УДК 343.9 **DOI: 10.34670/AR.2026.33.72.071**

Терроризм в информационном обществе: новые формы и методы воздействия

Османов Саидбег Магомедсаидович

Аспирант,
Всероссийский государственный университет
юстиции (РПА Минюста России),
117638, Российская Федерация, Москва, ул. Азовская, 2, корп. 1;
e-mail: saidbeg.osmanov@bk.ru

Аннотация

В статье анализируется трансформация терроризма в условиях информационного общества, при которой физическое насилие все в большей степени дополняется символическим, медиатизированным и информационно-психологическим воздействием. Показано, что цифровая среда изменила не только каналы распространения террористических сообщений, но и саму структуру общественного восприятия угрозы: аудитория превращается в участника тиражирования страха, а алгоритмически организованные коммуникации повышают скорость и масштаб резонанса. Делается вывод о том, что в информационном обществе ключевым объектом террористического воздействия становится не только физическая безопасность, но и когнитивная, эмоциональная и нормативная устойчивость общества, а потому эффективное противодействие должно сочетать уголовно-правовые, информационно-правовые, организационные и превентивные меры.

Для цитирования в научных исследованиях

Османов С.М. Терроризм в информационном обществе: новые формы и методы воздействия // Вопросы российского и международного права. 2026. Том 16. № 4А. С. 584-592. DOI: 10.34670/AR.2026.33.72.071

Ключевые слова

Терроризм, информационное общество, цифровая среда, радикализация, информационно-психологическое воздействие, медиатизация насилия, алгоритмическое распространение контента, информационная безопасность, противодействие терроризму, правовое регулирование.

Введение

Терроризм в XXI веке все менее поддается описанию исключительно через категорию непосредственного насилия, поскольку его общественная опасность в условиях информационного общества определяется не только причинением физического вреда, но и способностью производить масштабный символический, психологический и политический эффект. Именно поэтому современный научный анализ все чаще исходит из того, что террористический акт обращен не только против непосредственной жертвы, но прежде всего против массовой аудитории, для которой конструируется состояние уязвимости, неопределенности и страха. Такая постановка вопроса особенно значима в российском правовом контексте, где обеспечение безопасности должно сочетаться с конституционными гарантиями достоинства личности, свободы мысли и слова, права на информацию и допустимыми пределами ограничения прав в целях защиты основ конституционного строя и безопасности государства. В этом смысле терроризм в информационном обществе должен рассматриваться как сложный социально-правовой феномен, в котором акты насилия, коммуникационные технологии и механизмы общественной рецепции образуют единую систему воздействия.

Основная часть

Переход к сетевым моделям коммуникации принципиально изменил среду, в которой функционируют террористические практики. Если в предшествующие периоды основным условием их публичного эффекта было посредничество традиционных медиа, то в цифровой среде распространение образов, лозунгов, интерпретаций и эмоционально заряженных сообщений стало значительно менее зависимым от редакционного фильтра. Концепция сетевого общества М. Кастельса позволяет увидеть в этой трансформации не просто технический сдвиг, а изменение самой логики власти: коммуникационные потоки становятся пространством конкуренции за внимание, легитимность и способность определять рамки интерпретации событий [Шейнов, 2021]. В свою очередь, теория общества риска У. Бека помогает объяснить, почему даже единичный эпизод насилия, будучи многократно воспроизведенным в цифровой среде, начинает восприниматься как повсеместная и постоянно актуальная угроза [Усманов, 2024]. В этих условиях терроризм усиливает свое воздействие не столько за счет роста материальных ресурсов, сколько за счет способности использовать свойства сетевой публичности, где скорость распространения, эмоциональная заразительность и тиражируемость образов оказываются не менее значимыми, чем собственно факт преступления.

Терроризм всегда содержал демонстративный, театрализованный элемент, поскольку его целью является не только причинение вреда, но и посылание сообщения значительно более широкой аудитории, чем круг непосредственных жертв. М.Т. Томич развивает эту линию, рассматривая терроризм как форму коммуникации, в которой насилие функционирует как средство передачи политически нагруженного сигнала [Томич, 2022]. Однако эти подходы нуждаются в уточнении применительно к информационному обществу. Если у Б. Хоффмана «театр» насилия предполагает публичность как условие эффекта [Хоффман, 2003], то в цифровую эпоху сама аудитория становится частью механизма распространения, комментирования и вторичного усиления сообщения. Поэтому коммуникационный аспект

терроризма уже нельзя понимать только как одностороннюю трансляцию. Он становится интерактивным, платформенно опосредованным и алгоритмически структурированным. В этом состоит одно из принципиальных отличий современных форм воздействия: страх больше не распространяется лишь сверху вниз через новостную повестку, он циркулирует горизонтально, многократно переупаковывается и приобретает новые значения в пользовательских сетях.

Значимый аналитический вклад в понимание этой динамики внесла М. Креншоу, настаивавшая на том, что терроризм представляет собой стратегическую адаптацию к политическим ограничениям и ресурсной асимметрии. Ее позиция позволяет объяснить, почему цифровая среда оказалась особенно привлекательной для террористических структур и одиночных радикализированных субъектов: она снижает порог доступа к публичности, облегчает поиск сочувствующей аудитории и позволяет в короткие сроки добиться общественного резонанса, который прежде требовал более сложных организационных форм [Харитонова, 2018]. Вместе с тем теория Д. Рапопорта о «волнах» терроризма показывает и пределы чисто технологических объяснений [Rapoport, 2026]. Современная фаза не отменяет идеологические, религиозные, этнополитические и геополитические основания террористической активности; цифровизация не заменяет мотивацию, но радикально перестраивает способы ее выражения, легитимации и тиражирования. Следовательно, неправомерно сводить проблему к тезису о том, будто интернет сам по себе порождает терроризм. Корректнее говорить о том, что сетевые коммуникации трансформируют инфраструктуру воздействия, а не причинную природу феномена.

Именно здесь показательна дискуссия между Г. Вайманом и М. Конуэй. Вайман убедительно описал интернет как мультипликатор террористической активности, подчеркивая его значение для пропаганды, символического присутствия, поиска сторонников и формирования устойчивых идеологических сообществ [Weimann, 2015]. Конуэй, не отрицая этих эффектов, справедливо предостерегает от технологического детерминизма и указывает, что исследователь должен различать присутствие экстремистского контента в сети и доказанную причинную связь между потреблением такого контента и переходом к насильственному поведению [Conway, 2017]. Этот спор имеет принципиальное значение для права. Если преувеличивать автономную опасность цифровой среды, возникает соблазн чрезмерного расширения запретительных механизмов; если же недооценивать медиативную роль платформ, становится невозможным адекватное регулирование публичного оправдания терроризма, распространения террористической символики и устойчивых практик онлайн-радикализации. В научном плане наиболее обоснованным представляется промежуточный вывод: цифровая среда не заменяет офлайн-факторы радикализации, но создает условия для ускоренного идеологического подкрепления, эмоциональной синхронизации и нормализации насилия в определенных коммуникативных нишах.

Специфика информационного общества проявляется и в том, что формы террористического воздействия смещаются в сторону информационно-психологического давления. Объектом нападения становится не только жизнь и здоровье конкретных лиц, но также чувство коллективной безопасности, доверие к институтам, способность общества отличать факт от интерпретации и устойчивость правопорядка к паническим реакциям. Здесь продуктивны идеи о «информационных коконах» и групповой поляризации: в сегментированных цифровых средах люди чаще сталкиваются с содержанием, подтверждающим их первоначальные установки, а потому риск ускоренного радикального сдвига при наличии предварительных фрустраций

возрастает [Починская, 2025]. Цифровые платформы не являются нейтральными проводниками информации; они задают режим видимости, сортировки и удаления контента. Следовательно, медиатизация терроризма определяется не только действиями самих радикальных акторов, но и устройством коммерческих цифровых экосистем, в которых внимание монетизируется, а приоритет получают яркие, конфликтные и эмоционально насыщенные сообщения. Анализируя логику надзорного капитализма, можно увидеть в этой среде дополнительный риск: поведенческие данные и алгоритмическая персонализация сами по себе не создают террористической угрозы, но могут усиливать адресность и эффективность деструктивного воздействия на восприимчивые аудитории.

Отсюда вытекает необходимость точного разграничения близких, но не тождественных понятий. Терроризм не сводится к экстремизму, хотя может использовать экстремистскую идеологию как средство мобилизации; радикализация не тождественна совершению террористического преступления, хотя в ряде случаев предшествует ему; информационно-психологическое воздействие не всегда носит противоправный характер, но становится общественно опасным, когда направлено на оправдание, пропаганду или нормализацию террористического насилия. Необходимо также отличать террористическую активность в цифровой среде от кибертерроризма в узком смысле, который обычно связывается с посягательством на цифровую инфраструктуру, системы управления и критически важные объекты. В условиях современной медиасреды гораздо чаще наблюдается не высокотехнологичное разрушение инфраструктуры, а коммуникативное использование сети для символического расширения эффекта насилия. Именно поэтому правовое и научное смешение «терроризма в интернете» с «кибертерроризмом» способно дезориентировать как исследователя, так и правоприменителя.

Статистические и эмпирические материалы подтверждают, что цифровизация изменила прежде всего масштаб и дальность общественного резонанса террористических проявлений, а не отменила их зависимость от более широких конфликтных контекстов. Согласно Global Terrorism Index 2024, основная тяжесть смертельных последствий терроризма по-прежнему концентрируется в странах, затронутых вооруженными конфликтами и хронической политической нестабильностью, что указывает на сохраняющуюся связь терроризма с социально-политической дезорганизацией. Вместе с тем в европейских аналитических материалах подчеркивается, что даже при относительно ограниченном числе завершенных атак цифровая среда сохраняет центральное значение для распространения идеологии, самооправдания насилия и трансграничного обращения радикальных нарративов. Для России это означает, что угрозу нельзя оценивать только по числу фактически совершенных террористических актов: значимым индикатором становятся объемы выявления противоправного контента, публичных оправдательных высказываний и попыток вовлечения в деструктивные сообщества, что находит отражение в материалах Национального антитеррористического комитета.

Юридическая реакция на эти процессы в российском праве строится на сочетании конституционных начал, специального антитеррористического законодательства, норм информационного права и уголовно-правовых запретов. Федеральный закон от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» закрепляет систему предупреждения, выявления, пресечения и минимизации последствий террористической деятельности, исходя из того, что противодействие должно носить межведомственный и превентивный характер. Федеральный

закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» создает правовой каркас ограничения доступа к информации, распространение которой запрещено, а также определяет общие параметры взаимодействия государства, операторов и владельцев информационных ресурсов. Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности» важен постольку, поскольку цифровая радикализация нередко разворачивается на стыке экстремистских и террористических нарративов, однако их механическое отождествление недопустимо и влечет риск правовой неопределенности. Уголовный кодекс Российской Федерации содержит специальные составы, охватывающие террористическую деятельность, содействие ей, публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма и его пропаганду, что имеет особое значение именно для цифровой среды, где слово, образ и репост могут становиться самостоятельными носителями общественной опасности.

В то же время сама возможность уголовно-правового вмешательства в сферу публичной коммуникации требует особенно строгого соблюдения принципов определенности, соразмерности и вины. Расширительное толкование таких категорий, как «оправдание», «пропаганда», «призыв», создает риск смещения акцента с реального предотвращения терроризма на чрезмерную криминализацию спорных высказываний. В этом отношении существенное значение имеет судебное толкование, ориентирующее правоприменителя на установление контекста, направленности высказывания, его публичного характера и способности формировать позитивное отношение к террористической деятельности [Постановление Пленума ВС РФ № 1, 2012]. Научная литература справедливо подчеркивает, что эффективность противодействия определяется не количеством ограничительных мер как таковых, а качеством их адресации. Российские специалисты в области информационного права неоднократно указывали, что правовое регулирование цифровой среды не может строиться исключительно на запрете; оно должно учитывать архитектуру информационных отношений, статус субъектов, особенности оборота данных и гарантии прав личности. Иначе борьба с деструктивным контентом рискует вступить в противоречие с базовыми принципами правового государства.

Системные ориентиры такого подхода заданы и в стратегических документах Российской Федерации. Стратегия национальной безопасности относит защиту общества от деструктивного информационного воздействия к числу приоритетов, связывая информационную устойчивость с общим состоянием суверенитета, общественного согласия и правопорядка [Указ Президента РФ № 400, 2021]. Доктрина информационной безопасности, в свою очередь, фиксирует необходимость противодействия использованию информационной сферы в целях подрыва духовно-нравственных ценностей, дестабилизации общественно-политической обстановки и причинения ущерба безопасности личности, общества и государства [Указ Президента РФ № 646, 2016]. Применительно к теме терроризма это означает, что объект охраны расширяется: речь идет не только о пресечении конкретных преступлений, но и о сохранении устойчивости общественного сознания к манипулятивным и деструктивным воздействиям. Однако здесь важно избежать неопределенности понятийного аппарата. Категория «деструктивное информационное воздействие» полезна на уровне стратегии, но в правоприменении она должна быть переведена на язык четко установленных юридических признаков, иначе возрастает риск произвольного ограничения законной коммуникации.

Международный уровень регулирования подтверждает ту же тенденцию. Глобальная

контртеррористическая стратегия ООН исходит из необходимости сочетать меры безопасности с защитой прав человека и устранением условий, способствующих распространению терроризма. Это особенно важно в цифровой среде, где трансграничность платформ, различия национальных юрисдикций и скорость распространения контента объективно затрудняют правоприменение. Российская практика, как и зарубежная, сталкивается с проблемой того, что вредоносный контент может быть создан в одной стране, размещен на инфраструктуре другой, адресован аудитории третьей и воспроизводиться пользователями без прямой связи с первоначальным источником. В результате борьба с терроризмом приобретает выраженный координационный характер и требует не только уголовно-правовых запретов, но и процедур оперативного обмена информацией, взаимодействия с цифровыми посредниками, совершенствования судебной и экспертной практики.

Отдельного внимания заслуживает вопрос об онлайн-радикализации. В научной среде постепенно укрепляется позиция, согласно которой радикализация не представляет собой линейный, одинаковый для всех путь от потребления определенного контента к совершению преступления. На это указывают и М. Конуэй, и М. Креншоу: цифровая среда может ускорять включение человека в идеологически насыщенные сообщества, но решающую роль обычно играют сочетания личных кризисов, социальной изоляции, групповой динамики, политической фрустрации и поиска идентичности. Следовательно, правоохранительная и профилактическая политика должна избегать примитивной модели, в которой любой контакт с радикальным дискурсом автоматически трактуется как близость к террористической деятельности. Более продуктивным представляется риск-ориентированный подход, учитывающий совокупность поведенческих и контекстуальных признаков, но не превращающий профилактику в тотальный контроль над мировоззренческой сферой.

С учетом сказанного наиболее существенными новыми формами и методами воздействия терроризма в информационном обществе следует признать не технически сложные, а коммуникативно эффективные практики: создание эффекта повсеместной угрозы, символическое завоевание внимания, эксплуатацию визуальной шоковости, внедрение оправдательных нарративов, адресную работу с уязвимыми аудиториями, а также провоцирование вторичной общественной реакции в виде паники, стигматизации, взаимного недоверия и давления на государственные институты. Их особенность состоит в том, что они действуют опосредованно: непосредственный ущерб может быть локальным, а социально-психологический эффект – национальным или глобальным. По существу, терроризм в цифровую эпоху стремится захватить не территорию, а повестку; не только причинить вред, но и навязать обществу режим постоянного тревожного ожидания. В этом отношении новые формы воздействия тесно связаны с медиалогикой информационного общества, где ценность события определяется не только его содержанием, но и способностью к вирусному воспроизводству.

Следовательно, эффективное противодействие не может быть исчерпано удалением контента и уголовным преследованием. Не менее значимы повышение цифровой, правовой и финансовой грамотности [Восканян, 2021], развитие критического восприятия информации, подготовка специалистов по судебной лингвистике и психологии цифровой коммуникации, совершенствование процедур межведомственного обмена данными, а также формирование транспарентных стандартов взаимодействия государства с платформами. При этом превенция должна носить правовой, а не произвольный характер: каждое ограничение доступа к

информации, каждая квалификация высказывания как оправдывающего терроризм, каждое вмешательство в частную коммуникацию должны быть соразмерны, проверяемы и основаны на законе. Только при соблюдении этих условий противодействие терроризму сохраняет легитимность и не воспроизводит ту самую атмосферу страха и недоверия, с которой оно призвано бороться.

Заключение

Таким образом, в информационном обществе терроризм трансформируется из феномена, ориентированного преимущественно на физическое устрашение, в многоуровневую систему медиатизированного воздействия, использующую свойства сетевой коммуникации, алгоритмической видимости и цифровой повторяемости. Сравнение научных подходов показывает, что современный терроризм нельзя объяснить ни только идеологией, ни только технологией: он возникает на пересечении конфликтных социальных условий, стратегической адаптации радикальных акторов и специфики цифровой публичности. Для российского права это означает необходимость точного нормативного разграничения смежных явлений, укрепления доказательных стандартов, сохранения конституционного баланса между безопасностью и свободой, а также развития комплексной профилактики, направленной не только на пресечение преступлений, но и на повышение устойчивости общества к информационно-психологическому воздействию. Именно эта устойчивость становится сегодня одним из ключевых критериев национальной и информационной безопасности.

Библиография

1. Восканян Р.О. Роль цифрового образования в обеспечении экономического роста // Азимут научных исследований: экономика и управление. 2021. Т. 10, № 2(35). С. 136–139.
2. Постановление Пленума Верховного Суда Российской Федерации от 9 февраля 2012 г. № 1 «О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности» // Бюллетень Верховного Суда Российской Федерации. 2012. № 4.
3. Починская Д.А. Характер влияния новых медиа на общественное мнение // Вестник науки. 2025. Т. 4, № 6(87). С. 985–993.
4. Томич М.Т. Коммуникационные аспекты терроризма как феномена безопасности // Мировой политический процесс: информационные войны и «цветные революции» : сборник материалов Международной научно-практической конференции, Москва, 27–29 октября 2021 года. М.: Московский государственный лингвистический университет, 2022. С. 265–281.
5. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» // Официальный интернет-портал правовой информации pravo.gov.ru.
6. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации pravo.gov.ru.
7. Усманов Г.Р. Концепция «общества риска» Ульриха Бека: теоретический анализ // Вестник экономики, права и социологии. 2024. № 2. С. 247–250.
8. Харитонова О.Г. Изучая терроризм: Основные контуры дискуссии // Политическая наука. 2018. № 4. С. 13–33.
9. Хоффман Б. Терроризм – взгляд изнутри / пер. с англ. Е. Сажиной. М.: Ультра. Культура, 2003. 256 с.
10. Шейнов Т.Г. Понятие власти в концепции сетевого общества Мануэля Кастельса // Философия. Политология (МНСК-2021) : материалы 59-й Международной научной студенческой конференции, Новосибирск, 12–23 апреля 2021 года. Новосибирск: Новосибирский национальный исследовательский государственный университет, 2021. С. 31–33.
11. Conway M. Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research // Studies in Conflict & Terrorism. 2017. Vol. 40, No. 1. P. 77–98.
12. Rapoport D. The Four Waves of Modern Terrorism. – URL: http://www.international.uda.edu/cms/files/Rapoport-Four-Waves-of-Modem-Terrorism.pdf .

13. Weimann G. Terrorism in Cyberspace: The Next Generation. Washington, D.C.: Woodrow Wilson Center Press, 2015. 296 p.

Terrorism in the Information Society: New Forms and Methods of Influence

Saidbeg M. Osmanov

Postgraduate Student,
All-Russian State University of Justice
(RPA of the Ministry of Justice of Russia),
117638, 2, bldg. 1, Azovskaya str., Moscow, Russian Federation;
e-mail: saidbeg.osmanov@bk.ru

Abstract

The article analyzes the transformation of terrorism in the context of the information society, in which physical violence is increasingly supplemented by symbolic, mediatized, and information-psychological influence. It is shown that the digital environment has changed not only the channels for disseminating terrorist messages but also the very structure of public perception of the threat: the audience turns into a participant in the replication of fear, and algorithmically organized communications increase the speed and scale of resonance. A conclusion is drawn that in the information society, the key object of terrorist influence becomes not only physical security but also the cognitive, emotional, and normative stability of society, and therefore effective counteraction must combine criminal-legal, information-legal, organizational, and preventive measures.

For citation

Osmanov S.M. (2026) Terrorizm v informatsionnom obshchestve: novye formy i metody vozdeystviya [Terrorism in the Information Society: New Forms and Methods of Influence]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 16 (4A), pp. 584-592. DOI: 10.34670/AR.2026.33.72.071

Keywords

Terrorism, information society, digital environment, radicalization, information-psychological influence, mediatization of violence, algorithmic content distribution, information security, countering terrorism, legal regulation.

References

1. Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism,* 40(1), 77-98.
2. Decree of the President of the Russian Federation No. 646 of December 5, 2016 "On Approval of the Information Security Doctrine of the Russian Federation". (2016). *Official Internet Portal of Legal Information pravo.gov.ru*.
3. Decree of the President of the Russian Federation No. 400 of July 2, 2021 "On the National Security Strategy of the Russian Federation". (2021). *Official Internet Portal of Legal Information pravo.gov.ru*.
4. Kharitonova, O. G. (2018). Izuchaya terrorizm: Osnovnye kontury diskussii [Studying terrorism: Main contours of the discussion]. *Politicheskaya nauka*, 4, 13-33.
5. Hoffman, B. (2003). *Terrorizm – vzglyad iznutri* [Terrorism – a view from the inside] (E. Sazhina, Trans.). Moscow: Ultra. Kultura.

6. Pochinskaya, D. A. (2025). Kharakter vliyaniya novykh media na obshchestvennoe mnenie [The nature of the influence of new media on public opinion]. *Vestnik nauki*, 4(6), 985-993.
7. Rapoport, D. (2026). *The four waves of modern terrorism.* Retrieved from http://www.international.uda.edu/cms/files/Rapoport-Four-Waves-of-Modem-Terrorism.pdf
8. Resolution of the Plenum of the Supreme Court of the Russian Federation No. 1 of February 9, 2012 "On Certain Issues of Judicial Practice in Criminal Cases Concerning Terrorist-Related Crimes". (2012). *Bulletin of the Supreme Court of the Russian Federation*, 4.
9. Sheynov, T. G. (2021). Ponyatie vlasti v kontseptsii setevogo obshchestva Manuelya Kastelsa [The concept of power in Manuel Castells' concept of the network society]. In *Filosofiya. Politologiya (MNSK-2021)* (pp. 31-33). Novosibirsk: Novosibirsk National Research State University.
10. Tomich, M. T. (2022). Kommunikatsionnye aspekty terrorizma kak fenomena bezopasnosti [Communication aspects of terrorism as a security phenomenon]. In *Mirovoy politicheskiy protsess: informatsionnye voyny i "tsvetnye revolyutsii"* (pp. 265-281). Moscow: Moscow State Linguistic University.
11. Usmanov, G. R. (2024). Kontseptsiya "obshchestva riska" Ulricha Beka: teoreticheskiy analiz [Ulrich Beck's concept of "risk society": A theoretical analysis]. *Vestnik ekonomiki, prava i sotsiologii*, 2, 247-250.
12. Voskanyan, R. O. (2021). Rol tsifrovogo obrazovaniya v obespechenii ekonomicheskogo rosta [The role of digital education in ensuring economic growth]. *Azimut nauchnykh issledovaniy: ekonomika i upravlenie*, 10(2), 136-139.
13. Weimann, G. (2015). *Terrorism in cyberspace: The next generation*. Washington, D.C.: Woodrow Wilson Center Press.