Дата поступления рукописи в редакцию: 04.05.2025 г.
Дата принятия рукописи в печать: 13.05.2025 г.
DOI: 10.24412/2782-3830-2025-4-60-63

АХЪЯДОВ Эльман Саид-Мохмадович,
канд. юр. наук, доцент кафедры уголовного права, процесса и национальной безопасности, заместитель декана по научной работе юридического факультета ФГБОУ ВО «Чеченский государственный университет им. А.А. Кадырова», e-mail: Akhyadov1990@mail.ru

ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ О ПРОТИВОДЕЙСТВИИ ИНФОРМАЦИОННОМУ ТЕРРОРИЗМУ: СОВРЕМЕННЫЕ ВЫЗОВЫ И ПРАВОВЫЕ МЕХАНИЗМЫ

Аннотация. *Статья посвящена анализу законодательных мер Российской Федерации в области противодействия информационному терроризму. Рассматриваются ключевые нормативно-правовые акты, включая Федеральный закон «О противодействии терроризму» и Федеральный закон «Об информации, информационных технологиях и о защите информации», а также их роль в пресечении использования информационных ресурсов в террористических целях. Особое внимание уделено правовым механизмам блокировки экстремистского контента, регулированию деятельности интернет-площадок и международному сотрудничеству. На основе анализа судебной практики и научных работ выявлены пробелы в законодательстве и предложены пути их устранения.*

Ключевые слова: *информационный терроризм, кибертерроризм, законодательство РФ, экстремистский контент, информационная безопасность, противодействие терроризму.*

AKHYADOV Elman Said-Mokhmadovich,
Candidate of Law, Associate Professor of the Department of Criminal Law, Procedure and National Security, Deputy Dean for Research of the Faculty of Law Federal State Budgetary Educational Institution of Higher Education "Chechen State University named after A.A. Kadyrov"

LEGISLATION OF THE RUSSIAN FEDERATION ON COUNTERING INFORMATION TERRORISM: MODERN CHALLENGES AND LEGAL MECHANISMS

Annotation. *The article analyzes the legislative measures of the Russian Federation in the field of countering information terrorism. It examines key regulatory acts, including the Federal Law "On Combating Terrorism" and the Federal Law "On Information, Information Technologies and Information Protection", as well as their role in preventing the use of information resources for terrorist purposes. Special attention is paid to legal mechanisms for blocking extremist content, regulation of internet platforms, and international cooperation. Based on the analysis of judicial practice and scientific works, gaps in legislation are identified, and ways to address them are proposed.*

Key words: *information terrorism, cyberterrorism, Russian legislation, extremist content, information security, counterterrorism.*

Информационный терроризм, под которым понимается использование цифровых технологий для планирования, финансирования и пропаганды террористической деятельности, представляет собой одну из ключевых угроз национальной безопасности России. Несмотря на наличие развитой законодательной базы, динамичное развитие технологий требует постоянной адаптации правовых механизмов. Как отмечает А.А. Малюк, информационный терроризм трансформирует традиционные формы противодействия, перенося борьбу в виртуальное пространство [1]. Цель статьи — оценить эффективность действующих норм и предложить меры по их совершенствованию.

Информационный терроризм определяется как деятельность, направленная на дестабилизацию общества через распространение экстре-

мистской идеологии, организацию кибератак на критическую инфраструктуру и вербовку сторонников в интернете [2].

– Кибертерроризм — атаки на информационные системы.
– Информационный экстремизм — пропаганда радикальных идей без применения насилия.

Понятие информационного терроризма в российском законодательстве закреплен в Федеральном законе № 35-ФЗ «О противодействии терроризму», где акцент сделан на использовании цифровых технологий для угрозы национальной безопасности [3]. В 2016 году в западных странах были приняты законы, расширяющие трактовку терроризма в сфере киберпространства, включая усиление систем управления транспортом и энергетикой.

Эксперты подчёркивают, что ключевой целью таких действий является не только физический ущерб, но и подрыв доверия граждан к государственным институтам [5].

Роскомнадзор играет важную роль в мониторинге интернет-ресурсов в вопросах выявления материалов, угрожающих общественному и государственному правопорядку. Важным аспектом является предотвращение манипулирования общественным мнением посредством фейковых новостей, провоцирующих панику и межнациональные конфликты, а также использования анонимности Даркнета для проведения групповых атак, осложняющих работу соответствующих органов.

Законодательство также определяет «информационно-психологическое воздействие» как метод терроризма, когда массовая рассылка тех или иных материалов вызывает эффект, сравнимый с реальными терактами. Российские суды признают лиц виновными в информационном терроризме даже за репосты экстремистских материалов, если они способствуют дезорганизации общества.

В рамках Стратегии кибербезопасности РФ до 2030 года особое внимание уделяется защите критической инфраструктуры от двойных ударов — физических и цифровых.

Экономический ущерб от таких действий включает в себя не только прямые потери, но и долгосрочное сокращение инвестиций из-за репутационных рисков, а аналитические прогнозы определяют ужесточение законодательства в области регулирования нейросетей, способных ограничить дезинформацию в масштабах, угрожающих национальной безопасности.

Кибертерроризм, в отличие от информационного, фокусируется исключительно на технологических атаках, например, взломах баз данных, тогда как информационный терроризм придерживается более широкого спектра методов, включая идеологический подход.

Проблема выявления кибератак, когда злоумышленники используют серверы третьих стран, чтобы замести следы, также подчёркивает характер разграничения киберпреступности и террористических мотивов в цифровой среде.

Федеральный закон № 35-ФЗ «О противодействии терроризму» устанавливает правовые барьеры для использования цифровых технологий в преступных целях. Статья 3 данного закона прямо запрещает распространение террористической идеологии, вербовку и финансирование экстремистских групп через интернет, что способствует снижению киберугроз национальной безопасности. В рамках статьи 15.3 операторы связи обязаны хранить данные о пользователях и их онлайн-активности, что позволяет правоохранительным органам оперативно расследовать инциденты. Эти меры направлены на пресечение каналов коммуникации террористов, использующих анонимность сети для координации атак.

Федеральный закон № 149-ФЗ дополняет антитеррористическое законодательство, фокусируясь на контроле контента [4]. Согласно статье 15.1, ресурсы, распространяющие материалы, связанные с терроризмом или экстремизмом, подлежат немедленной блокировке. Данное положение включает не только сайты, но и социальные сети, мессенджеры и другие платформы, где может распространяться запрещённая информация. Механизм блокировки реализуется через взаимодействие Роскомнадзора с интернет-провайдерами, в том числе посредством внедрения систем фильтрации трафика.

Комплексное взаимодействие законов создаёт многоуровневую систему защиты: 35-ФЗ предотвращает злоупотребление инфраструктурой связи, а 149-ФЗ ограничивает доступ к опасному контенту. Однако реализация этих норм вызывает дискуссии о балансе между безопасностью и приватностью: хранение персональных данных повышает риски утечек, а автоматическая блокировка иногда приводит к ошибкам, затрагивающим легитимные ресурсы. Для минимизации таких последствий законодательство предусматривает судебный надзор за решениями о блокировке и чёткие сроки хранения метаданных.

В свою очередь, техническая сторона исполнения законов требует от операторов значительных инвестиций в системы шифрования и архивации данных. Например, срок хранения информации о пользователях может достигать трёх лет, что усложняет работу небольших компаний. Между тем, международный опыт показы-

вает, что аналогичные меры в ЕС и США сопровождаются строгим регулированием доступа госорганов к данным, чтобы избежать злоупотреблений. В России вопросы прозрачности таких процессов остаются предметом общественных дебатов.

Критики подчёркивают, что эффективность законов зависит не только от жёсткости санкций, но и от развития цифровой грамотности населения. Профилактика терроризма требует осторожности от граждан в вопросах взаимодействия с подозрительным контентом. В свою очередь, владельцы онлайн-платформ несут ответственность за мониторинг контента, что стимулирует разработку алгоритмов искусственного интеллекта (AI) для автоматического выявления угроз.

Правоприменительная практика в области блокировки экстремистского контента сталкивается с системными сложностями, обусловленными несовершенством законодательной базы. Отсутствие юридически чёткого определения «экстремистского контента» приводит к субъективному толкованию норм, что провоцирует как избыточные блокировки, так и пропуск реальных угроз.

Технические и правовые сложности дополняются отсутствием единой базы данных заблокированных ресурсов, что затрудняет работу провайдеров и пользователей. Роскомнадзор в 2023 году анонсировал разработку ИИ-системы для прогнозирования создания зеркал, однако её внедрение затягивается из-за бюджетных ограничений. Параллельно растёт запрос на прозрачность судебных решений: публикация обоснований блокировок помогла бы сформировать устойчивую правоприменительную практику. В долгосрочной перспективе только комплексный подход, сочетающий законодательные уточнения, технологические инновации и повышение квалификации судей, позволит снизить риски злоупотреблений и повысить эффективность борьбы с экстремизмом.

Создание единого реестра экстремистских материалов с открытым доступом способно повысить прозрачность и координацию между государствами, IT-компаниями и гражданским обществом. Такой реестр, интегрированный с международными базами данных, позволит оперативно обновлять списки запрещённых ресурсов, минимизируя дублирование усилий. Открытость системы снизит риски злоупотреблений, так как общественность сможет оспаривать включение спорных материалов через специальные апелляционные комиссии. Однако реализация требует решения вопросов защиты персональных данных и предотвращения утечек, которые могут быть использованы злоумышленниками. Технически реестр должен поддерживать мультиязычный поиск и анализ контента с использованием технологий распознавания изображений и текста.

Усиление ответственности социальных сетей за пользовательский контент, по аналогии с европейским Общим регламентом по защите данных, предполагает введение жёстких штрафов за несвоевременное удаление экстремистских материалов. Это стимулирует платформы внедрять превентивные инструменты, такие как алгоритмы AI для автоматической модерации и системы верификации авторов опасных публикаций. Одновременно необходимо законодательно закрепить обязанность соцсетей предоставлять правоохранительным органам метаданные о распространении запрещённого контента. Опыт ЕС показывает, что подобные меры сокращают время реакции на инциденты, но требуют баланса между безопасностью и свободой выражения мнений, чтобы не превратить платформы в инструмент цензуры.

Разработка международной конвенции по кибертерроризму под эгидой ООН должна унифицировать правовые подходы к преследованию преступников в трансграничном цифровом пространстве. Документ мог бы установить стандарты криптографической расшифровки данных, экстрадиции подозреваемых и совместных кибероперациий. Ключевым вызовом остаётся согласование позиций стран с разным отношением к цифровому суверенитету — например, США, Китая и России. Для ускорения процесса целесообразно создать рабочие группы с участием юристов, технологов и представителей спецслужб. Конвенция также должна предусматривать механизмы финансирования программ кибербезопасности для развивающихся государств, чьи слабые инфраструктуры часто эксплуатируются террористами.

Внедрение этих мер требует синхронизации на национальном и глобальном уровнях. Например, реестр экстремистских материалов станет эффективным только при условии его интеграции с международными базами Interpol. Параллельно важно развивать образовательные программы для судей и сотрудников правоохранительных органов, чтобы они могли работать с цифровыми доказательствами. Критическим фактором остаётся публичный диалог: обсуждение законопроектов с IT-экспертами и правозащитниками поможет избежать принятия решений, нарушающих базовые права граждан.

Таким образом, предложенные инициативы формируют дорожную карту для построения устойчивой экосистемы противодействия терроризму, сочетающей технологические инновации и правовые гарантии.

Список литературы:

[1] Федеральный закон от 06.03.2006 № 35-ФЗ «О противодействии терроризму».

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

[3] Малюк А.А. Информационная безопасность: современные вызовы. Москва: Горячая линия-Телеком, 2020. 320 с.

[4] Стрельцов А.А. Правовые основы противодействия кибертерроризму. Москва: Юрлитинформ, 2019. 215 с.

[5] Петров А. И. Цели и методы информационного терроризма в цифровую эпоху // Журнал российского права. — 2021. — № 5. — С. 45–58.

Spisok literatury:

[1] Federal`ny`j zakon ot 06.03.2006 № 35-FZ «O protivodejstvii terrorizmu».

[2] Federal`ny`j zakon ot 27.07.2006 № 149-FZ «Ob informacii, informacionny`x texnologiyax i o zashhite informacii».

[3] Malyuk A.A. Informacionnaya bezopasnost`: sovremenny`e vy`zovy`. Moskva: Goryachaya liniya-Telekom, 2020. 320 s.

[4] Strel`czov A.A. Pravovy`e osnovy` protivodejstviya kiberterrorizmu. Moskva: Yurlitinform, 2019. 215 s.

[5] Petrov A. I. Celi i metody` informacionnogo terrorizma v cifrovuyu e`poxu // Zhurnal rossijskogo prava. — 2021. — № 5. — S. 45–58.

