инструкцию, регламентирующую порядок действий при обнаружении в Интернете материалов, содержащих запрещенную информацию. В ней описаны критерии, по которым оцениваются признаки экстремистского, террористического и иного запрещенного контента, а также алгоритм взаимодействия с уполномоченными органами. Документ предназначен для граждан, организаций и провайдеров, помогая определить последовательность шагов: фиксацию нарушения, обращение в компетентные органы и возможные меры по ограничению доступа к таким материалам [18].

Основными правовыми инструментами, которые ОВД используют для борьбы с экстремизмом в сети на сегодняшний день, являются [19]: блокировка экстремистских сайтов, привлечение к ответственности лиц, распространяющих экстремистские материалы, а также конфискация материалов, которые могут быть использованы для экстремистской деятельности. Важным элементом правового противодействия является взаимодействие с Роскомнадзором, который осуществляет блокировку доступа к интернет-ресурсам, признанным экстремистскими.

Уголовный кодекс РФ 1996 г. предусматривает ответственность за распространение экстремистского контента в сети [20, с. 26–35]. В частности, ст. 280.1 касается призывов к экстремистской деятельности через Интернет, за что предусмотрено наказание вплоть до лишения свободы [8]. Статья 205.2 устанавливает ответственность за пропаганду терроризма, публикацию материалов, оправдывающих насильственные действия, что влечет уголовную ответственность и серьезные санкции.

Российское законодательство в сфере борьбы с экстремизмом в Интернете развивается в последние десятилетия. Одним из первых законов в данном направлении является Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» [21]. В этом Законе определяются основные механизмы и меры противодействия экстремизму, включая блокировку интернет-ресурсов, содержащих экстремистские материалы. Законодательство также регулирует права и обязанности организаций, предоставляющих доступ к интернет-ресурсам, и устанавливает ответственность за распространение экстремистских материалов.

Примечательно, что совсем недавно был утвержден указ Президента РФ от 28 декабря 2024 г. № 1124, который устанавливает меры по противодействию экстремизму в информационной среде, включая мониторинг интернет-ресурсов, выявление и удаление экстремистского контента, а также сотрудничество государства с интернет-компаниями для обеспечения безопасности пользователей [22].

Также кратко отметим некоторые из последних нововведений, принятых в 2022–2025 гг.:

1) Федеральным законом от 14 июля 2022 г. № 303-ФЗ скорректированы положения ст. 265.10 Кодекса административного судопроизводства РФ, а также ст. 13

и 15 Федерального закона «О противодействии экстремистской деятельности» [23]. Данный законодательный акт устанавливает правила определения информационных материалов как экстремистских;

2) Федеральный закон № 32-ФЗ, принятый 4 марта 2022 г., установил уголовную ответственность за действия, подрывающие авторитет Вооруженных Сил РФ, распространение недостоверных сведений об их применении, а также за призывы к санкциям против России [24];

3) Федеральным законом от 13 июня 2023 г. № 231-ФЗ внесены поправки в ст. 20.29 КоАП РФ, определяющие ответственность за массовое распространение (производство или хранение в целях массового распространения) материалов, входящих в федеральный перечень экстремистских [25];

4) Федеральный закон от 28 февраля 2025 г. № 15-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» нацелен на предотвращение финансирования экстремистской деятельности и вступает в законную силу с 1 июня 2025 г. [26].

Ключевой проблемой в существующем законодательстве является нахождение компромисса между потребностью в обеспечении безопасности общества от экстремистских угроз и гарантией гражданских прав и свобод.

Вопросы, касающиеся цензурирования информации, уважения свободы выражения мнения и защиты личных данных, приобретают первостепенное значение при разработке нормативно-правовой базы в данной области.

Представляется, что для повышения эффективности борьбы с экстремизмом в Интернете следует работать в трех направлениях:

1) разработать дополнительные механизмы мониторинга и идентификации экстремистской деятельности (например, системы раннего обнаружения, способные анализировать социальные связи);

2) усовершенствовать законодательство в области защиты данных и свободы слова в Интернете, создавая при этом правовые гарантии от чрезмерной цензуры; например, в текущих условиях репост новости о митинге может трактоваться как экстремизм или административное правонарушение – это создает правовую неопределенность и затрудняет прогнозирование рисков для пользователей;

3) установить четкие правила взаимодействия с международными организациями для борьбы с транснациональным экстремизмом (учитывая стратегическую переориентацию России на Восток в 2020-х гг., целесообразным может являться обращение к опыту КНР).

3. Технологические аспекты оперативно-разыскной деятельности ОВД

В заключение рассмотрим вопрос определения технологических и методических особенностей осуществления оперативно-разыскных мероприятий органами внутренних дел при противодействии экстремистской деятельности в глобальной сети Интернет.

Одним из центральных элементов эффективной борьбы с интернет-экстремизмом является разработка и внедрение стратегий и технологий, направленных на профилактику и пресечение экстремистской деятельности [19, с. 150–156].

Важнейшим стратегическим подходом, который следует отметить, является мониторинг и анализ сети – ранее мы фрагментарно затрагивали их специфику, однако она нуждается в более подробном освещении [10].

Органы внутренних дел Российской Федерации и другие правоохранительные органы систематически отслеживают онлайн-платформы для быстрого обнаружения контента, включающего экстремистские воззвания или агитацию насилия. С этой целью применяются специализированные программные инструменты и алгоритмы, способные автоматически идентифицировать подобные материалы по заданным ключевым словам, визуальным элементам и видеоматериалам.

С точки зрения понятийного аппарата *мониторинг сети Интернет* – это процесс сбора, анализа и оценки информации, размещенной или передаваемой через Интернет, с целью выявления определенных угроз, в том числе экстремистской деятельности, распространения незаконного контента или иной вредоносной информации. Этот процесс является важной частью борьбы с интернет-экстремизмом, терроризмом и другими угрозами в цифровой среде.

Обычно типовыми целями мониторинга сети Интернет на предмет выявления незаконного контента экстремистской направленности являются:

1) *выявление экстремистского контента*. Главной целью мониторинга является обнаружение и анализ материалов, содержащих экстремистскую, террористическую или иным образом опасную информацию. Это могут быть тексты, изображения, видео, сообщения в социальных сетях, форумах, блогах и других ресурсах, на которых распространяются радикальные идеи;

2) *пресечение противоправной деятельности*. Контроль за интернет-ресурсами помогает предотвратить распространение запрещенной информации и деятельность, связанную с насилием, экстремизмом, пропагандой терроризма, а также с вербовкой людей в экстремистские или террористические группировки;

3) *защита информационной безопасности*. Речь идет о выявлении и предотвращении кибератак, фишинга, распространения вредоносных программ, утечек данных и других угроз, которые могут повредить как частным пользователям, так и организациям;

4) *анализ и предсказание угроз*. Прогнозирование потенциальных угроз, например возможности возникновения массовых беспорядков или террористических актов, основанное на активности в Интернете, является важной частью работы правоохранительных органов и спецслужб;

5) *сбор доказательств*. Мониторинг Интернета помогает правоохранительным органам собирать доказательства преступной деятельности, в том числе следы распространения экстремистской пропаганды, террористической деятельности, призывы к насилию и другие противоправные действия.

При этом в ходе проведения мониторинга сотрудниками органов внутренних дел должны быть решены следующие задачи:

1) *идентификация источников экстремистской активности*. Задача мониторинга – найти сайты, форумы, аккаунты в социальных сетях, видеохостинги и другие ресурсы, на которых распространяются радикальные идеи;

2) *оценка распространения экстремистского контента*. Анализ того, как быстро распространяется экстремистский контент, сколько людей охватывает, а также какие темы вызывают наибольший интерес среди пользователей;

3) *поддержка правоохранительных органов*. Сбор и передача информации о нарушениях закона соответствующим государственным органам для проведения расследования и принятия мер;

4) *оценка воздействия контента на общественное мнение*. Определение того, как экстремистские материалы могут влиять на общественные настроения, поведение граждан, молодежи и социальных групп.

Сам процесс мониторинга правоохранительными органами может быть разбит на несколько последовательных этапов:

1) *сбор информации*. На первом этапе осуществляется сбор данных о содержимом сети Интернет, которое может содержать признаки экстремистской, террористической или другой запрещенной деятельности;

2) *анализ контента*. После сбора информации необходимо провести ее анализ с целью выявления экстремистских материалов. В зависимости от характера материала зачастую применяются автоматические системы (в том числе на основе искусственного интеллекта), реже – ручная проверка контента специалистами для подтверждения того, что он действительно нарушает законодательство;

3) *оценка и фильтрация контента*. Важным этапом является фильтрация контента на основе установленных критериев: экстремистская идеология, насилие, ненависть, угрозы и другие нарушения. В этот этап может включаться:

– блокировка материалов на основе анализа;

– сообщения о найденных материалах в правоохранительные органы;

– применение санкций к пользователям, распространяющим такой контент (например, временная блокировка аккаунтов);

4) *документирование и хранение данных*. Все выявленные и проанализированные данные должны быть должным образом задокументированы для возможного использования в правовых и судебных процессах – речь, в частности, идет о создании отчетов, хранении доказательств (например, скриншотов, ссылок, текстов) для дальнейшего расследования;

5) *реагирование и блокировка контента*. На основе анализа и оценки материалов принимаются меры для блокировки или удаления незаконного контента. Важно, чтобы эти действия выполнялись в рамках закона и соблюдали баланс между безопасностью и правами человека (например, свободой слова);

6) *обратная связь и улучшение систем мониторинга*. После выполнения основных этапов важно провести анализ эффективности мониторинга, оценить, какие подходы работают, а какие нуждаются в улучшении.

С развитием цифровых технологий органы внутренних дел начали активно применять цифровые методы для мониторинга сети Интернет и выявления экстремистских материалов. Среди таких технологий можно выделить системы автоматического анализа текстов, которые позволяют распознавать признаки экстремистской деятельности в различных формах: от откровенных призывов к насилию до скрытых форм агитации. Одним из важных инструментов являются системы, ос-

нованные на обработке естественного языка (*Natural Language Processing, NLP*[1]), которые помогают анализировать текстовый контент и выявлять радикальные высказывания, призывы к насилию, разжигание вражды.

Эти системы позволяют не только анализировать тексты, но и выявлять схожие паттерны в разных источниках, что значительно ускоряет процесс выявления экстремистских материалов. Важным инструментом является также использование метаданных для отслеживания источников и распространителей экстремистской информации. В общем случае для эффективного мониторинга и анализа на современном этапе используется ряд нижепредставленных технологий и инструментов:

– *автоматические фильтры и системы анализа данных*, которые могут автоматически сканировать интернет-ресурсы на наличие экстремистского контента;

– *использование машинного обучения и нейронных сетей* для распознавания изображений, видео и текстов, связанных с экстремизмом;

– *краудсорсинговые платформы для сообщества*, которые помогают пользователям сообщать о подозрительных материалах;

– *инструменты анализа социальных сетей* для отслеживания активности пользователей и выявления экстремистской пропаганды;

– *системы для анализа больших данных (Big Data)*, которые обрабатывают большие объемы информации и могут выявлять скрытые паттерны экстремистской деятельности.

В качестве иллюстрации эффективного использования подобных инструментов можно привести систему автоматизированного контроля контента, созданную Роскомнадзором в партнерстве с МВД России. Она предназначена для выявления сомнительных материалов в социальных медиа и на онлайн-платформах (имеется в виду Единая информационная система Роскомнадзора).

Эффективность системы можно оценить по следующему показателю: в 2023 г. Роскомнадзор заблокировал или удалил 529 тыс. интернет-страниц, содержащих запрещенную информацию [27].

Особенно подчеркнем перспективность внедрения отмеченных выше технологий искусственного интеллекта (ИИ) в ОРД. Эти технологии позволяют автоматизировать процесс поиска и анализа экстремистского контента, что значительно увеличивает скорость реагирования на угрозы. Машинное обучение помогает системам обучаться на огромных объемах данных и точно определять контекст, в котором может быть использовано экстремистское содержание.

Так, в 2022 г. Роскомнадзором на основе ИИ была разработана система «Окулус» – она позволяет отслеживать подозрительные материалы в социальных сетях и на интернет-платформах, распознавать изображения и символы, противоправные сцены и действия, анализировать текст в фото- и видеоматериалах. Известно, что в 2022 г. с ее помощью было удалено или заблокировано свыше ста тысяч сайтов

[1] Обработка текстов на естественном языке (*Natural Language Processing, NLP*) – общее направление искусственного интеллекта и математической лингвистики. Оно изучает проблемы компьютерного анализа и синтеза текстов на естественных языках.

с фейками, в том числе о ходе СВО [28]. Также согласно тексту Стратегии противодействия экстремизму в Российской Федерации [22] к 2026 г. планируется развертывание единой базы данных экстремистского контента, интегрирующей большой массив данных из информационно-коммуникационных сетей с применением технологий ИИ для мониторинга «путем проведения потокового анализа данных, деанонимизации участников экстремистской деятельности».

Однако использование столь высоких технологий в борьбе с экстремизмом ставит перед правоохранительными органами важную задачу по соблюдению принципов безопасности и конфиденциальности. При сборе и обработке данных необходимо учитывать требования законодательства, связанного с защитой персональных данных, и обеспечивать прозрачность в процессе использования цифровых технологий. Важно обеспечить баланс между защитой прав граждан на конфиденциальность и необходимостью обеспечения общественной безопасности. Особое внимание следует уделять защите от утечек данных, особенно если речь идет о конфиденциальной информации, собранной в ходе оперативных мероприятий.

Заключение

Итак, в ходе исследования были рассмотрены основные аспекты оперативно-разыскной деятельности органов внутренних дел в борьбе с экстремизмом в сети Интернет. Выделены организационно-управленческие, правовые и технологические проблемы, а также предложены пути их решения.

Важно отметить, что эффективность борьбы с экстремизмом зависит от взаимодействия между различными государственными и частными структурами, а также от применения современных технологий. Одним из основных выводов является необходимость совершенствования законодательства в сфере противодействия экстремизму, особенно в контексте защиты прав граждан и обеспечения безопасности.

Перспективы дальнейшего развития работы органов внутренних дел в борьбе с экстремизмом в сети Интернет заключаются в интеграции новых технологий и улучшении координации с международными партнерами. Для этого необходимо развивать системы анализа больших данных, использовать блокчейн для мониторинга финансовых транзакций, а также совершенствовать механизмы защиты прав граждан в условиях цифровизации.

Кроме того, важно продолжать совершенствование образовательных программ для сотрудников правоохранительных органов и привлекать специалистов из области ИТ и кибербезопасности. Прогрессивные изменения в этих сферах откроют новые горизонты для обеспечения безопасности и стабильности в обществе в условиях второй четверти XXI в.

Пристатейный библиографический список

1. *Сундиев И. Ю., Смирнов А. А., Костин В. Н.* Новое качество террористической пропаганды: медиаимперия ИГИЛ // Информационные войны. 2015. № 1 (33).

2. Number of crimes of extremist nature registered in Russia from 2010 to 2023 // Statista : сайт. URL: https://www.statista.com/statistics/1044921/russia-number-of-extremist-related-crimes/ (дата обращения: 01.03.2025).

3. Данные МВД и ВС: в 2020 году число зарегистрированных «экстремистских» преступлений выросло, число приговоров сократилось // Сова : сайт. URL: https://www.sova-center.ru/racism-xenophobia/news/counteraction/2021/02/d43634/ (дата обращения: 01.03.2025).

4. *Шведчикова В., Ануфриева Е. А.* Понятие и задачи оперативно-розыскной деятельности // Всероссийский научный журнал «Вопросы права». 2024. № 3.

5. *Дудулина Н. В.* Оперативно-розыскная деятельность как разновидность правоохранительной деятельности // Современные научные исследования и инновации. 2017. № 11 (79).

6. *Архипцев И. Н., Сарычев А. В., Красников Р. В.* Совершенствование подготовки сотрудников правоохранительных органов по противодействию преступлениям, совершаемым с использованием информационных технологий // Правовая парадигма. 2020. Т. 19. № 2.

7. *Лисицын А. Г.* Некоторые аспекты деятельности органов внутренних дел по противодействию экстремизму // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2021. № 1 (86).

8. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 28 декабря 2024 г.) (с изм. и доп., вступ. в силу с 1 марта 2025 г.) // СЗ РФ. 1996. № 25. Ст. 2954.

9. Сведения о состоянии преступности и результатах расследования преступлений // СПС «КонсультантПлюс».

10. *Бедарев К. В.* К вопросу о мониторинге сети Интернет при выявлении преступлений экстремистской направленности // Бизнес. Образование. Право. 2018. № 2 (43).

11. Резолюция Генеральной Ассамблеи ООН от 8 сентября 2006 г. № 60/288 «Глобальная контртеррористическая стратегия Организации Объединенных Наций» // СПС «Гарант».

12. Рекомендация Европейской комиссии 2018/334 от 1 марта 2018 г. о мерах по эффективной борьбе с нелегальным онлайн-контентом // СПС «Гарант».

13. *Сигарев А. В.* Правовое регулирование противодействия экстремизму : курс лекций. Новосибирск : Изд-во СибАГС, 2015.

14. Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. 2011. № 1. Ст. 48.

15. Федеральный закон от 28 июля 2012 г. № 139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»» // СЗ РФ. 2012. № 31. Ст. 4328.

16. Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 23 декабря 2024 г.) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 1 января 2025 г.) // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

17. Статистика блокировок // RKNWEB : сайт. URL: https://rknweb.ru/statistics/ (дата обращения: 01.03.2025).

18. Информация Роскомнадзора: «Алгоритм действий в случае обнаружения в сети «Интернет» материалов с признаками наличия запрещенной информации, включая материалы экстремистского и (или) террористического характера» // Федеральная служба по надзору в сфере связи, информационных технологий и мас-

совых коммуникаций : сайт. URL: https://rkn.gov.ru/activity/electronic-communications/algoritm/ (дата обращения: 01.03.2025).

19. *Богданов А. В., Хазов Е. Н.* Основные направления противодействия экстремизму и терроризму оперативными подразделениями органов внутренних дел в современной России // Вестник Московского университета МВД России. 2017. № 4.

20. *Меркурьев В. В., Агапов П. В.* Криминологическая характеристика преступности, связанной с организацией экстремистского сообщества // Криминологический журнал. 2013. № 1.

21. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // СЗ РФ. 2002. № 30. Ст. 3031.

22. Указ Президента РФ от 28 декабря 2024 г. № 1124 «Об утверждении Стратегии противодействия экстремизму в Российской Федерации» // СЗ РФ. 2024. № 53 (ч. I). Ст. 8669.

23. Федеральный закон от 14 июля 2022 г. № 303-ФЗ «О внесении изменений в статью 265.10 Кодекса административного судопроизводства Российской Федерации и статьи 13 и 15 Федерального закона «О противодействии экстремистской деятельности»» // Президент России : сайт. URL: http://www.kremlin.ru/acts/bank/48081 (дата обращения: 01.03.2025).

24. Федеральный закон от 4 марта 2022 г. № 32-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации» // Президент России : сайт. URL: http://www.kremlin.ru/acts/bank/47616 (дата обращения: 01.03.2025).

25. Федеральный закон от 13 июня 2023 г. № 231-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // Президент России : сайт. URL: http://www.kremlin.ru/acts/bank/49374 (дата обращения: 01.03.2025).

26. Федеральный закон от 28 февраля 2025 г. № 15-ФЗ «О внесении изменений в Кодекс Российской Федерации об административных правонарушениях» // СПС «КонсультантПлюс».

27. За год Роскомнадзор заблокировал или удалил 529 тысяч страниц с запрещенной информацией // Sostav : сайт. URL: https://www.sostav.ru/publication/roskomnadzor-65332.html (дата обращения: 01.03.2025).

28. В России включили «Окулус»: что это за система, как работает и какой запрещенный контент ищет // Вечерняя Москва : сайт. URL: https://vm.ru/technology/1031988-v-rossii-vklyuchili-okulus-chto-eto-za-sistema-kak-rabotaet-i-kakoj-zapreshennyj-kontent-ishet (дата обращения: 01.03.2025).

References

1. *Sundiev I. Iu., Smirnov A. A., Kostin V. N.* New Quality of Terrorist Propaganda: The ISIS Media Empire. *Information Wars*, 2015, no. 1 (33). (In Russ.)

2. Number of Crimes of Extremist Nature Registered in Russia from 2010 to 2023. URL: https://www.statista.com/statistics/1044921/russia-number-of-extremist-related-crimes/ (date of the application: 01.03.2025). (In Russ.)

3. Data from the Ministry of Internal Affairs and the Supreme Court: In 2020, the Number of Registered "Extremist" Crimes Increased, the Number of Sentences Decreased. URL: https://www.sova-center.ru/racism-xenophobia/news/counteraction/2021/02/d43634/ (date of the application: 01.03.2025). (In Russ.)

4. *Shvedchikova V., Anufrieva E. A.* The Concept and Tasks of Operational-Search Activity. *All-Russian Scientific Journal "Questions of Law"*, 2024, no. 3. (In Russ.)

5. *Dudulina N. V.* Operational-Search Activity as a Type of Law Enforcement Activity. *Modern Scientific Research and Innovation*, 2017, no. 11 (79). (In Russ.)

6. *Arkhiptsev I. N., Sarychev A. V., Krasnikov R. V.* Improving the Training of Law Enforcement Officers to Counter Crimes Committed Using Information Technologies. *Legal Paradigm*, 2020, vol. 19, no. 2. (In Russ.)

7. *Lisitsyn A. G.* Some Aspects of the Activities of Internal Affairs Bodies to Combat Extremism. *Scientific Bulletin of the Oryol Law Institute of the Ministry of Internal Affairs of Russia Named After V. V. Lukyanov*, 2021, no. 1 (86). (In Russ.)

8. Criminal Code of the Russian Federation of June 13, 1996 No. 63-FZ (as amended on December 28, 2024) (as amended and supplemented, entered into force on March 1, 2025). *Collection of Legislation of the Russian Federation*, 1996, no. 25, art. 2954. (In Russ.)

9. Information on the State of Crime and the Results of Crime Investigations (SPS "ConsultantPlus"). (In Russ.)

10. *Bedarev K. V.* On Monitoring the Internet in Identifying Extremist Crimes. *Business. Education. Law*, 2018, no. 2 (43). (In Russ.)

11. UN General Assembly Resolution of September 8, 2006 No. 60/288 "The United Nations Global Counter-Terrorism Strategy" (SPS "Garant"). (In Russ.)

12. European Commission Recommendation 2018/334 of March 1, 2018 on Measures to Effectively Combat Illegal Online Content (SPS "Garant"). (In Russ.)

13. *Sigarev A. V.* Legal Regulation of Countering Extremism: Course of Lectures. Novosibirsk: Publishing House SibAGS, 2015. (In Russ.)

14. Federal Law of December 29, 2010 No. 436-FZ "On the Protection of Children from Information Harmful to Their Health and Development". *Collection of Legislation of the Russian Federation*, 2011, no. 1, art. 48. (In Russ.)

15. Federal Law of July 28, 2012 No. 139-FZ "On Amendments to the Federal Law 'On the Protection of Children from Information Harmful to Their Health and Development'". *Collection of Legislation of the Russian Federation*, 2012, no. 31, art. 4328. (In Russ.)

16. Federal Law of July 27, 2006 No. 149-FZ (as amended on December 23, 2024) "On Information, Information Technologies and the Protection of Information" (as amended and supplemented, entered into force on January 1, 2025). *Collection of Legislation of the Russian Federation*, 2006, no. 31 (part I), art. 3448. (In Russ.)

17. Blocking Statistics. URL: https://rknweb.ru/statistics/ (date of the application: 01.03.2025). (In Russ.)

18. Information from Roskomnadzor "Algorithm of Actions in Case of Detection on the Internet of Materials with Signs of the Presence of Prohibited Information, Including Materials of an Extremist and (or) Terrorist Nature". URL: https://rkn.gov.ru/activity/electronic-communications/algoritm/ (date of the application: 01.03.2025). (In Russ.)

19. *Bogdanov A. V., Khazov E. N.* The Main Directions of Counteracting Extremism and Terrorism by Operational Units of Internal Affairs Bodies in Modern Russia. *Bulletin of Moscow University of the Ministry of Internal Affairs of Russia*, 2017, no. 4. (In Russ.)

20. *Merkuriev V. V., Agapov P. V.* Criminological Characteristics of Crime Associated with the Organization of an Extremist Community. *Criminological Journal*, 2013, no. 1. (In Russ.)

21. Federal Law of July 25, 2002 No. 114-FZ "On Counteracting Extremist Activity". *Collection of Legislation of the Russian Federation*, 2002, no. 30, art. 3031. (In Russ.)

22. Decree of the President of the Russian Federation of December 28, 2024 No. 1124 "On Approval of the Strategy for Countering Extremism in the Russian Federation". *Collection of Legislation of the Russian Federation*, 2024, no. 53 (part I), art. 8669. (In Russ.)

23. Federal Law of July 14, 2022 No. 303-FZ "On Amendments to Article 265.10 of the Code of Administrative Procedure of the Russian Federation and Articles 13 and 15 of the Federal Law 'On Combating Extremist Activity'". URL: http://www.kremlin.ru/acts/bank/48081 (date of the application: 01.03.2025). (In Russ.)

24. Federal Law of March 4, 2022 No. 32-FZ "On Amendments to the Criminal Code of the Russian Federation and Articles 31 and 151 of the Criminal Procedure Code of the Russian Federation". URL: http://www.kremlin.ru/acts/bank/47616 (date of the application: 01.03.2025). (In Russ.)

25. Federal Law of June 13, 2023 No. 231-FZ "On Amendments to the Code of the Russian Federation on Administrative Offenses". URL: http://www.kremlin.ru/acts/bank/49374 (date of the application: 01.03.2025). (In Russ.)

26. Federal Law of February 28, 2025 No. 15-FZ "On Amendments to the Code of the Russian Federation on Administrative Offenses". URL: http://www.kremlin.ru/acts/bank/49374 (date of the application: 01.03.2025). (In Russ.)

27. Federal Law of February 28, 2025 No. 15-FZ "On Amendments to the Code of the Russian Federation on Administrative Offenses". URL: http://www.kremlin.ru/acts/bank/49374 (date of the application: 01.03.2025). (In Russ.)

28. Russia Has Switched on Oculus: What Kind of System Is It, How Does It Work, and What Kind of Prohibited Content Does It Search For? URL: https://vm.ru/technology/1031988-v-rossii-vklyuchili-okulus-chto-eto-za-sistema-kak-rabotaet-i-kakoj-zapreshennyj-kontent-ishet (date of the application: 01.03.2025). (In Russ.)

Сведения об авторах:
В. В. Баранов – кандидат юридических наук.
В. М. Пашин – доктор юридических наук.

Information about the authors:
V. V. Baranov – PhD in Law.
V. M. Pashin – Doctor of Law.

Статья поступила в редакцию 21.02.2025; одобрена после рецензирования 01.04.2025; принята к публикации 02.06.2025.

The article was submitted to the editorial office 21.02.2025; approved after reviewing 01.04.2025; accepted for publication 02.06.2025.