- НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ -

Дата поступления рукописи в редакцию: 18.06.2025 г. DOI: 10.24412/2782-3830-2025-6-47-50
Дата принятия рукописи в печать: 21.07.2025 г.

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

НУРАДИЕВА Анжела Абуевна,
ассистент кафедры уголовного права, процесса и национальной безопасности Чеченского государственного университета им. А.А. Кадырова,
e-mail: nuradision98@mail.ru

ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОМУ ЭКСТРЕМИЗМУ И ТЕРРОРИЗМУ НА СОВРЕМЕННОМ ЭТАПЕ РАЗВИТИЯ ОБЩЕСТВА

Аннотация. *В статье исследуется феномен информационного терроризма как ключевой угрозы национальной и международной безопасности в условиях цифровой трансформации общества. Анализируются сущность, цели, методы и каналы распространения деструктивного информационного воздействия террористических организаций. На основе системного подхода рассматриваются теоретические основы и методологические принципы построения эффективной системы противодействия, включая правовые, организационные и технологические аспекты. Подчеркивается необходимость комплексного, междисциплинарного и международно-координированного подхода. Целью данного исследования является всестороннее осмысление феномена информационного терроризма в современном обществе, его сущности, форм проявления и угроз, а также правовых и организационных подходов к противодействию данному виду террористической активности.*

Ключевые слова*: Информационный терроризм, гибридные угрозы, информационная безопасность, деструктивное информационное воздействие, противодействие информационному экстремизму и терроризму, цифровая среда, национальная безопасность, медиапространство.*

Работа выполнена при поддержке Минобрнауки РФ (FEGS-2024-0017)

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"

NURADIEVA Anzhela Abuyevna,
Assistant of the Department of Criminal Law, Procedure and National Security of the Chechen State University named after A.A. Kadyrov

THEORETICAL AND METHODOLOGICAL FOUNDATIONS OF COUNTERACTING INFORMATION EXTREMISM AND TERRORISM AT THE PRESENT STAGE OF DEVELOPMENT OF SOCIETY

Annotation. *The article examines the phenomenon of information terrorism as a key threat to national and international security in the context of the digital transformation of society. The essence, goals, methods and channels of dissemination of the destructive information impact of terrorist organizations are analyzed. Based on the systems approach, the theoretical foundations and methodological principles of building an effective counteraction system are considered, including legal, organizational and technological aspects. The need for an integrated, interdisciplinary and internationally coordinated approach is emphasized. The purpose of this study is a comprehensive understanding of the phenomenon of information terrorism in modern society, its essence, forms of manifestation and threats, as well as legal and organizational approaches to countering this type of terrorist activity.*

Key words: *Information terrorism, hybrid threats, information security, destructive information impact, countering information extremism and terrorism, digital environment, national security, media space.*

Актуальность проблемы совершенствования наказуемости за преступления террористической направленности в российском уголовном праве обусловлена тем, что меры уголовной репрессии являются значимой частью системы противодействия террористической и экстремистской деятельности в России. Насколько видоизменяются и модифицируются указанные виды деятельности, настолько и уголовное наказание должно отвечать «вызовам» настоящего времени, где обязательным условием является согласованность отечественного уголовного законодательства и международных конвенций по противодействию различным аспектам терроризма по ключевым аспектам квалификации преступлений и наказуемости за их совершение. Необходимость ужесточения наказуемости за совершение данных преступлений предопределяется тем, что предупреждение такой преступной деятельности затруднено и ограничено в тех случаях, когда центры организации идеологии и практики терроризма находятся за пределами РФ.

Современная эпоха характеризуется стремительным развитием информационно-коммуникационных технологий, которые оказывают глубокое воздействие на все сферы общественной жизни, включая сферу безопасности. Традиционные формы терроризма постепенно уступают место новым, более гибким и трудно прогнозируемым формам, среди которых особое место занимает информационный терроризм.

«Как отмечает А. И. Комиссаров, трансформация терроризма в условиях цифровизации происходит не только за счёт применения террористами новых технологий, но и благодаря переосмыслению самих целей террористической деятельности» [1]. Современные террористические группы всё чаще прибегают к использованию интернета и цифровых платформ не только как инструмента пропаганды, но и как средства воздействия на массовое сознание, мобилизации сторонников и координации действий.

«Ю. И. Наумов подчеркивает, что появление новых форм коммуникации позволило террористическим структурам выйти за рамки территориальных ограничений: Сетевая структура современного терроризма делает его менее уязвимым для традиционных методов силового противодействия» [2].

Таким образом, террористическая активность в XXI веке все больше ориентирована на информационное пространство, в котором разворачиваются атаки на символы, ценности и когнитивные установки общества.

На сегодняшний день в научной литературе отсутствует единое, общепринятое определение информационного терроризма, что обусловлено сложностью феномена и его междисциплинарным характером. Вместе с тем, существует ряд подходов, позволяющих очертить основные черты этого явления.

«С точки зрения уголовного права, как отмечает А. Н. Рарог, информационный терроризм представляет собой деятельность, направленную на дестабилизацию политической, социальной или экономической системы с использованием информационных средств и технологий, обладающую признаками террористического акта» [3].

Сущностные характеристики информационного терроризма можно обозначить следующим образом:

- Целенаправленное информационное воздействие, имеющее террористическую цель.
- Использование цифровых технологий как основного канала агрессии.

– Манипуляция общественным сознанием, направленная на подрыв доверия к институтам власти.
– Интеграция с другими видами терроризма, в том числе традиционным и кибертерроризмом.

Информационный терроризм представляет собой реальную угрозу общественной стабильности, поскольку воздействует на ключевые элементы общественного сознания, нарушает когнитивные и нормативные ориентиры.

Во-первых, одной из самых острых угроз является дестабилизация социальной среды. Посредством распространения фейковой информации, провокационных видео и манипулятивных сообщений террористические структуры добиваются разжигания паники, недоверия и общественного недовольства. Комиссаров указывает, что даже единичные информационные атаки могут вызвать массовые протесты и усиление социальной напряжённости.

Во-вторых, информационный терроризм способствует радикализации сознания. Это особенно касается молодежи, подверженной воздействию идеологической пропаганды через социальные сети. По мнению автора, «информационное пространство стало основным полем идеологической борьбы, где осуществляется вербовка и формирование радикальных взглядов».

В-третьих, воздействие террористических информационных кампаний подрывает доверие к государственным институтам, правовым системам и средствам массовой информации. Создаётся впечатление всеобщей незащищённости, неэффективности власти и слабости правопорядка. Это, в свою очередь, формирует социальную апатию и правовой нигилизм.

В-четвёртых, через каналы информационного терроризма осуществляется рекрутинг новых участников террористических группировок, чему способствуют псевдорелигиозная риторика, романтизация терроризма и искажённое представление о героизме «борьбы против системы».

Таким образом, научная значимость настоящего исследования обусловлена необходимостью комплексного подхода к пониманию и нейтрализации одной из наиболее актуальных угроз современного мира — терроризма в его информационном измерении.

«Информационный терроризм представляет собой форму деструктивного воздействия, направленного на подрыв стабильности общества посредством информационных каналов» [5]. Среди ключевых целей можно выделить распространение страха, деморализацию населения, провоцирование социальной напряжённости, разрушение доверия к государственным институтам. Кроме того, информационные атаки могут быть направлены на создание паники и искажение общественного восприятия действительности. Ещё одной важной целью является формирование нужного мировоззрения и побуждение к определённым действиям, в том числе противоправным. Через цифровые платформы злоумышленники стремятся управлять общественным сознанием и манипулировать восприятием событий.

Автор отмечает, что наиболее распространёнными методами информационного воздействия являются распространение фейковых новостей, использование провокационного контента, манипуляция фото- и видеоматериалами. Активно применяются технологии фабрикации информации, включая так называемые «фейковые аккаунты», «бот-сети» и системы автоматической генерации контента. Важным инструментом остаются кибератаки, направленные на дестабилизацию функционирования критически важной инфраструктуры и подрыв цифровой безопасности. Значительное внимание уделяется психологическому воздействию через методы троллинга, давления и систематического распространения запугивающих сообщений. Также широко используются мессенджеры и социальные сети для быстрого и неконтролируемого распространения агрессивной или ложной информации.

По мнению автора, информационно-деструктивные воздействия направляются на различные группы населения, учитывая их возрастные, социальные и культурные характеристики. Наиболее уязвимыми часто становятся молодёжь и пожилые граждане, обладающие ограниченным критическим восприятием цифровой информации. Особенности подачи контента подбираются с учётом языковых и визуальных предпочтений целевой аудитории, что усиливает эффект вовлечённости. Отметим, что в отдельных случаях сообщения адресуются конкретным группам с целью дестабилизации их настроений или разжигания конфликтов. Подобная таргетированная стратегия способствует максимальному охвату и повышению уровня воздействия на общественное сознание.

«Согласно позициям, Солдатовой Г.У., Рассказова Е. И. информационный терроризм выступает одной из наиболее опасных форм современных угроз, опирающейся на возможности цифровой среды» [4]. Его особенность заключается в способности незаметно проникать в общественное сознание, манипулировать восприятием и подрывать доверие к ключевым институтам государства. Использование новых технологий, дезинформации и психологического давления делает такие формы воздействия особенно

эффективными и трудноуловимыми. Современное общество сталкивается с постоянным риском информационного вмешательства, которое способно вызвать социальную напряжённость и нарушить стабильность.

Также необходимо совершенствовать законодательную базу, регулирующую вопросы информационной безопасности, обеспечивая баланс между мерами защиты и сохранением демократических принципов. Принятие превентивных мер и внедрение современных технологий защиты позволяет снизить уязвимость информационной среды. Важную роль играет развитие международного сотрудничества, направленного на обмен опытом и согласование подходов к противодействию транснациональным информационным угрозам. Информационный терроризм не признаёт границ, и адекватный ответ возможен лишь при объединении усилий разных стран.

В конечном счёте, устойчивость к информационным атакам формируется не только за счёт технических средств, но и через укрепление общественной сплочённости, доверия и открытого диалога. Только системная работа, сочетающая профилактику, просвещение и правовые механизмы, способна обеспечить безопасность информационного пространства.

Список литературы:

[1] Комиссаров А. И. Противодействие терроризму в условиях цифрового общества // Вестник МГЮА. — 2021. — № 6. — С. 23

[2] Наумов Ю. И. Терроризм в условиях глобализации: проблемы правового регулирования. — М.: Норма, 2019. — С. 45

[3] Рарог А. Н. Уголовно-правовая охрана информационной безопасности // Уголовное право. — 2020. — № 1. — С. 7.

[4] Солдатова Г.У., Рассказова Е.И. Психология цифровой компетентности и уязвимости к деструктивному контенту в сети. – М.: Смысл, 2021. – 288 с.

[5] Петухов Валерий Интернет и «Информационный терроризм» // 2008. №5. URL: https://cyberleninka.ru/article/n/internet-i-informatsionnyy-terrorizm (дата обращения: 16.06.2025).

Spisok literatury:

[1] Komissarov A. I. Protivodejstvie terrorizmu v usloviyax cifrovogo obshhestva // Vestnik MGYuA. — 2021. — № 6. — S. 23

[2] Naumov Yu. I. Terrorizm v usloviyax globalizacii: problemy` pravovogo regulirovaniya. — M.: Norma, 2019. — S. 45

[3] Rarog A. N. Ugolovno-pravovaya oxrana informacionnoj bezopasnosti // Ugolovnoe pravo. — 2020. — № 1. — S. 7.

[4] Soldatova G.U., Rasskazova E.I. Psixologiya cifrovoj kompetentnosti i uyazvimosti k destruktivnomu kontentu v seti. – M.: Smy`sl, 2021. – 288 s.

[5] Petuxov Valerij Internet i «Informacionny`j terrorizm» // 2008. №5. URL: https://cyberleninka.ru/article/n/internet-i-informatsionnyy-terrorizm (data obrashheniya: 16.06.2025).

