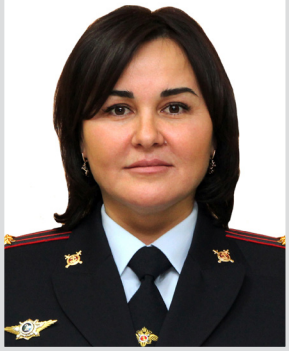
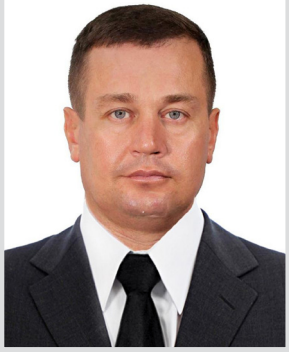
УДК 343
DOI: 10.24412/1998-5533-2025-4-179-183

Некоторые особенности противодействия экстремизму в условиях развития информационно-коммуникационных технологий



Минзянова Д.Ф.
Кандидат педагогических наук, доцент кафедры экономики, финансового права и информационных технологий в деятельности органов внутренних дел Казанского юридического института МВД России



Выстропов В.Г.
Кандидат юридических наук, доцент, доцент кафедры управления органами внутренних дел в особых условиях центра командно-штабных учений Академии управления МВД России (Москва)

Настоящая статья посвящена анализу комплекса проблем и особенностей, возникающих в сфере противодействия экстремизму в условиях стремительного развития информационно-коммуникационных технологий (далее – ИКТ). Целью данного исследования является рассмотрение новых форм и методов распространения экстремистских идеологий, вербовки, финансирования и координации действий экстремистских групп, обусловленных использованием ИКТ. Теоретическая значимость заключается в углублении научного понимания феномена экстремизма в условиях цифровизации, выявлении новых закономерностей его распространения и форм проявления в информационно-коммуникационной среде. Практическая значимость состоит в разработке конкретных рекомендаций по совершенствованию правовых, организационных и оперативно-розыскных мер противодействия экстремизму, а также профилактической работы в цифровом пространстве. Научная новизна исследования определяется комплексным и систематизированным анализом специфических черт экстремизма в условиях цифровой трансформации, которые требуют переосмысления традиционных подходов к противодействию. В заключении обосновывается необходимость разработки унифицированных международных стандартов реагирования на трансграничные проявления киберэкстремизма и создания эффективных механизмов обмена информацией между государствами; особое внимание уделяется превентивным мерам; подчеркивается, что успех в борьбе с киберэкстремизмом возможен при условии выработки стратегии, сочетающей многогранные аспекты на национальном и международном уровнях.

Ключевые слова: *экстремизм, киберэкстремизм, ИКТ, сеть Интернет, противодействие, правовые меры, сотрудничество*

Для цитирования: *Минзянова Д.Ф., Выстропов В.Г. Некоторые особенности противодействия экстремизму в условиях развития информационно-коммуникационных технологий // Вестник экономики, права и социологии. 2025. № 4. С. 179–183. DOI: 10.24412/1998-5533-2025-4-179-183.*

Экстремизм во всех его проявлениях представляет собой одну из наиболее серьезных угроз национальной безопасности и общественному порядку в современном мире. Исторически сложившиеся формы экстремистской деятельности, основанные на насилии, разжигании ненависти и вражды, в последние десятилетия претерпели существенные изменения под влиянием стремительного развития информационно-коммуникационных технологий (далее – ИКТ). Сеть Интернет, включая социальные сети, мессенджеры и другие цифровые платформы, стала мощным инструментом для распространения радикальных идеологий, вербовки новых сторонников, координации действий и финансирования экстремистских организаций.

Следует отметить, что традиционные подходы к противодействию экстремизму, разработанные в «доцифровую» эпоху, зачастую оказываются неэффективными перед лицом новых вызовов, порожденных глобальным и анонимным характером цифровой среды. Преступники активно используют возможности и преимущества ИКТ для обхода государственного контроля, преодоления географических барьеров и быстрого охвата широкой аудитории, что обуславливает необходимость глубокого переосмысления существующих стратегий и тактик борьбы с экстремизмом, а также разработки новых, адаптивных механизмов реагирования.

Следует отметить, что на территории нашей страны правовая основа противодействия экстремизму закреплена в Федеральном законе от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» (далее – ФЗ № 114-ФЗ), Уголовном кодексе РФ (далее – УК РФ) (ст.ст. 280, 280.1, 282, 282.1, 282.2, 282.3) и других нормативных правовых актах [1]. По мнению авторов настоящей статьи, противодействие экстремизму в условиях развития ИКТ – это стратегический информационный иммунитет общества, формируемый через комплекс мер, направленных на деконструкцию экстремистских нарративов, укрепление цифровой грамотности граждан, создание альтернативных позитивных контентов и своевременное пресечение деструктивной деятельности в информационном пространстве с целью защиты общественного сознания и реального мира от цифровых угроз.

Принимая во внимание вышеизложенное, напрашивается вывод, что ИКТ значительно расширили возможности преступников, сделав их деятельность более эффективной и трудно контролируемой [2, с. 189], поскольку:

− социальные сети и видеохостинги стали основными площадками для распространения экстремистских материалов;

− алгоритмы ранжирования контента могут непреднамеренно способствовать формированию «эхо-камер», где пользователи получают информацию, подтверждающую их предвзятые мнения, что усиливает радикализацию;

− активно используются мемы, короткие видеоролики, стримы, прямые эфиры для быстрой передачи своих идей, часто маскирующиеся под безобидный или развлекательный контент, а технологии *Deepfake* позволяют создавать поддельные видео- и аудиоматериалы, дискредитирующие оппонентов или призывающие к насилию, что затрудняет их верификацию.

По мнению авторов настоящей статьи, к наиболее распространенным видам профилактических мер следует относить:

− принятие мер, направленных на улучшение социальной и экономической ситуации среди тех слоев населения, которые более подвержены экстремистским высказываниям; впоследствии переходят в активное или пассивное противодействие действующей власти с целью свержения существующего режима на территории нашей страны [3, с. 12];

− осуществление технологических и оперативных мероприятий (развитие и внедрение в органах внутренних дел систем автоматического выявления негативного контента, популяризирующего экстремизм; сотрудничество с IT-платформами и компаниями; анализ цифровых следов и сетевой структуры);

− реализация правовых и организационных мероприятий, направленых на создание правового поля, позволяющего эффективно пресекать преступления, не нарушая при этом конституционные права на свободу слова;

− превентивно-профилактическая работа с потенциально уязвимыми группами, которая должна быть адресной, учитывая, что вербовка часто нацелена на лиц, испытывающих социальную изоляцию, идеологический вакуум или находящихся в уязвимом психологическом состоянии и др.

Следует отметить, что их реализация требует межведомственного взаимодействия и постоянного мониторинга технологических трендов, поскольку методы и инструменты злоумышленников меняются очень быстро.

Следует также отметить, что противодействие экстремизму в условиях развития ИКТ сталкивается с рядом специфических вызовов, к которым следует относить: трансграничный характер экстремистской деятельности, который создает правовые и юрисдикционные проблемы; серверы, на которых размещается экстремистский контент, могут находиться в разных странах, что затрудняет применение национального законодательства и требует сложного международного правового сотрудничества в вопросах экстрадиции и правовой помощи; проблемы доказательной базы возникают из-за возможности легкого удаления или подделки цифровых следов; сбор и закрепление электронных доказательств требует специальных знаний, технологий и унифицированных международных стандартов.

Принимая во внимание вышеизложенное, следует отметить, что технологические вызовы, которые в настоящее время стоят перед правоохранительными органами, включают повсеместное шифрование и анонимность. Использование сквозного шифрования в мессенджерах и технологий анонимизации, таких как *VPN* и *Tor*, делает практически невозможным перехват и дешифровку переписки преступников без прямого доступа к устройству [4, с. 138]. Скорость распространения экстремистского контента также является проблемой, поскольку он может быть распространен миллионам пользователей за считанные минуты, делая оперативное блокирование крайне сложной задачей. Кроме того, преступники используют ИИ для автоматической генерации контента, создания фейковых аккаунтов, обхода систем модерации и обнаружения, использования Даркнета как «убежища» для наиболее опасных форм экстремистской деятельности, включая торговлю оружием и наркотиками, а также обмен инструкциями по совершению исследуемых видов преступлений.

Технологические проблемы не являются единственными, поскольку также существуют организационные и кадровые проблемы. Правоохранительные органы часто испытывают дефицит высококвалифицированных IT-специалистов и криминалистов в IT-сфере, способных эффективно работать с современными технологиями. Вместе с тем слабое международное взаимодействие, отсутствие единых международных стандартов и процедур, а также политические разногласия между государствами препятствуют эффективному сотрудничеству в борьбе с трансграничным киберэкстремизмом.

Недостаточное государственно-частное партнерство также влияет на предупреждение исследуемых видов преступлений. Крупные IT-компании обладают значительными ресурсами и экспертизой в области модерации контента и анализа данных, но сотрудничество с ними со стороны правоохранительных органов не всегда налажено должным образом.

Вместе с тем, эффективное противодействие киберэкстремизму требует комплексного и многоуровневого подхода, который включает следующие направления:

1. Совершенствование правовой базы [5, с. 180–181]. Необходимо разработать международные конвенции и соглашения, унифицирующие подходы к определению экстремизма в цифровой среде, стандартизирующие процедуры сбора и предоставления электронных доказательств.

2. Адаптация существующих правовых норм, которые должны учитывать специфику цифровых преступлений, ответственность за использование ИИ для создания экстремистского контента.

3. Укрепление международного сотрудничества [6, с. 1040–1043], в рамках которого необходимо создавать эффективные механизмы правовой помощи, ускоренной экстрадиции, обмена оперативной информацией между правоохранительными органами разных стран.

4. Развитие технологических решений, а именно: применение ИИ и *Big Data*. Системы ИИ используются для автоматизированного мониторинга цифрового пространства, выявления и анализа экстремистского контента, прогнозирования угроз, а технологии *Big Data* обрабатывают огромные массивы информации для выявления скрытых связей и паттернов поведения [7, с. 169–170].

Вместе с тем необходимо укреплять взаимодействие с частными организациями, чьи интересы связаны с противодействием киберугрозам и соответствующим преступлениям. В первую очередь данное взаимодействие связано с вопросами оперативного выявления и удаления экстремистского контента, предоставления данных в рамках закона и разработки совместных технологических решений.

Исходя из изложенного выше, считаем необходимым подчеркнуть важность разработки и внедрения целого ряда мероприятий комплексного характера, направленных как на общее повышение уровня профилактики экстремизма, так и на конкретные меры реагирования на проявления экстремистских действий, включая деятельность, распространяемую посредством сети Интернет. Это предполагает необходимость принятия целенаправленных шагов как на законодательном уровне, так и в области информационной политики, образования и культуры, позволяющих эффективно предупреждать возникновение экстремистских настроений и пресекать попытки их распространения в виртуальном пространстве.

Развитие ИКТ радикально изменило ландшафт угроз, связанных с экстремистской деятельностью. Цифровая среда предоставила преступникам беспрецедентные возможности для распространения идеологий, вербовки, координации и финансирования, сделав их деятельность более анонимной, глобальной и трудно контролируемой. При этом традиционные методы противодействия экстремизму оказываются недостаточными перед лицом новых вызовов.

Эффективная борьба с экстремизмом в условиях цифровой трансформации требует комплексного, многоаспектного подхода, который сочетает совершенствование правовой базы, активное внедрение передовых технологических решений, укрепление международного и государственно-частного сотрудничества, а также развитие и принятие превентивных решений. По мнению авторов настоящей статьи, данные меры направлены на повышение цифровой грамотности и формирование устойчивого иммунитета к радикальным идеологиям в обществе.

Принимая во внимание вышеизложенное, представляется критически важным внедрение следую-

щих конкретных направлений по противодействию экстремизму в условиях развития ИКТ:

1. Создание и развертывание высокотехнологичных платформ, использующих машинное обучение, нейронные сети и обработку естественного языка для автоматического выявления, классификации и прогнозирования распространения экстремистских нарративов, фейковых новостей, *Deepfake*-материалов и призывов к насилию.

2. Создание и обучение мобильных групп, состоящих из экспертов по кибербезопасности, цифровой форензике, психологов, лингвистов, культурологов и специалистов по медиакоммуникациям.

3. Инициирование и участие в разработке унифицированных международных стандартов и протоколов по борьбе с киберэкстремизмом, включая механизмы оперативного обмена данными о киберугрозах, совместные расследования и экстрадицию киберпреступников.

4. Включение в образовательные программы высших и средних профессиональных учебных заведений модулей по цифровой криминалистике, анализу больших данных, киберпсихологии, методам идентификации AI-генерированного контента (*Deepfake*, поддельные тексты), а также стратегиям контрпропаганды и медиаграмотности; организация регулярных курсов повышения квалификации для сотрудников правоохранительных органов по работе с новыми технологиями и угрозами в киберпространстве.

Литература:

1. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» // Российская газета. 2002. № 138–139.
2. Опалев А.В. Современные информационные технологии как инструмент деятельности экстремистских и террористических организаций // Вестник Московского университета МВД России. 2022. № 5. С. 187–190.
3. Семихатская А.В. Методы и способы борьбы с экстремизмом // Актуальные вопросы теории и практики в деятельности подразделений полиции: материалы внутриведомственной науч.-практ. конф., Волгоград, 30-31 марта 2022 г. М.: Спутник+, 2022. С. 10–14.
4. Сергеев С.М. Некоторые проблемы противодействия использованию в преступной деятельности средств обеспечения анонимизации пользователя в сети Интернет // Вестник Санкт-Петербургского университета МВД России. 2017. № 1 (73). С. 137–140.
5. Шхагапсоев З.Л. Совершенствование методов противодействия экстремизму и терроризму в Российской Федерации // Пробелы в российском законодательстве. 2024. Т. 17, № 3. С. 177–184.
6. Савинов Я.А. Особенности международного сотрудничества при борьбе с экстремизмом // Право и правосудие в современном мире (к 100-летию Верховного Суда Российской Федерации): сб. науч. статей молодых исследователей X ежегодной всеросс. студенческой науч.-практ. конф. студентов, магистрантов и соискателей с межд. участием, Санкт-Петербург, 25-26 марта 2022 г. / Под общ. ред. Я.Б. Жолобова, А.А. Дорской. СПб.: Центр научно-информационных технологий «Астерион», 2022. С. 1040–1043.
7. Антонов В.В., Родионова Л.Е., Калимуллин Н.Р., Вояковская Я.С. Особенности извлечения данных из социальных сетей // Охрана, безопасность, связь. 2021. № 6-2. С. 168–175.

Some Specific Features of Countering Extremism in the Context of Developing Information and Communication Technologies

Minzyanova D.F.
Kazan Law Institute of the Ministry of Internal Affairs of Russia
Vystropov V.G.
Academy of Management of the Ministry of Internal Affairs of Russia (Moscow)

This article analyzes a range of issues and specific features arising in the field of countering extremism in the context of the rapid development of information and communications technologies (hereinafter referred to as ICT). The purpose of this study is to examine new forms and methods of disseminating extremist ideologies, recruiting, financing, and coordinating the actions of extremist groups, driven by the use of ICT. The theoretical significance of this study lies in deepening the scientific understanding of

the phenomenon of extremism in the context of digitalization, identifying new patterns of its dissemination and manifestations in the information and communications environment. The practical aspect is the development of specific recommendations for improving legal, organizational, and investigative measures to counter extremism, as well as preventative work in the digital space. The scientific novelty of this study lies in its comprehensive and systematized analysis of the specific characteristics of extremism in the context of digital transformation, which require a rethinking of traditional approaches to countering it. The conclusion substantiates the need to develop unified international standards for responding to cross-border manifestations of cyber-extremism and to create effective mechanisms for information exchange between states. Particular attention is paid to preventive measures. It is emphasized that success in the fight against cyber-extremism is possible only through the development of a strategy that combines multifaceted aspects at the national and international levels.

Keywords: extremism, cyber-extremism, ICT, internet, counteraction, legal measures, cooperation