УДК 343.34

КЛЮЧЕВЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ЭКСТРЕМИЗМУ В СЕТИ ИНТЕРНЕТ

Рощин А.С.

магистрант 2 курса юридического института

ФГБОУ ВО «МГУ им. Н.П. Огарёва»

г. Саранск, Россия

Аннотация. Статья посвящена анализу проблемы распространения экстремистских материалов в цифровой среде и рассмотрению комплекса мер по её решению. Акцентируется внимание на актуальности темы, обусловленной стремительным ростом интернет -аудит скоростью распространения информации, возможностью анонимного размещения контента и активным использованием сети экстремистскими группировками для вербовки и координации противоправной деятельности. В работе систематизированы основные направления противодействия, включающие правовое регулирование (анализ действующего законодательства, вопросы юрисдикции и международной координации), технологический контроль (мониторинг сетевого пространства, выявление и блокировка запрещённого контента), профилактическую работу (информирование населения, формирование медиаграмотности, психолого -педаг (координация органов власти, правоохранительных структур, ИТ -компа и гражданского общества). В работе подчёркивается, что эффективная борьба с экстремизмом в интернете требует комплексного подхода, сочетающего ужесточение ответственности за распространение запрещённых материалов, развитие систем раннего предупреждения, популяризацию альтернативных ценностных ориентиров через цифровые платформы и международное сотрудничество в сфере кибербезопасности.

Ключевые слова: экстремизм, интернет, кибербезопасность, противодействие, законодательство, профилактика, мониторинг, информационная безопасность.

KEY ASPECTS OF COUNTERING EXTREMISM ON THE INTERNET

Roshchin A.S.
2nd year Master's student at the Law Institute
Ogarev Mordovian State University,
Saransk, Russia

Annotation. The article is devoted to the analysis of the problem of the dissemination of extremist materials in the digital environment and the consideration of a set of measures to solve it. Attention is focused on the relevance of the topic due to the rapid growth of the Internet audience, the high speed of information dissemination, the possibility of anonymous posting of content and the active use of the network by extremist groups to recruit and coordinate illegal activities. The work systematizes the main areas of counteraction, including legal regulation (analysis of current legislation, issues of jurisdiction and international coordination), technological control (monitoring of the network space, identification and blocking of prohibited content), preventive work (informing the public, formation of media literacy, psychological and pedagogical measures) and interdepartmental interaction (coordination of authorities, law enforcement agencies, IT companies and civil society). The paper emphasizes that an effective fight against extremism on the Internet requires an integrated approach combining tougher responsibility for the dissemination of prohibited materials, the development of early warning systems, the popularization of alternative value orientations through digital platforms and international cooperation in the field of cybersecurity.

Keywords: extremism, Internet, cybersecurity, counteraction, legislation, prevention, monitoring, information security.

С каждым годом степень опасности экстремизма в сети становится всё больше и больше. Количество преступлений увеличивается, а вместе с этим развиваются и способы их совершения. Поэтому борьба с экстремизмом в современных реалиях стала очень важным направлением деятельности правоохранительных органов. Такая растущая динамика данного преступления прежде всего связана с общественно-политическими процессами как внутри России, так и на международной арене [1]. Если раньше, до широкой популяризации Интернета случаи проявления экстремистской деятельности возникали в рамках определённой территории какого-либо региона или города, то сейчас преступник и жертва могут находится на разных континентах [2].

Цифровые платформы стали мощным инструментом для радикальных сообществ: они позволяют открыто продвигать идеологию, вести публичные дискуссии и привлекать многотысячную аудиторию – порой охватывая сотни тысяч пользователей одновременно. Виртуальная среда, по данным исследований, играет решающую роль в вовлечении граждан в противоправную экстремистскую деятельность [3]. Основные формы активности таких групп включают распространение политических доктрин, проведение агитационных кампаний и целенаправленную вербовку новых сторонников. Особенно тревожно, что подобная деятельность часто активизируется на фоне напряжённости в зонах этнических и религиозных конфликтов.

Масштаб проблемы усугубляется тем, что современные технологии дают экстремистам дополнительные преимущества: анонимность, возможность использовать шифрование, трансграничный характер коммуникаций и инструменты быстрого распространения контента через соцсети и мессенджеры. По прогнозам экспертов, в ближайшие годы число экстремистских и террористических проявлений в интернете будет расти, но при этом значительная часть таких правонарушений остаётся скрытой от

правоохранительных органов. Среди ключевых причин такой ситуации не только высокая латентность преступлений в цифровой среде, но и недостаточное ресурсное обеспечение мер противодействия, технологическое отставание от новых методов обхода блокировок, а также пробелы в нормативно-правовом регулировании, которые не всегда успевают адаптироваться к быстро меняющимся цифровым реалиям.

Для повышения эффективности борьбы с экстремизмом в онлайн-пространстве требуется комплексный подход. Прежде всего, необходимо усовершенствовать нормативно-правовую базу, регулирующую противодействие экстремизму в цифровой среде: актуализировать законы с учётом новых форм противоправной активности, уточнить механизмы взаимодействия с интернет-платформами и усилить ответственность за распространение запрещённого контента. Не менее важно повысить уровень профессиональной подготовки сотрудников оперативных подразделений: обучить их работе с современными технологиями кибербезопасности, методам анализа цифровых следов и распознавания новых форм пропаганды. Кроме того, критически значимо улучшить материально-техническое оснащение правоохранительных структур: закупить специализированное программное обеспечение для мониторинга соцсетей и даркнета, создать централизованные базы данных экстремистских материалов с функцией автоматического распознавания, обеспечить подразделения мощными вычислительными ресурсами для обработки больших объёмов информации.

В последние годы российское законодательство в сфере противодействия экстремизму и терроризму в интернет-пространстве претерпело существенные изменения, направленные на расширение полномочий правоохранительных органов. Ключевым нововведением стало наделение Генерального прокурора РФ и его заместителей правом инициировать блокировку интернет-ресурсов с экстремистским контентом через Роскомнадзор. При этом подразделения МВД России по

противодействию экстремизму также могут выступать инициаторами подобных обращений в рамках своей оперативно-служебной деятельности.

Существенный шаг вперёд был сделан в 2014 году с принятием «антитеррористического пакета» законов. В частности, поправки в Федеральный закон «Об информации, информационных технологиях и о защите информации» [4] установили обязанность регистрации в Роскомнадзоре для владельцев интернет-ресурсов. Кроме того, нормативная база была усовершенствована в части квалификации преступлений экстремистской направленности: ранее закон охватывал только деяния, совершённые «публично» или «с использованием средств массовой информации», что оставляло без правовой оценки многие виды онлайн-активности, например, частную переписку или распространение материалов через закрытые сообщества.

Параллельно с развитием национального законодательства особую значимость приобретает международное сотрудничество в борьбе с цифровыми угрозами. Однако здесь возникает ряд сложностей. Прежде всего, в мире отсутствует единый подход к определению и криминализации экстремизма: большинство стран не закрепляют это понятие в уголовном законодательстве в целом, а предусматривают ответственность лишь за отдельные деяния: возбуждение национальной, расовой или религиозной вражды, распространение запрещённой идеологии и символики и т. д. Несмотря на рост подобных преступлений во всём мире, до сих пор нет всеобъемлющего международного договора, который охватывал бы все проявления экстремизма и терроризма, включая их реализацию через интернет.

С начала XXI века в рамках Организации Объединённых Наций продолжаются переговоры о создании всеобъемлющего международного соглашения, направленного на противодействие терроризму. Ключевой

задачей такого документа должно стать формулирование единого, юридически точного определения терроризма.

В структуре ООН действует специализированная Рабочая группа, фокусирующаяся на проблеме эксплуатации интернет-пространства в террористических целях. Её деятельность охватывает:

- исследование актуальных способов совершения киберпреступлений террористической направленности;
- комплексную оценку степени опасности подобных деяний;
- разработку стратегий противодействия на различных уровнях, от национального до глобального.

При этом инициатива о подготовке отдельного международного договора, целенаправленно регулирующего борьбу с онлайн-терроризмом, пока не вынесена на официальное рассмотрение.

В настоящее время базовым многосторонним инструментом в сфере киберправонарушений остаётся Конвенция Совета Европы о компьютерной преступности (Будапештская конвенция), принятая в 2001 году [5]. Данный правовой акт:

- формирует классификацию преступлений в цифровой среде;
- регламентирует механизмы межведомственного взаимодействия между странами при расследовании преступлений, выходящих за рамки национальных границ.

Среди подписантов конвенции не только государства европейского региона, но и такие страны, как Соединённые Штаты Америки, Япония, Канада, Южно-Африканская Республика и другие.

Российская Федерация, однако, не планирует становиться участницей этого соглашения. Подобная позиция существенно затрудняет выстраивание эффективного международного сотрудничества в сфере кибербезопасности, что особенно заметно на фоне обострившихся геополитических противоречий.

В этих условиях перспективным направлением становится развитие двусторонних и региональных соглашений с дружественными странами в рамках СНГ, ШОС, БРИКС и других объединений. Такие договорённости могли бы предусматривать единые стандарты выявления и блокировки экстремистского контента, механизмы оперативного обмена информацией между правоохранительными органами, совместные программы подготовки специалистов по кибербезопасности, а также координацию действий по противодействию финансированию терроризма через цифровые каналы.

Важную роль играет взаимодействие с технологическими компаниями и интернет-платформами. Совместная работа может включать разработку отраслевых стандартов модерации контента, внедрение автоматизированных систем обнаружения запрещённой информации, создание прозрачных процедур реагирования на запросы правоохранительных органов и проведение совместных учений по отработке сценариев кибератак и распространения экстремистских материалов.

В сфере противодействия экстремизму критически важно наращивать потенциал технологических решений. Современные достижения в области искусственного интеллекта и машинного обучения дают возможность эффективно обрабатывать колоссальные массивы информации, что позволяет на ранних этапах выявлять сообщества, склонные к распространению деструктивных идей. Перспективным направлением выглядит создание единой национальной платформы для мониторинга интернет-пространства, оснащённой инструментами предиктивной аналитики. Такая система сможет прогнозировать возникновение очагов радикализации, опираясь на комплексный анализ социально-экономических и демографических показателей. Не менее значимым представляется развитие отечественных технологий, направленных на установление личностей распространителей запрещённого контента при строгом соблюдении норм законодательства о защите персональных данных. Дополнительно требуется усовершенствовать

систему фильтрации интернет-трафика на уровне провайдеров: внедрить механизмы оперативной актуализации реестров заблокированных ресурсов, автоматизировать процессы обновления «чёрных списков» и интегрировать передовые инструменты анализа контента для повышения точности блокировок. Комплексный подход к модернизации технологических инструментов позволит существенно повысить эффективность противодействия экстремистским проявлениям в цифровой среде.

Не менее значима профилактическая работа с обществом, особенно с молодёжью. Включение в школьные и вузовские программы модулей по цифровой грамотности и информационной безопасности поможет разъяснить риски вовлечения в радикальные группы. Поддержка просветительских проектов блогеров и лидеров мнений, популяризирующих традиционные ценности и межэтническое согласие, может стать эффективным инструментом профилактики. Дополнительно целесообразно организовать тематические форумы, хакатоны и конкурсы для IT-специалистов по разработке инструментов противодействия экстремизму, а также создать горячую линию и онлайн-платформу для анонимного сообщения о подозрительной активности в сети с гарантией защиты заявителей.

Совершенствование национального законодательства также требует особого внимания. Необходимо уточнить понятийный аппарат, введя чёткие определения таких явлений, как «киберэкстремизм», «онлайн-вербовка» и «цифровая пропаганда». Целесообразно ввести дифференцированную ответственность за различные формы участия в экстремистской деятельности в сети и упростить процедуры блокировки ресурсов, чётко разграничив экстремистский контент и дискуссии на острые темы. Кроме того, стоит поддержать научные исследования в области киберпсихологии для изучения механизмов радикализации в онлайн-среде и разработки профилактических мер.

Комплексный подход, объединяющий совершенствование законодательства, развитие международного сотрудничества, внедрение передовых технологий и системную профилактическую работу с обществом, позволит эффективно противостоять угрозам экстремизма и терроризма в цифровой среде. Такой подход не только минимизирует правовые пробелы и повысит оперативность реагирования на новые вызовы, но и укрепит безопасность граждан в условиях стремительно меняющегося технологического ландшафта.

Противодействие экстремизму в интернет-пространстве сталкивается с комплексом взаимосвязанных проблем, корни которых лежат в геополитической асимметрии цифрового мира, технологических особенностях сети и ограниченном ресурсном потенциале правоохранительных структур.

Ключевой вызов связан с исторической и структурной зависимостью глобальной интернет-инфраструктуры от США. Фундаментальные протоколы сети были разработаны американскими специалистами, а ключевые управляющие институты, функционируют под влиянием американского правительства. Это создаёт асимметрию в доступе к пользовательским данным: российские правоохранительные органы сталкиваются с серьёзными препятствиями при запросах информации, поскольку американские компании и спецслужбы располагают приоритетным доступом к этим сведениям. Более того, политика США в сфере киберпространства вряд ли станет более лояльной к попыткам других государств усилить контроль над национальными сегментами интернета.

Технологические особенности сети усугубляют ситуацию. Современные инструменты шифрования и анонимизации позволяют преступникам эффективно скрывать свою деятельность. Российские органы могут контролировать лишь отечественные почтовые сервисы, тогда как зарубежные платформы остаются практически недоступными для мониторинга. Даже при

формальном сотрудничестве компаний с правоохранительными органами объём предоставляемой информации ограничен.

Проблема материально-технического оснащения подразделений, занимающихся противодействием экстремизму, остаётся крайне актуальной. В настоящее время сотрудники зачастую вынуждены прибегать к ручному поиску и анализу противоправного контента, используя обычные поисковые сервисы и просматривая веб-страницы визуально. Подобная практика демонстрирует низкую результативность: она сопряжена со значительными временными издержками, не обеспечивает достаточного охвата информации и не позволяет оперативно обрабатывать большие объёмы данных.

Для эффективного решения обозначенных проблем требуется многоаспектный подход, объединяющий технологические, правовые и организационные инструменты. Первоочередной задачей видится укрепление цифровой автономии России. Это предполагает: развитие отечественных поисковых платформ, социальных сетей и мессенджеров, создание альтернативных систем доменных имён и коммуникационной инфраструктуры. Подобные меры позволят уменьшить зависимость от зарубежных цифровых сервисов и упростят надзор за российской частью интернет-пространства.

Несмотря на то, что российские IT-компании создали несколько автоматизированных систем мониторинга, их внедрение сталкивается с серьёзными барьерами. Высокая стоимость таких решений и сложности технической интеграции препятствуют оснащению всех оперативных подразделений необходимым инструментарием. Одновременно технологический прогресс порождает новые риски: к примеру, финансирование экстремистской деятельности через блокчейн-транзакции с применением криптовалют крайне затруднительно отследить. Кроме того, распространение пропагандистских материалов всё чаще осуществляется с

помощью автоматизированных ботов и нейросетевых алгоритмов, что существенно осложняет выявление и пресечение противоправного контента.

Одновременно необходимо модернизировать нормативно-правовую базу, конкретизировать законодательные положения, касающиеся использования шифрования, методов анонимизации и операций с криптовалютами. Важным направлением работы становится выстраивание международного взаимодействия с государствами-партнёрами в рамках таких объединений, как СНГ, ШОС и БРИКС. Заключение соответствующих соглашений могло бы зафиксировать обязательства сторон по обмену оперативными данными и оказанию взаимной правовой поддержки в сфере кибербезопасности, что существенно повысило бы эффективность противодействия трансграничным угрозам.

Для эффективной борьбы с экстремизмом в цифровой среде необходим комплексный подход, охватывающий технологические, кадровые, профилактические и межведомственные направления. Прежде всего следует ускорить разработку отечественных систем автоматизированного мониторинга на базе искусственного интеллекта и машинного обучения, такие решения способны обрабатывать огромные массивы данных, выявлять экстремистский контент по текстовым, аудио и видеопризнакам, отслеживать активность подозрительных сообществ и прогнозировать потенциальные угрозы. Не менее важно укреплять кадровый потенциал: расширять программы подготовки специалистов по кибербезопасности и налаживать продуктивный обмен опытом между сотрудниками правоохранительных органов и IT-экспертами. Существенную роль играет и профилактическая работа, необходимо повышать цифровую грамотность населения, проводить просветительские кампании о рисках вовлечения в радикальные группы, а также взаимодействовать с лидерами мнений и общественными организациями для формирования устойчивого антиэкстремистского дискурса. Кроме того, требуется усилить сотрудничество

правоохранительных органов с отечественным IT-сектором через реализацию совместных проектов: разработку инструментов выявления и блокировки запрещённого контента, внедрение систем предиктивной аналитики и создание платформ для анонимного информирования о подозрительной активности. Только объединение этих усилий позволит выстроить эффективную систему противодействия экстремистским угрозам в современном киберпространстве.

Библиографический список

1. Стукалов В.В. Борьба с преступлениями террористической и экстремистской направленности на современном этапе / В.В. Стукалов А.Н. Горбунов // Вестн. Краснодар. ун-та МВД России. 2015. № 4(30). – Текст : непосредственный.

2. Кубякин Е.О. Молодежный экстремизм в сети Интернет как социальная проблема // Историческая и социально-образовательная мысль. 2011. № 4. – Текст : непосредственный.

3. Гуреева А.Н Цифровые платформы как субъекты конфликтогенной коммуникации: особенности, эффекты, риски / А.Н. Гуреева, П.А. Киреева // Вопросы теории и практики журналистики. 2022. №4. – URL: https://cyberleninka.ru/article/n/tsifrovye-platformy-kak-subekty-konfliktogennoy-kommunikatsii-osobennosti-effekty-riski. – Текст : электронный.

4. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2006 г. № 149-ФЗ (в ред. от 13 июля 2015 г.) // Рос. газ. 2006. 29 июля. – Текст : непосредственный.

5. Конвенция о преступности в сфере компьютерной информации – ETS N 185: принята в Будапеште 23 нояб. 2001 г. – URL: https://base.garant.ru/4089723/. – Текст : электронный