Научная статья
УДК 343.9
https://doi.org/10.24412/2073-0454-2025-3-10-16
EDN: https://elibrary.ru/vyqxdl
NIION: 2003-0059-3/25-293
MOSURED: 77/27-003-2025-03-492

Стратегии противодействия информационному терроризму в современной России: институциональные, правовые и социальные аспекты

Эльман Саид-Мохмадович Ахъядов
Чеченский государственный университет имени А.А. Кадырова, Грозный, Россия, Akhyadov1990@mail.ru

Аннотация. Исследуются актуальные вызовы, связанные с информационным терроризмом в условиях цифровизации российского общества. Анализируется комплекс мер, направленных на противодействие данному явлению, включая правовое регулирование, технологические решения и социально-образовательные инициативы. Особое внимание уделяется роли государственных институтов, медиабезопасности и киберпространству как ключевым элементам национальной безопасности. На основе анализа работ российских ученых предлагается многоуровневая модель противодействия, сочетающая законодательные ограничения, технологические инновации и повышение медиаграмотности населения. Результаты исследования подчеркивают необходимость межведомственного взаимодействия и международной кооперации для минимизации угроз.

Ключевые слова: информационный терроризм, кибербезопасность, медиабезопасность, правовое регулирование, социальные институты, Россия

Для цитирования: Ахъядов Э. С.-М. Стратегии противодействия информационному терроризму в современной России: институциональные, правовые и социальные аспекты // Вестник Московского университета МВД России. 2025. № 3. С. 10–16. https://doi.org/10.24412/2073-0454-2025-3-10-16. EDN: VYQXDL.

Original article

Strategies for countering information terrorism in modern Russia: institutional, legal and social aspects

Elman S.-M. Akhyadov
Chechen State University named after A.A. Kadyrov, Grozny, Russia, Akhyadov1990@mail.ru

Abstract. The study examines the current challenges associated with information terrorism in the conditions of digitalization of Russian society. It analyzes a set of measures aimed at countering this phenomenon, including legal regulation, technological solutions and social and educational initiatives. Special attention is paid to the role of state institutions, media security and cyberspace as key elements of national security. Based on the analysis of Russian scientists' works, a multilevel model of counteraction is proposed, combining legislative restrictions, technological innovations and increasing media literacy of the population. The results of the study emphasize the need for interagency cooperation and international cooperation to minimize threats.

Keywords: information terrorism, cybersecurity, media security, legal regulation, social institutions, Russia

For citation: Akhyadov E. S.-M. Strategies for countering information terrorism in modern Russia: institutional, legal and social aspects. Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2025;(3):10–16. (In Russ.). https://doi.org/10.24412/2073-0454-2025-3-10-16. EDN: VYQXDL.

Введение. Вся история человеческого развития является ярким свидетельством тому, как информационные данные могли выступать не только в качестве средства, но и объекта противоборства, при этом иметь существенное значение при достижении всевозможных побед, тем самым влияя на определение судьбы не только отдельной страны, но и мощных военно-политических блоков. И не случайно вопросы роли и места информационных факторов занимают центральное место в истории.

Методика исследования. В основу работы положены сравнительно-правовой, формально-юридический и социологический методы, анализ статистики и междисциплинарный подход. Это позволило систематизировать стратегии противодействия информационному терроризму, включая правовые, технологические и образовательные механизмы.

Осуществляемое в отношении населения воздействие различными информационными сведениями требует контроля не только со стороны граждан-

ского общества, но и различных государственных структур в лице правоохранительных органов, поскольку неконтролируемое информационное пространство, помимо различных информационных конфликтов, может нести в себе явные либо скрытые деструктивные угрозы, в том числе террористического характера, негативно сказывающиеся на состоянии российского общества.

Информационный терроризм, как инструмент дестабилизации общества, приобрел в XXI в. глобальный масштаб. В России, где цифровизация охватила все сферы жизни, угрозы проявляются в форме кибератак на критическую инфраструктуру, распространения фейковых новостей и манипуляций общественным мнением. Например, в 2022 г. Роскомнадзор зафиксировал более 150 тыс. случаев распространения запрещенного контента, связанного с террористической пропагандой. Актуальность исследования обусловлена необходимостью защиты цифрового суверенитета и психического здоровья граждан. Цель статьи — систематизировать стратегии противодействия, включая правовые, технологические и социальные механизмы. Задачи: анализ эффективности законодательства, оценка роли ИИ-технологий, разработка рекомендаций по медиаобразованию.

Информационный терроризм определяется как «использование информационных ресурсов для нанесения ущерба государству, обществу или отдельным лицам через дезинформацию, кибератаки или психологические манипуляции» [2]. В отличие от классического терроризма, он не требует физического насилия, но способен парализовать работу институтов, дестабилизировать общественное сознание, подорвать доверие к государственным органам и создать хаос в социально-политической сфере. Одним из примеров является атака на сайты государственных органов, массовая дезинформация в социальных сетях, а также манипулятивное использование цифровых технологий для провокации массовых беспорядков.

Информационный терроризм может быть классифицирован по нескольким критериям.

1. По способу воздействия:

♦ дезинформационный терроризм (распространение ложных сведений);

♦ кибертерроризм (атаки на информационные системы, взломы);

♦ психологический терроризм (использование страха и паники для управления обществом).

2. По субъектам:

♦ индивидуальный информационный терроризм (активность отдельных лиц, хакеров, блогеров);

♦ групповой (организованные преступные сообщества, террористические организации);

♦ государственный (использование информационного терроризма как инструмента геополитического давления).

3. По целям:

♦ политический (дискредитация власти, провокация протестов);

♦ экономический (атаки на финансовые системы, обрушение биржевых котировок);

♦ социальный (распространение паники, дестабилизация общества).

Российское законодательство в сфере информационной безопасности начало формироваться в начале 2000-х гг. в ответ на рост угроз, связанных с распространением деструктивной информации, киберпреступности и манипуляции общественным сознанием через цифровые технологии. Основные законодательные акты в этой сфере включают:

♦ **Федеральный закон «Об информации, информационных технологиях и о защите информации» (2006 г.).** Этот закон стал базовым для регулирования цифровой сферы, в том числе устанавливает нормы по ограничению доступа к интернет-ресурсам, содержащим запрещенные материалы. В частности, с его помощью государство регулирует блокировку сайтов, распространяющих экстремистские материалы, призывы к насилию, а также пропаганду терроризма;

♦ **Федеральный закон «О противодействии экстремистской деятельности» (2002 г.).** Включает нормы, направленные на борьбу с распространением экстремистских материалов в сети Интернет. В 2012 г. к нему были внесены поправки, позволившие в досудебном порядке блокировать сайты, содержащие экстремистский контент;

♦ **Федеральный закон «О фейковых новостях» (2019 г.).** Ввел административную ответственность за распространение заведомо ложной информации, способной нанести вред обществу. Согласно закону, распространение недостоверных сведений, угрожающих жизни и здоровью граждан, может повлечь наложение штрафов для:

♦ физических лиц — до 400 тыс. руб.;

♦ должностных лиц — до 900 тыс. руб.;

♦ юридических лиц — до 1,5 млн руб.

Несмотря на наличие законодательных актов, регулирование информационной безопасности в России сталкивается с рядом проблем, например, отсутствие четких критериев «фейковой информации». В законе 2019 г. не раскрывается, какие именно сведения можно считать заведомо ложными, что создает риски субъективного правоприменения.

Современные угрозы, такие как дипфейки, алгоритмическая манипуляция общественным мнением и применение нейросетей для генерации дезинформации, остаются вне сферы регулирования или регулируются недостаточно оперативно.

Вопросы свободы слова и защиты персональных данных требуют балансировки между национальными интересами и соблюдением международных обязательств.

Анализ судебной практики показывает, что одни и те же нормы могут применяться по-разному, что подчеркивает необходимость унификации подходов и разъяснения отдельных положений законов.

Развитие законодательства в сфере информационной безопасности идет в направлении усиления государственного контроля над распространением информации. Однако для повышения его эффективности необходимы устранение правовых пробелов, введение четких определений терминов, а также адаптация законодательства к новым вызовам цифровой эпохи.

Современный цифровой терроризм представляет собой угрозу национальной и международной безопасности и требует комплексного подхода к противодействию. Использование информационно-коммуникационных технологий террористическими группами для пропаганды, координации действий, кибератак и сбора финансирования делает необходимым развитие эффективных технологических мер противодействия.

Одной из первостепенных задач в борьбе с цифровым терроризмом является обеспечение кибербезопасности стратегически важных объектов, таких как энергетические системы, банковский сектор, транспорт и государственные сервисы. Это достигается путем:

♦ внедрения многоуровневых систем аутентификации и шифрования данных;

♦ регулярного обновления программного обеспечения и устранения уязвимостей;

♦ использования искусственного интеллекта и машинного обучения для выявления аномального поведения в сетях.

Цифровые платформы активно используются террористами для вербовки, координации действий и распространения идеологии. Противодействие этим угрозам требует:

♦ создания автоматизированных систем мониторинга, основанных на алгоритмах обработки больших данных;

♦ разработки методов выявления экстремистского контента с использованием нейросетей;

♦ совместной работы правоохранительных органов и интернет-компаний по блокировке террористических ресурсов.

Борьба с цифровым терроризмом невозможна без комплексного подхода, включающего технологические, правовые и организационные меры. Современные разработки в области кибербезопасности, мониторинга и искусственного интеллекта позволяют эффективно выявлять и предотвращать террористические угрозы, однако их успешное применение требует тесного сотрудничества между государственными структурами, частным сектором и международными партнерами.

Одним из ключевых инструментов борьбы с информационным терроризмом является образование. Оно позволяет формировать у граждан критическое мышление, навыки анализа информации и устойчивость к деструктивным воздействиям. В данном контексте можно выделить несколько направлений образовательной деятельности.

Формирование медиаграмотности среди школьников и студентов включает в себя обучение навыкам проверки источников информации — способность анализировать, оценивать и интерпретировать информацию, поступающую из различных источников: Интернета, телевидения, печатных изданий и социальных сетей. Важной частью медиаграмотности является понимание механизмов создания новостей, интересов медиакомпаний и алгоритмов цифровых платформ, влияющих на доступность информации.

Основные принципы проверки информации.

1. **Анализ источника** — необходимо оценить авторитетность ресурса, проверять, кто является автором материала, его квалификацию и репутацию.

2. **Фактическая проверка** — рекомендуется сверять сведения с другими надежными источниками, особенно с официальными организациями, научными публикациями и государственными структурами.

3. **Оценка объективности** — важно учитывать, существует ли явная предвзятость в подаче информации, используются ли манипулятивные методы, такие как эмоциональные заголовки и искажение фактов.

4. **Определение первоисточника** — информация, распространяемая в СМИ и соцсетях, часто является пересказом без ссылки на оригинальный источник. Важно находить первоисточник и оценивать его достоверность.

Формирование медиаграмотности у школьников и студентов является важной задачей современного образования. В условиях цифровой эпохи критическое мышление и способность к проверке информации становятся ключевыми навыками, позволяющими защищать себя от дезинформации, принимать взвешенные решения и осознанно воспринимать окружающую реальность. Внедрение образовательных программ по медиаграмотности поможет воспитать новое поколение сознательных и ответственных граждан.

Программы цифровой безопасности для граждан разных возрастных групп играют ключевую роль в обеспечении безопасности личных данных и профилактике киберугроз. Эти программы адаптированы для различных возрастных категорий, что позволяет обеспечить доступность и понятность материала для всех пользователей Интернета, независимо от их уровня технической подготовки. Рассмотрим подробнее программы, направленные на обучение граждан правилам безопасного поведения в Интернете и защите личных данных.

Для детей и подростков важно создать безопасную среду, в которой они смогут обучаться безопасному поведению в Интернете с раннего возраста. Образовательные программы для данной группы чаще всего ориентированы на игровые формы обучения, которые делают процесс увлекательным и понятным.

1. **Цели:** формирование осознанного подхода к личной безопасности, повышение осведомленности о киберугрозах (например, фишинг, буллинг, вирусы), и обучение основам защиты данных.

2. **Основные темы:**

♦ безопасное общение в социальных сетях и мессенджерах;

♦ правила создания сложных паролей;

♦ умение распознавать мошенничество в Интернете (например, обманы с помощью фишинга);

♦ основы защиты личных данных;

♦ тспользование антивирусных программ и обновлений программного обеспечения.

3. **Методы:** использование интерактивных обучающих игр, видеороликов, квестов и анимаций, что помогает лучше усваивать материал и применять знания на практике.

Для взрослой аудитории программы цифровой безопасности чаще всего нацелены на более глубокое осознание рисков, связанных с личными данными, и на обучение более сложным аспектам безопасности, таким как защита корпоративной информации и предотвращение киберугроз в повседневной жизни.

Пожилые люди часто оказываются наиболее уязвимой группой в Интернете, поскольку не всегда имеют достаточный опыт или навыки для защиты своих данных. Программы для этой аудитории часто фокусируются на простоте изложения материала и шаг за шагом обучают основам безопасного использования Интернета.

Образовательные программы цифровой безопасности для разных возрастных категорий играют важнейшую роль в повышении уровня осведомленности граждан о возможных угрозах в сети и обучении эффективным методам защиты личных данных. С помощью таких программ можно существенно снизить риски, связанные с кибермошенничеством и утечками данных, а также повысить общую цифровую грамотность населения.

Повышение квалификации государственных служащих в сфере информационной безопасности и борьба с информационным терроризмом являются важными элементами государственной политики в области защиты национальной безопасности. В условиях стремительного развития технологий и увеличения угроз в киберпространстве, государственные служащие должны обладать необходимыми знаниями и навыками для эффективного реагирования на вызовы информационной войны и борьбы с террористическими угрозами в Интернете.

По мнению А. А. Козлова, информационная безопасность представляет собой не только защиту от внешних атак, но и создание системы предотвращения и выявления угроз в пределах государственного аппарата [3]. Это требует постоянного повышения

квалификации сотрудников, поскольку изменения в технологии и методах работы преступников налагают новые требования к профессиональным навыкам. Программы повышения квалификации должны охватывать как теоретические основы информационной безопасности, так и практические аспекты, включая защиту персональных данных, борьбу с киберугрозами и понимание правовых аспектов информационной безопасности.

Таким образом, повышение квалификации государственных служащих в сфере информационной безопасности является необходимым шагом в укреплении системы защиты от информационного терроризма. Эффективная подготовка кадров обеспечит защиту национальных интересов в условиях современных угроз.

Образование тесно связано с социальными мерами, направленными на борьбу с информационным терроризмом.

Создание государственных и общественных программ по противодействию дезинформации является важным шагом в обеспечении национальной безопасности и защите общественного порядка в условиях глобализации и быстрого распространения информации. Дезинформация, распространяемая через различные каналы, включая социальные сети, медиа и интернет-платформы, представляет собой угрозу для стабильности общества, может нарушить функционирование политических институтов и подорвать доверие граждан к государственной власти.

По мнению В. Д. Карпова, дезинформация не только нарушает объективность общественного восприятия, но и способствует манипуляциям общественным мнением с целью дестабилизации ситуации в стране [4]. В связи с этим важнейшим элементом политики государства должно стать создание и внедрение программ, направленных на выявление, предотвращение и нейтрализацию угроз, связанных с распространением ложной информации. Такие программы должны включать как меры юридической ответственности для распространителей дезинформации, так и образовательные инициативы, направленные на повышение информационной грамотности населения.

Важным аспектом является взаимодействие государственных и общественных структур. Общественные организации и неправительственные инициативы могут сыграть ключевую роль в мониторинге и анализе дезинформации, а также в обучении граждан, особенно в вопросах критического восприятия информации. Как отмечает Е. А. Белова, важность общественных инициатив заключается в том, что они позволяют не только бороться с последствиями распространения дезинформации, но и предотвращать ее на ранних стадиях [5]. В условиях современного информационного общества, где каждый пользователь может стать источником как правдивой, так и ложной информации, гражданское общество играет значительную роль в укреплении общественного иммунитета к манипуляциям.

Создание эффективных программ по противодействию дезинформации требует комплексного подхода, включающего правовые, образовательные и общественные инициативы, а также межведомственное сотрудничество. Это обеспечит устойчивость общества к угрозам дезинформации и усилит защиту национальных интересов.

Формирование культуры ответственного потребления информации через социальные кампании играет важную роль в борьбе с информационным терроризмом, который становится все более актуальной угрозой в условиях цифровой трансформации общества. В последние годы внимание уделяется не только борьбе с информационными атаками, но и вопросам того, как граждане воспринимают и распространяют информацию. Ответственное потребление информации предполагает способность критически оценивать источники, различать факты от манипуляций и не становиться частью информационных атак, направленных на дестабилизацию общества.

По мнению А. Е. Дмитриева, ключевым аспектом формирования культуры ответственного потребления является повышение уровня медиаобразования и создание инициатив, способствующих развитию у граждан навыков аналитического подхода к потребляемой информации [6]. Социальные кампании, направленные на просвещение граждан, должны включать обучение тому, как распознавать фейки, дезинформацию и манипуляции в СМИ, а также призывать к осторожности при распространении непроверенных сведений.

В борьбе с информационным терроризмом, как утверждает Н. И. Савин, эффективная противодействующая стратегия должна включать не только создание законодательных и технических барьеров, но и активную работу с общественностью, чтобы

вовлечь граждан в процесс защиты от информационных угроз [7]. Информационный терроризм, в отличие от традиционного, ориентирован на воздействие через информационные каналы с целью создания паники, провокации насилия или дестабилизации политической обстановки. Одним из методов нейтрализации таких угроз является создание программ, которые учат граждан критически подходить к получаемой информации, а также вовлечь их в процессы опровержения ложных данных.

Социальные кампании должны охватывать широкий спектр тем, начиная от основ цифровой гигиены и заканчивая подробным разбором механизмов функционирования информационного терроризма. Важно, чтобы такие инициативы были не только информационными, но и вовлекающими, создавая среду, где граждане ощущают свою ответственность за информацию, которую они потребляют и распространяют.

Борьба с информационным терроризмом невозможна без формирования культуры ответственного потребления информации, которая должна быть интегрирована в образовательные и социальные практики. Это позволит значительно снизить влияние дезинформации и повысить осведомленность о реальных угрозах информационной безопасности.

Заключение. Как для России, так и для зарубежных стран информационный терроризм представляет собой серьезную угрозу для национальной безопасности, поскольку он может быть использован для дестабилизации политической ситуации, разрушения доверия к институтам власти и подрыва социальной гармонии. Рассмотрение опыта зарубежных стран и России в этой области позволяет выявить эффективные практики и подходы, которые могут быть использованы для противодействия данной угрозе.

Зарубежный опыт борьбы с информационным терроризмом разнообразен. В США, например, значительное внимание уделяется защите критической инфраструктуры от кибератак и пропаганды через интернет-ресурсы. В 2018 г. в США был принят Закон о противодействии иностранному вмешательству в выборы, который направлен на борьбу с дезинформацией и манипуляциями в электоральных процессах через социальные сети и другие цифровые платформы. Исследования, такие как работа Р. Ш. Вудса, отмечают, что государственные органы США активно сотрудничают с технологическими компаниями для быстрого реагирования на угрозы, связанные с распространением ложной информации, и выявления источников подобных атак [8].

Особое внимание в зарубежных странах уделяется и правовому регулированию в сфере информационной безопасности. В Европейском Союзе для борьбы с информационным терроризмом создана сеть Европейского агентства по кибербезопасности (ENISA), которая занимается мониторингом и анализом угроз, связанных с распространением террористической пропаганды в Интернете. Как указывает М. Д. Петрова, основными методами борьбы являются не только правовые меры, но и общественные инициативы, такие как проведение образовательных программ для граждан и совместная работа с интернет-платформами по удалению экстремистского контента [9].

Как отмечает Ю. Б. Мельников, одним из важных аспектов российской практики является создание федеральных законов, регулирующих использование интернета для распространения экстремистской и террористической информации. Например, в 2017 г. был принят закон, который обязывает интернет-платформы блокировать сайты, содержащие пропаганду терроризма [10]. Также большое значение придается работе с молодежью и проведению образовательных программ по информационной безопасности, направленных на предупреждение возможных угроз.

Опыт зарубежных стран и России в области борьбы с информационным терроризмом подтверждает необходимость комплексного подхода, включающего правовые, технологические и образовательные меры. Важно, чтобы государства продолжали развивать механизмы сотрудничества и обмена опытом, чтобы эффективно противодействовать информационным угрозам в глобализированном мире.

Выводы. Информационный терроризм является серьезной угрозой национальной и международной безопасности. В борьбе с ним важную роль играет образование, способствующее формированию критического мышления и информационной устойчивости у граждан. В сочетании с государственными мерами, направленными на мониторинг и регулирование информационного пространства, социально-образовательные инициативы могут существенно снизить уровень угрозы информационного терроризма и повысить безопасность общества в цифровую эпоху.

Список источников

1. Петров А. В. Искусственный интеллект в борьбе с киберпреступностью. М. : Техносфера, 2020.

2. Сидоров С. И. Информационный терроризм: теория и практика. СПб. : Политехника, 2019.

3. Козлов А. А. Информационная безопасность в государственных структурах. М. : Наука, 2019.

4. Карпов В. Д. Проблемы дезинформации в современном обществе. М. : Политическая наука, 2021.

5. Белова Е. А. Общественные программы по борьбе с дезинформацией. СПб., 2022.

6. Дмитриев А. Е. Культура ответственного потребления информации: теоретические основы и практическое применение. М., 2020.

7. Савин Н. И. Информационный терроризм: вызовы и решения для современной безопасности. СПб. : Политический анализ, 2021.

8. Вудс Р. Ш. Противодействие информационному терроризму в США. Нью-Йорк : Информационная безопасность, 2020.

9. Петрова М. Д. Правовые меры борьбы с информационным терроризмом в странах Европейского Союза. М. : Право и безопасность, 2021.

10. Мельников Ю. Б. Российский опыт борьбы с информационным терроризмом: правовые и организационные меры. М. : Юридический мир, 2020.

References

1. Petrov A. V. Artificial intelligence in the fight against cybercrime. M. : Technosphere, 2020.

2. Sidorov S. I. Information terrorism: theory and practice. SPb. : Polytechnic, 2019.

3. Kozlov A. A. Information security in government structures. M. : Science, 2019.

4. Karpov V. D. Problems disinformation in modern society. M. : Political science, 2021.

5. Belova E. A. Public programs to combat disinformation. SPb., 2022.

6. Dmitriev A. E. Culture of responsible information consumption: theoretical foundations and practical application. M., 2020.

7. Savin N. I. Information terrorism: challenges and solutions for modern security. SPb. : Political Analysis, 2021.

8. Woods R. S. Countering information terrorism in the United States. New York : Information Security, 2020.

9. Petrova M. D. Legal measures to combat information terrorism in the countries of the European Union. M. : Law and Security, 2021.

10. Melnikov Yu.B. Russian experience in combating information terrorism: legal and organizational measures. M. : Legal World, 2020.

Информация об авторе

Ахъядов Э. С.-М. — доцент кафедры уголовного права, процесса и национальной безопасности Чеченского государственного университета имени А.А. Кадырова, заместитель декана по научной работе юридического факультета, кандидат юридических наук.

Information about the author

Akhyadov E. S.-M. — Associate Professor of the Department of Criminal Law, Procedure and National Security of the Chechen State University named after A.A. Kadyrov, Deputy Dean for Research of the Faculty of Law, Candidate of Legal Sciences.

Статья поступила в редакцию 03.03.2025; одобрена после рецензирования 31.03.2025; принята к публикации 25.04.2025.

The article was submitted 03.03.2025; approved after reviewing 31.03.2025; accepted for publication 25.04.2025.