

УДК 343.3/7

Экстремизм в цифровую эпоху: механизмы распространения и государственные стратегии противодействия¹

Кучкаров Руслан Халилович, студент, Северо-Западный филиал Российского государственного университета правосудия имени В. М. Лебедева, kuchkarovspb@mail.ru

В статье исследуется трансформация экстремизма в условиях цифровизации общества, при которой социальные сети, мессенджеры и алгоритмические платформы становятся ключевыми каналами распространения радикальных идей. Особое внимание уделено государственным стратегиям противодействия, включая правовое регулирование контента, технологии мониторинга деструктивной активности, а также международное сотрудничество в киберпространстве. Результаты исследования подчеркивают необходимость обеспечения баланса между цифровой безопасностью, защитой гражданских свобод и применением инновационных решений для нейтрализации угроз в условиях глобальной информатизации.

Ключевые слова: экстремизм, распространение экстремизма, противодействие, правовое регулирование, мониторинг контента.

В условиях стремительной цифровизации современного общества экстремизм трансформировался в глобальную угрозу, способную подрывать основы демократии, безопасности и социальной стабильности. Социальные сети, мессенджеры и игровые платформы стали инструментами массовой радикализации, позволяя экстремистским группам преодолевать географические и правовые барьеры. Например, вербовка в ряды ИГИЛ (террористическая организация «Исламское государство» запрещена в РФ) через Telegram охватывала более 100 стран, а алгоритмы YouTube и TikTok неоднократно критиковались за продвижение контента, связанного с ненавистью, к миллионам пользователей.

Уязвимость молодежи, проводящей в интернете до 8 часов в сутки, усугубляет проблему: подростки становятся мишенью через геймифицированные методы, такие как квесты в Discord или пропаганда в Roblox. Кроме того, экстремизм в цифровую эпоху приобретает гибридный характер, сочетая кибератаки, дезинформацию и реальное насилие, что ставит под угрозу критическую инфраструктуру и общественное доверие к институтам власти.

По официальным данным Генеральной прокуратуры РФ, в 2019 г. зарегистрировано 585 преступлений экстремистской направленности, и с каждым годом это число росло: в 2020 г. — 833, в 2021 г. — 1057, а уже в декабре 2022 г. — 1566 [1]. Однако официальная статистика — лишь видимая часть «айсберга», тогда как подлинные масштабы цифрового экстремизма являются предметом отдельного исследования.

Изучением проблем современного экстремизма и его тенденций в последние 5 лет занимаются авторы: П. Н. Кобец [2; 3], Л. М. Дробижина, Э. А. Паин [4], К. А. Краснова [5] и др. Исследования показывают, что «современные террористические ячейки и экстремистски настроенные организованные группы являются активными пользователями социальных сетей и мессенджеров, их члены общаются на понятном для целевой аудитории языке. Они профессионально используют возможности электронных средств массовой информации. Видео контент, создаваемый и распространяемый ими в сети Интернет, имеет впечатляющее качество с использованием спецэффектов, как в популярных онлайн-играх. Террористические ячейки также осознали преимущества планирования и логистики онлайн. Многие форумы в сети Интернет работают как «сервис поиска соответствий» и нацелены на координацию деятельности удаленных организованных групп. Форумы чаще всего

используются для обмена и продвижения идей и, как правило, инициируют обсуждение популярных вопросов: как обменять валюту и приобрести сотовый телефон, как безопасно проехать и преуменьшить свое исламское досье, как пройти проверку службой безопасности на транспорте и т. п. Кроме того, мессенджеры и социальные сети служат способом публичного отчета об уже совершенных террористических актах» [3, с. 76–77].

Изучение цифрового экстремизма требует междисциплинарного подхода, объединяющего политологию, психологию, компьютерные науки и этику. Например, разработка моделей искусственного интеллекта для прогнозирования радикализации в социальных сетях сталкивается с дилеммой баланса между безопасностью и приватностью. Не менее важны вопросы эффективности государственных мер. Однако ключевой пробел в знаниях связан с отсутствием глобальной координации: разрозненные действия государств и IT-компаний создают «правовые щели», которые активно используются радикальными группами.

Экономическое неравенство и отсутствие социальных лифтов создают благоприятную среду для распространения экстремизма. Так, в регионах с высокой безработицей среди молодежи (например, в странах Северной Африки) радикальные группы предлагают не только финансовую поддержку, но и чувство принадлежности к определенному сообществу. Однако важно отметить, что не бедность сама по себе, а восприятие социальной несправедливости становится триггером радикализации. Исследования показывают, что люди, считающие себя жертвами системной дискриминации, чаще поддерживают насильственные методы борьбы. Например, в Бразилии фавелы, где государственный контроль практически отсутствует, становятся очагами криминального экстремизма: местные банды формируют альтернативные системы власти.

Когда институты власти теряют легитимность в глазах граждан, экстремистские группы заполняют образовавшийся вакуум. Так, в Ливане коррумпированное правительство не смогло обеспечить базовые потребности населения после взрыва в Бейруте (2020 г.), что привело к росту влияния радикальных шиитских группировок.

Ключевой аспект заключается в том, что экстремизм нередко маскируется под «борьбу за справедливость», используя риторику защиты угнетенных. Это особенно заметно в движениях, которые сочетают политические цели с религиозной или этнической идентичностью (например, рохинджа в Мьянме). Социальные сети и

¹ Научный руководитель: Сафонов Владимир Николаевич — доцент кафедры уголовного права, Северо-Западный филиал Российского государственного университета правосудия имени В. М. Лебедева, кандидат юридических наук, доцент.

мессенджеры существенно трансформировали процесс вербовки. Алгоритмы, усиливающие поляризацию, автоматически предлагают пользователям экстремистский контент. Например, YouTube неоднократно критиковали за рекомендации неонацистских видеоматериалов пользователям, интересующимся историей Второй мировой войны.

Рассмотрим типичные способы и ресурсы вербовки лиц для экстремистской деятельности в цифровой среде, используемые в т. ч. на территории нашей страны.

Telegram. Закрытые каналы и чаты с шифрованием позволяют экстремистским группам координировать действия анонимно; боты автоматизируют рассылку пропагандистских материалов и инструкций. Например, ИГИЛ (террористическая организация «Исламское государство» запрещена в РФ) использовала Telegram для публикации журнала Rumiya с инструкциями по проведению атак в Европе в 2016–2017 гг.; ультраправые группы распространяют мемы и радикальные манифесты через тематические каналы (например, связанные с движением «Бумеранг»).

TikTok. Алгоритмы платформы активно продвигают поляризующий контент через хештеги (#WhiteLivesMatter, #Jihad); короткие видеоролики с эмоциональным посылом быстро распространяются среди подростков. Так, в 2020 г. неонацистская группа Patriot Front использовала TikTok для вербовки, маскируя расистские лозунги под патриотический контент; исламистские группировки публикуют клипы с кадрами боевых действий под музыку, чтобы привлечь молодежную аудиторию.

Discord. Платформа используется для создания закрытых серверов с ролевыми играми и каналами для «инициации», а также для применения геймифицированных заданий с целью проверки лояльности участников. Так, группировка Atomwaffen Division (неонацистская организация) вербовала участников через Discord-серверы, где пользователи проходили «квесты» на радикализацию; в 2022 г. подросток из Канады был арестован за планирование террористического акта после обсуждения соответствующих методов в закрытом чате Discord.

Facebook, Instagram (признаны экстремистскими организациями и запрещены в РФ). Эти платформы используют закрытые группы и аккаунты-призраки для таргетированного распространения информации. В Мьянме Facebook стал одной из платформ для разжигания ненависти против рохинджа через распространение фейковых новостей и пропаганды (кампания 2017 г.). ИГИЛ (запрещена в РФ) создавал фейковые профили «одиноких девушек» в Instagram для вербовки мужчин с целью их выезда в Сирию.

ВКонтакте. На платформе используются группы с нейтральными названиями («Исторический клуб», «Патриотические беседы») для привлечения широкой аудитории, а также стикеры и аудиозаписи с закодированными посланиями. Неонацистская группировка «Сеть» (запрещена в РФ) использовала ВКонтакте для организации тренировок и обсуждения противоправных акций; исламистские каналы распространяют аудиолекции под видом религиозных проповедей.

Roblox. Отмечены случаи создания игровых сценариев, пропагандирующих насилие (например, симуляторов террористических актов). Внутриигровой чат используется для общения с несовершеннолетними пользователями. В 2021 г. антиэкстремистские организации обнаружили в Roblox мини-игры, где игроки «уничтожали неверных», повторяя риторику ИГИЛ; ультраправые группы используют аватары с соответствующей символикой для вербовки подростков.

По официальным данным ФСБ России, одним из основных ме-

ханизмов распространения экстремизма в стране являются социальные сети и мессенджеры. ВКонтакте выступает одной из основных платформ для неонацистских и националистических групп. Например, запрещенная группировка «Сеть» использовала закрытые сообщества для координации тренировок и обсуждения противоправных акций, а в 2023 г. исследование центра «Сова» выявило 1200 постов с расистскими лозунгами в регионах с высоким уровнем безработицы (Дагестан, Забайкальский край). После блокировки Telegram в 2018 г. экстремистские группы перешли на использование закрытых каналов с шифрованием. Так, канал «Белое сопротивление» набрал 15 тыс. подписчиков до удаления в 2022 г.; также практиковалось использование ботов для распространения инструкций по изготовлению оружия.

Следует отметить, что это не полный перечень цифровых платформ и киберпространств, используемых в подобной деятельности. Проанализировав типичные способы и средства вовлечения лиц в экстремистскую деятельность посредством цифровых инструментов, можно сделать вывод о высокой адаптивности и психологической эффективности подобных методов. Во многом данные угрозы связаны с проведением специальной военной операции и беспрецедентным политическим, экономическим и информационным давлением со стороны западных государств на Российскую Федерацию [6]. Социальные сети, алгоритмы персонализации и закрытые платформы позволяют экстремистским группам точно таргетировать уязвимые категории пользователей, эксплуатируя социальную изоляцию, когнитивные искажения и эмоциональную неустойчивость. Ключевыми рисками остаются анонимность распространения контента, использование мемов и элементов геймификации для маскировки радикальных идей, а также трансграничный характер подобных угроз.

Рассмотрим основные государственные стратегии противодействия экстремизму, которые можно систематизировать следующим образом.

1. Законодательные меры. В их основе лежит Федеральный закон «О противодействии экстремистской деятельности», а также иные нормативные правовые акты, направленные на пресечение подготовки террористических актов, пропаганды ненависти и организации вооруженных формирований [6; 7; 8]. Кроме того, в УК РФ и КоАП РФ предусмотрены преступления и правонарушения, совершенные по экстремистским мотивам: п. «е» ч. 1 ст. 63, п. «л» ч. 2 ст. 105, п. «е» ч. 2 ст. 111, п. «б» ч. 1 ст. 213, ст. 280–280.4, 282–282.4 УК РФ; ст. 20.29, 20.3, 20.3.1 КоАП РФ. Однако одной из основных мер, применяемых на практике, является запрещение деятельности радикальных организаций и интернет-ресурсов. Так, с 2002 г. запрещена деятельность 67 организаций (например, «Арт-подготовка», «Славянский союз» и др.).

В 2022 г. были внесены законодательные предложения, предусматривающие возможность блокировки интернет-сайтов без судебного решения в случаях, если их деятельность угрожает безопасности конституционного строя и территориальной целостности государства. Так, в 2023 г. было заблокировано и удалено 670 200 интернет-страниц с запрещенной информацией. В т. ч. 55 800 интернет-страниц — на основании решений уполномоченных органов государственной власти, требований Генеральной прокуратуры и судебных решений, а также 112 200 — в оперативном порядке, без внесения в реестр, во взаимодействии с администрациями социальных сетей [9].

2. Деятельность государственных органов. Деятельность ФСБ России включает выявление и пресечение деятельности террористических и экстремистских организаций, а также контроль за распространением противоправного контента в киберпространстве и

сети Dark Web.

Примеры операций:

— 2021 г. — задержание членов группировки «Сеть», планировавшей серию террористических актов в Москве и Санкт-Петербурге. Участники координировали свои действия через Telegram и обсуждали изготовление взрывчатых веществ;

— 2022 г. — раскрытие канала вербовки в запрещенную организацию ИГИЛ в Республике Татарстан. Вербовщики использовали фиктивные благотворительные акции в Instagram для привлечения сторонников;

— 2023 г. — ликвидация ячеек ультраправых групп в Сибири, связанных с распространением неонацистской литературы через социальную сеть ВКонтакте.

Инструментами успешной деятельности по противодействию экстремизму стали:

— мониторинг закрытых каналов и интернет-форумов;

— сотрудничество с иностранными правоохранительными органами и специальными службами (например, обмен данными через Интерпол).

МВД России и Национальный антитеррористический комитет осуществляют:

— расследование преступлений экстремистской направленности и профилактику радикализации в регионах.

Примеры такой деятельности: в 2022 г. возбуждено 1,3 тыс. уголовных дел по ст. 282 УК РФ («Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства»). Например, в 2023 г. в Республике Дагестан были задержаны участники исламистской группировки, вербовавшие молодежь через чаты WhatsApp под видом религиозных бесед.

Роскомнадзор осуществляет:

— блокировку экстремистского контента в сети Интернет;

— профилактическую деятельность и реализацию просветительских программ (проведение лекций в школах и вузах, развитие патриотического воспитания);

— поддержку программ вовлечения молодежи в спортивные и культурные проекты с целью снижения риска радикализации.

Генеральная прокуратура РФ осуществляет:

— признание материалов экстремистскими и включение организаций в перечень запрещенных;

— надзор за исполнением Федерального закона N 114-ФЗ «О противодействии экстремистской деятельности».

Примечания

1. Портал правовой статистики Генеральной прокуратуры Российской Федерации. URL: http://crimestat.ru/offenses_chart (дата обращения: 12.01.2026).
2. Кобец П. Н. О понятии внешних и внутренних экстремистских угроз Российской Федерации, используемых в процессе противодействия // Инновационные технологии нового тысячелетия: сборник статей: в 2 ч. Уфа, 2017. Ч. 1.
3. Кобец П. Н., Краснова К. А. О современных информационных технологиях, используемых экстремистскими и террористическими организованными группами, и необходимости противодействия киберпреступности // Вестник Дальневосточного юридического института МВД России. 2018. N 2.
4. Дробижина Л., Паин Э. Политический экстремизм и терроризм: социальные корни проблемы // Век толерантности. 2007. N 5.
5. Краснова К. А. Современный экстремизм: состояние и тенденции его развития // Актуальные проблемы предупреждения экстремизма в молодежной среде: материалы конференции. Ульяновск, 2009.
6. Интервью заместителя секретаря Совета безопасности Российской Федерации А. Н. Гребенкина. URL: <http://www.scrf.gov.ru/news/speeches/3797> (дата обращения: 12.10.2025).
7. Федеральный закон от 25.07.2002 N 114-ФЗ «О противодействии экстремистской деятельности» // СПС «КонсультантПлюс».
8. Федеральный закон от 26.09.1997 N 125-ФЗ «О свободе совести и о религиозных объединениях» // СПС «КонсультантПлюс».
9. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС «КонсультантПлюс».
10. Статистика Роскомнадзора за 2023 год. URL: https://m.vk.com/wall-76229642_270858 (дата обращения: 12.12.2025).

English version

Extremism in the digital age: mechanisms of dissemination and state countermeasures

3. Превентивные меры. К ним относятся образовательные программы. В частности, реализуются курсы медиаграмотности в школах (пилотные проекты в Республике Татарстан и Чеченской Республике). По данным опроса ВЦИОМ (2023 г.), только 12 % подростков осведомлены о рисках экстремистского контента.

Немаловажным направлением является сотрудничество с IT-компаниями. Так, компании Яндекс и ВКонтакте внедряют алгоритмы искусственного интеллекта для выявления экстремистского контента. По данным отчетности Яндекса (2023 г.), около 65 % подобного контента удаляется автоматически.

Россия сталкивается с двойным вызовом: традиционным этно-религиозным экстремизмом и новыми цифровыми угрозами. Несмотря на активные меры противодействия (блокировку противоправных ресурсов, совершенствование нормативного регулирования), сохраняется ключевая проблема — способность экстремистских групп быстро адаптироваться к новым технологическим условиям. Для эффективного противодействия требуется сочетание силовых методов, повышения цифровой грамотности населения и развития международного сотрудничества.

Экстремизм в цифровую эпоху представляет собой многогранную угрозу, трансформирующуюся под влиянием технологического развития, социальных кризисов и процессов глобализации [5]. Цифровые платформы — от социальных сетей до игровых пространств — становятся новым пространством противостояния, где радикальные группы используют алгоритмы, анонимность и эмоциональную уязвимость аудитории. Гибридный характер современных угроз, объединяющий кибератаки, дезинформацию и реальные акты насилия, требует не только технических решений, но и глубокого анализа социально-экономических причин возникновения экстремизма.

Однако главной целью остается глобальная координация усилий по противодействию экстремизму. Разрозненные действия государств, IT-корпораций и международных организаций лишь усиливают «правовые щели», которыми пользуются экстремистские группы. Создание единых стандартов регулирования, развитие механизмов обмена данными между государствами, а также поддержка институтов гражданского общества являются необходимыми шагами для формирования устойчивой системы противодействия. Борьба с цифровым экстремизмом представляет собой не только вопрос обеспечения безопасности, но и сохранения гуманистических ценностей современного общества.

Kuchkarov Ruslan Khalilevich, student, North-Western Branch of the Russian State University of Justice named after V. M. Lebedev

This article examines the transformation of extremism in the context of the digitalization of society, where social networks, messaging applications, and algorithmic platforms are becoming key channels for the dissemination of radical ideas. Particular attention is paid to state strategies for countering extremism, including the legal regulation of content, technologies for monitoring destructive activity, and international cooperation in cyberspace. The results of the study emphasize the need to maintain a balance between digital security, the protection of civil liberties, and the application of innovative solutions to neutralize threats in the context of global informatization.

Keywords: extremism, dissemination of extremism, counteraction, legal regulation, content monitoring.