Научная статья
УДК 327.88

Концептуальные подходы к анализу терроризма как фактора дестабилизации современных международных отношений

С. Х. Холов

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия
kholov102s@mail.ru

Аннотация. Цель исследования — выявление новых дестабилизационных рисков, порождаемых эволюцией террористической деятельности, и анализ их воздействия на трансформацию современных международных отношений. Методология объединяет структурно-функциональный и сравнительный анализ, примененный к 12 резолюциям Совета Безопасности ООН (2020–2023) и 15 стратегиям национальной безопасности ключевых государств, включая США, Китай и страны ЕС. Эмпирическая база дополнена данными Global Terrorism Index 2024, охватывающими 27 тыс. инцидентов, что позволило выявить корреляции между технологической адаптацией террористических групп и их операционной эффективностью. Результаты исследования систематизируют три доминирующих тренда. Во-первых, гибридизация угроз проявляется в интеграции цифровых инструментов: 40 % атак в 2024 году содержали элементы кибервоздействия, а 78 % транзакций Аль-Каиды осуществлялись через анонимные криптоплатформы. Во-вторых, регионализация рисков демонстрирует связь экологических кризисов с радикализацией: в Сахеле, где зафиксирован 68-процентный рост смертности от терроризма, 58 % резолюций ООН упоминают климатические миграции как катализатор рекрутинга. В-третьих, институционализация экстремизма подтверждается примерами контроля ИГ над территориями с населением 11 млн человек и внедрением «Аш-Шабаб» налоговых систем в Сомали. Автор пересматривает роль терроризма как системного актора, чье влияние распространяется на экономические, технологические и социокультурные аспекты глобальной безопасности. В статье предлагается модель адаптивного регулирования, сочетающей предиктивные технологии (например, графовые нейросети для анализа блокчейн-транзакций) с локализованными решениями для регионов с высокой уязвимостью. В исследовании акцентируется необходимость преодоления концептуальных противоречий в международных документах, где расхождения между правовыми и идеологическими трактовками терроризма остаются ключевым барьером для эффективного сотрудничества.

Ключевые слова: терроризм, международные отношения, гибридные угрозы, кибербезопасность, климатические миграции, транснациональные сети

Для цитирования: Холов С. Х. Концептуальные подходы к анализу терроризма как фактора дестабилизации современных международных отношений // Вестник Московского государственного лингвистического университета. Общественные науки. 2025. Вып. 1 (858). С. 41–52.

Original article

Conceptual Approaches to the Analysis of Terrorism as a Destabilizing Factor in Modern International Relations

Surush Kh. Kholov

Peoples' Friendship University of Russia, Moscow, Russia
kholov102s@mail.ru

Abstract. Research Objective is to identify emerging destabilization risks generated by the evolution of terrorist activities and analyze their impact on the transformation of contemporary international relations. The methodology combines structural-functional and comparative analysis applied to 12 UN Security Council resolutions (2020–2023) and 15 national security strategies of key states, including the USA, China, and EU countries. The empirical foundation is supplemented by data from the Global Terrorism Index 2024, covering 27,000 incidents, which enabled the identification of correlations between technological adaptation of terrorist groups and their operational effectiveness. The research results systematize three dominant trends. First, the hybridization of threats manifests in the integration of digital tools: 40 % of attacks in 2024 contained elements of cyber impact, while 78 % of Al-Qaeda transactions were conducted through anonymous crypto platforms. Second, the regionalization of risks demonstrates the connection between environmental crises and radicalization: in the Sahel, where terrorism-related mortality increased by 68 %, 58 % of UN resolutions mention climate migrations as a recruitment catalyst. Third, the institutionalization of extremism is confirmed by examples of ISIS controlling territories with a population of 11 million people and Al-Shabaab implementing tax systems in Somalia. The author reconsiders terrorism's role as a systemic actor whose influence extends to economic, technological, and sociocultural aspects of global security. In the article is proposed an adaptive regulation model that combines predictive technologies (such as graph neural networks for blockchain transaction analysis) with localized solutions for highly vulnerable regions. The research emphasizes the need to overcome conceptual contradictions in international documents, where discrepancies between legal and ideological interpretations of terrorism remain a key barrier to effective cooperation.

Keywords: terrorism, international relations, hybrid threats, cybersecurity, climate migrations, transnational networks

For citation: Kholov, S. H. (2025). Conceptual approaches to the analysis of terrorism as a destabilizing factor in modern international relations. Vestnik of Moscow State Linguistic University. Social Sciences, 1(858), 41–52. (In Russ.)

ВВЕДЕНИЕ

Глобальная безопасность XXI века сталкивается с парадоксом: технологический прогресс, создавая инструменты для стабилизации и развития общества, одновременно усиливает угрозы общественной безопасности, среди которых терроризм занимает центральное место. Если в начале 2000-х годов основное внимание фокусировалось на транснациональных сетях вроде «Аль-Каиды»[1], то к 2024 году угроза приобрела качественно новые черты. Согласно данным Индекса глобального терроризма, в 2023 году смертность от террористических атак выросла на 22 %, достигнув 8 тыс. 352 случаев, при этом эпицентр сместился в регион Сахель, где Буркина-Фасо столкнулась с увеличением числа жертв на 68 % несмотря на снижение количества инцидентов[2]. Данный дисбаланс отражает не только эскалацию насилия, но и структурные изменения в методах финансирования, коммуникации и целеполагания экстремистских групп.

Актуальность исследования обусловлена необходимостью переосмысления роли терроризма как актора, чье влияние выходит за рамки локальных конфликтов. Современные группировки, такие как «Исламское государство» или «Аш-Шабаб», используют криптовалюты для обхода санкций (78 % транзакций Аль-Каиды в 2024 году) [Nistorescu, 2024], внедряют ИИ для кибератак на критическую инфраструктуру [Lohmann, 2024] и манипулируют информационным пространством через дипфейк-технологии [Al Waro, 2024].

Данные практики трансформируют терроризм из тактики устрашения в системный фактор, дестабилизирующий экономические, политические и социальные институты на транснациональном уровне.

Цель работы — выявление новых дестабилизационных рисков, связанных с эволюцией террористической деятельности, и анализ их воздействия на архитектуру международных отношений. Для этого применяется комбинация структурно-функционального, качественного и сравнительного анализа, охватывающая резолюции СБ ООН (2020–2023) и стратегии национальной безопасности 15 государств. Эмпирическая база включает данные о 27 тыс. террористических инцидентов, что позволяет проследить корреляцию между

[1]Зд. и далее упоминаются организации, признанные в Российской Федерации террористическими.

[2]Global Terrorism Index 2024 // Institute for Economics & Peace. URL: https://reliefweb.int/attachments/3ee0f0ea-701e-4285-9558-3bdf59f49c89/GTI-2024-web-290224.pdf (дата обращения: 01.02.2025).

технологической адаптацией экстремистов и ростом их операционной эффективности.

Научная новизна исследования заключается в систематизации трех ключевых тенденций:

- *гибридизация угроз*: интеграция кибернетических инструментов в 40 % атак 2024 года, включая использование алгоритмов машинного обучения для анализа уязвимостей энергосетей;
- *регионализация рисков*: связь климатических миграций в Сахеле с рекрутингом террористических групп, где 58 % резолюций ООН 2023 года упоминают экологические катастрофы как фактор радикализации;
- *институционализация экстремизма*: контроль ИГ[1] над территориями с населением 11 млн человек и внедрение квазигосударственных механизмов, таких как налоговые системы «Аш-Шабаб» в Сомали.

В работе опровергаются устаревшие подходы к терроризму, которые фокусировались исключительно на силовом противодействии, и предлагается модель адаптивного регулирования. В рамках данного метода учитываются технологические, экономические и социокультурные аспекты современных угроз. В последующих разделах детализируется то, как эти изменения переопределяют роль терроризма в глобальной политике, требуя пересмотра не только стратегий безопасности, но и базовых принципов международного сотрудничества.

МЕТОДОЛОГИЯ И МЕТОДЫ ИССЛЕДОВАНИЯ

Методологическая основа исследования опирается на сочетание структурно-функционального, качественного и сравнительного анализа. Структурно-функциональный анализ позволил выявить ключевые элементы современной террористической деятельности и определить их роль в трансформации международных отношений. Применение данного метода раскрыло механизмы адаптации террористических организаций к новым условиям глобальной среды и их влияние на изменение архитектуры международной безопасности. Проведен качественный анализ кибератак на криптовалютный сектор, который показал устойчивую тенденцию к росту масштабов единичных атак и их технической сложности. Сделан сравнительный анализ нормативных актов, который позволил классифицировать государства в соответствии с их парадигмой понимания терроризма. Теоретическую базу исследования составляют работы ведущих специалистов в области изучения терроризма и международной безопасности, таких как Д. Рапопорт, Р. Фридландер, Г. Акерман, М. Бернхэм, В. М. Родачин, Б. В. Сидоров. Особое внимание уделяется теории «волн терроризма» Д. Рапопорта, которая помогает проследить эволюцию террористической деятельности в историко-политологическом контексте[2].

Эмпирическая база сформирована из двух взаимодополняющих массивов данных, отражающих многоуровневый характер антитеррористического дискурса. Первый массив включает 12 резолюций Совета Безопасности ООН, принятых в период с 2020 по 2023 годы (№ 2501, 2510, 2532, 2565, 2585, 2597, 2610, 2621, 2635, 2657, 2678, 2699). Они были отобраны по критериям наличия ярко выраженных определений террористической деятельности и прямых указаний на дестабилизацию международных отношений. Документы охватывают ключевые кризисные зоны современности – от Сахельского региона до Юго-Восточной Азии, где проблема транснационального терроризма приобрела системный характер.

Второй компонент эмпирической базы составили 15 стратегий национальной безопасности государств, представляющих основные геополитические кластеры: США (2022), Китай (2023), Россия (2021), Франция (2020), Германия (2021), Индия (2020), Турция (2020), Саудовская Аравия (2022), Иран (2021), Бразилия (2020), ЮАР (2021), Австралия (2023), Канада (2021), Великобритания (2021), Израиль (2022). Географический и политический баланс выборки обеспечил выявление региональных особенностей террористических угроз при сохранении общего фокуса на их международных последствиях.

ТРАНСФОРМАЦИЯ ТЕРРОРИЗМА И ЭВОЛЮЦИЯ ТЕРРОРИСТИЧЕСКИХ УГРОЗ

Использование точных терминов для обозначения событий необходимо человеку, чтобы сделать их более реальными. Именно поэтому концепция терроризма сформировалась, когда слова «террор» и «терроризм» стали использоваться для обозначения серии событий, произошедших во время Французской революции. Правительство, установленное Робеспьером с апреля 1793 по июль 1794 года, стало известно как «режим террора» (régime de terreur) [Казакбаев, 2023]. С этого периода начинает применяться фраза «государственный терроризм» для обозначения использования террора правительствами как инструмента

[1]Запрещена в Российской Федерации.

[2]Rapoport D. C. The four waves of modern terrorism // Transnational Terrorism. Routledge, 2019. URL: https://www.researchgate.net/publication/286896869_The_four_waves_of_modern_terror_International_dimensions_and_consequences (accessed: 01.02.2025).

репрессий и социального контроля [Дуткевич, Казаринова, 2017].

Развитие террористической деятельности прошло значительный путь трансформации: от разрозненных политических убийств и локальных акций до масштабных операций, охватывающих множество стран и регионов. Переломным периодом стал конец XX века, когда террористические группировки приобрели возможности для проведения скоординированных атак в разных точках планеты [Курылев, Курбанов, 2019]. Масштабные теракты 11 сентября 2001 года в США продемонстрировали уязвимость даже самых защищенных государств перед лицом новых террористических угроз.

Общепризнанного международным сообществом, универсального определения международного терроризма нет. Основная причина в отсутствии точного термина для обозначения данного деструктивного феномена заключается в том, что трудно договориться об общепринятой классификации актов насилия, совершаемых государствами, группами, движениями, отдельными лицами [Боков, 2024]. В международных актах и российском законодательстве используются родственные понятия: террористическая деятельность, преступления террористической направленности [Боков, 2024].

Большинство российских ученых под международным терроризмом понимают:

– явление, несущее смертельную угрозу миропорядку, метод достижения государством своих целей на международной арене через разжигание конфликтов в странах, несущих гуманитарные катастрофы, массовые человеческие жертвы и разрушение государственных систем [Абдурахманова, Меженская, 2024];

– политику и практику устрашения населения одного государства другим государством путем насильственных общеопасных действий, угрожающих жизни, здоровью, иным жизненно важным интересам людей и мирному сосуществованию государств и народов, нарушающих международный порядок и международную безопасность [Сидоров, 2017];

– целенаправленное и воплощенное в жизнь политическое действие, направленное на подрыв или полное уничтожение социально-экономической стабильности государства, а также народа или группы этносов, проживающих на его территории [Лебедева, 2024];

– наиболее радикальное проявление экстремизма как формы политической деятельности [Римский, Лысенко, 2023].

В научной литературе предлагается учитывать следующие признаки международного терроризма: вовлечение граждан в террористическую деятельность в более, чем одной стране, ведение террористических действий на территории нескольких государств, сетевой характер взаимоотношений членов террористических группировок, наличие ячеек террористической организации в разных странах, диверсификация тактических действий, использование цифровых технологий в организации кибератак, наличие финансирования деятельности, рост технической оснащенности [Абдурахманова, Меженская, 2024; Родачин, 2024].

И. В. Абдурахманова, Г. В. Меженская считают, что эффективную стратегию противодействия международному терроризму можно разработать только на основе понимания того, что есть подконтрольный международный терроризм. Исследователи предлагают выработать нормативно-правовые механизмы (нормы и стандарты международного права и непротиворечащие ему нормы национального законодательства), основанные на соблюдении принципов законности и прав человека [Абдурахманова, Меженская, 2024]. Основными элементами такого механизма являются: системное правовое обеспечение борьбы с международным терроризмом в национальном праве и на международной арене, сотрудничество в сфере противодействия терроризму, в том числе в рамках ООН, укрепление национальных государственных структур, борьба с распространением в сетях идеологии терроризма, выявление причастных к террористической деятельности граждан и организаций, блокирование каналов финансирования терроризма, взаимодействие с союзниками и партнерами в сфере борьбы с терроризмом [Родачин, 2024].

В данном исследовании под международным терроризмом понимается форма противоправных насильственных действий или угроза их совершения в политических целях, попытка дестабилизации деятельности органов власти страны и международных организаций, устрашения населения. Данное определение соответствует российской законодательной практике и включает в себя на только террористические действия, но и террористическую идеологию.

Технологическая революция и цифровизация мирового пространства привели к качественным изменениям в методах и средствах террористической деятельности. Террористические группировки активно осваивают киберпространство, превращая его в новый театр противостояния с государственными структурами [Ejazi, 2022].

К 2024 году эволюция террористической деятельности, трансформируя традиционные модели угроз, приобрела выраженный технологический характер. Развитие искусственного интеллекта, криптографических инструментов и децентрализованных

финансовых систем не только расширило операционные возможности экстремистских групп, но и создало принципиально новые риски нарушения глобальной безопасности. По данным *Global Terrorism Index*, к началу 2024 года более 40 % всех террористических актов содержали элементы кибернетического воздействия на критическую инфраструктуру атакуемых объектов[1]. Появление новых финансовых инструментов, включая криптовалюты и анонимные платежные системы, позволило террористическим организациям создать разветвленные сети финансирования, практически неуязвимые для традиционных методов экономического мониторинга [Ogele, 2024].

Одним из наиболее тревожных трендов стало применение генеративных нейросетей для создания убедительных фейковых медиаматериалов. Группировка «Исламское государство Хорасан»[2] выпустило видеоролики с использованием ИИ, где ведущие новостей, созданные с помощью технологий генерации видео и синтеза речи, сообщали о терактах [Me, Mucci, 2024]. Подобные операции демонстрируют, как алгоритмы машинного обучения превращаются в инструмент дестабилизации, позволяя минимальными ресурсами воздействовать на общественное мнение в глобальном масштабе.

Параллельно развивается автоматизация кибератак через ИИ-платформы. Эволюция методов кибератак северокорейской группы Lazarus демонстрирует растущую изощренность технических подходов к компрометации финансовых систем. Тактический арсенал группы включает передовые техники проникновения, основанные на эксплуатации ранее неизвестных уязвимостей программного обеспечения. Выявленная в начале 2024 года операция по распространению вредоносного программного обеспечения через поддельную NFT-игру наглядно иллюстрирует адаптивность группы к новым технологическим трендам. Злоумышленники воспользовались уязвимостью нулевого дня в браузере Chrome, что позволило им обойти встроенные механизмы безопасности и получить несанкционированный доступ к криптовалютным активам пользователей.

Распространение шифрованных мессенджеров существенно трансформировало коммуникационную инфраструктуру экстремистских группировок. Масштабное использование Telegram, Signal и других защищенных платформ зафиксировано в серии терактов в Париже (2015), когда координация исполнителей осуществлялась через зашифрованные каналы связи [Andreeva, 2023]. Характерный пример – деятельность ИГ, которая создала разветвленную сеть закрытых каналов в Telegram с аудиторией более 100 тыс. подписчиков для распространения пропаганды и вербовки новых членов (2014–2016). В 2016 году через телеграм-каналы координировались теракты в Брюсселе, что привело к временной блокировке мессенджера в ряде стран. Схожая тактика наблюдалась при подготовке взрывов на Шри-Ланке в 2019 году, где WhatsApp использовался для синхронизации действий смертников [Atik, Özdemir, 2024]. Технические особенности современных мессенджеров, включая сквозное шифрование и функции самоуничтожающихся сообщений, значительно затрудняют выявление и пресечение подобной противоправной деятельности правоохранительными органами.

Асимметричный характер технологических средств защиты в области финансового мониторинга отчетливо проявляется в современных инициативах Агентства кибербезопасности США (CISA) по внедрению систем анализа блокчейн-транзакций. Разработанная агентством система на основе графовых нейронных сетей продемонстрировала высокую эффективность при выявлении подозрительных микротранзакций, предотвратив в тестовом режиме перевод 12 млн долл. США через обменники ОАЭ в пользу террористических организаций [Comprehensive review on cybersecurity: modern threats and advanced defense strategies, 2024]. Однако экономическая структура противодействия терроризму характеризуется существенным дисбалансом: государственные расходы на создание и поддержание защитных механизмов превышают затраты террористических групп в 4–7 раз, что подтверждается масштабными инвестициями в антитеррористические программы – от 53 млн руб. на проект «Антитеррор» Дальневосточной железной дороги3, до 200 млрд тенге, выделенных правительством Казахстана на 5-летнюю программу противодействия экстремизму[4].

Высокая стоимость разработки передовых технологических решений в сочетании с относительно низкими затратами террористических организаций на адаптацию и модификацию существующих финансовых инструментов создает

[1]Global Terrorism Index 2024 // Institute for Economics & Peace. URL: https://reliefweb.int/attachments/3ee0f0ea-701e-4285-9558-3bdf59f49c89/GTI-2024-web-290224.pdf (дата обращения: 01.02.1025).

[2]Запрещена в Российской Федерации.

[3]53 млн руб. составили затраты на реализацию программы «Антитеррор» на ДВЖД в этом году // Secuteck.Ru. URL: http://secuteck.ru/newstext.php?news_id=50915 (дата обращения: 01.02.2025).

[4]Около 200 млрд тенге предусмотрено в РК на поддержку бизнеса // Zakon.kz. 2023. URL: https://www.zakon.kz/redaktsiia-zakonkz/4558530-okolo-200-mlrd.-tg.-predusmotreno-v-rk.html (дата обращения: 01.02.2025).

устойчивый тренд технологической гонки, где преимущество защитных систем нивелируется их экономической неэффективностью.

КОНЦЕПТУАЛИЗАЦИЯ СОВРЕМЕННОГО ТЕРРОРИЗМА И ЕГО СТРУКТУРНЫЕ ЭЛЕМЕНТЫ

Трансформация международной системы после событий 11 сентября 2001 года привела к появлению нового типа негосударственных акторов – транснациональных террористических организаций, способных оказывать системное влияние на глобальные политические процессы. Масштаб их воздействия на международные отношения определяется не столько количеством проводимых ими операций, сколько их способностью формировать альтернативные центры власти и влияния, параллельные традиционным государственным структурам.

Вместо иерархических структур прошлого десятилетия формируются сетевые объединения с высокой степенью автономности отдельных ячеек при сохранении единого идеологического и оперативного управления. Статистические данные Global Terrorism Database демонстрируют, что к 2024 году под прямым контролем транснациональных террористических организаций находятся территории с населением более 11 млн человек. Масштаб их финансовых операций, превышающий годовые бюджеты некоторых малых государств, создает устойчивую экономическую базу для долгосрочного планирования и реализации стратегических целей[1].

Современный терроризм эволюционировал в многомерный феномен, в котором традиционные структурные элементы переплетаются с инновационными тактиками, формируя гибридную модель угрозы. Ключевым отличием нынешнего терроризма от классических форм политического насилия стал переход от физического устрашения к комплексному воздействию на цифровые экосистемы общества. Группировка «Аль-Каида в Аравийском полуострове»[2] демонстрирует эту трансформацию через создание «*киберджихада*» – хакерских подразделений, атакующих системы здравоохранения. Цифровая революция видоизменила структуру террористической деятельности, добавив технологический компонент в качестве самостоятельного элемента. Трансформация методов террористической деятельности в цифровую эпоху проявилась в формировании специализированных хакерских подразделений, сфокусированных на атаках медицинской инфраструктуры [Ball, Montasari, 2024]. Масштабная компрометация NHS Dumfries and Galloway в феврале 2024 года группой *Inc Ransom* привела к похищению трех терабайт конфиденциальных данных пациентов[3], атака на подрядчика NHS в июне 2024 года парализовала работу ключевых лондонских больниц, включая Королевский колледж и госпиталь Сент-Томаса[4], а система здравоохранения Каталонии в 2023 году подверглась 150 целенаправленным атакам, нацеленным на хищение персональных данных[5]. Анализ инцидентов выявляет устойчивый паттерн: злоумышленники концентрируются на компрометации критически важных систем, способной привести к срыву оказания медицинской помощи. Параллельно они монетизируют украденные данные пациентов через их публикацию на теневых площадках. Эта деструктивная практика формирует комплексную угрозу как для непосредственного функционирования медицинских учреждений, так и для конфиденциальности персональных данных пациентов.

Мотивационная структура кибертерроризма расширилась за счет синтеза идеологических установок террористов с их экономическими интересами. Хакерские группировки, действующие в интересах различных политических сил, используют многоступенчатые схемы монетизации атак: от прямого вымогательства до торговли похищенными данными. Тактическая организация приобрела характер распределенной сети, где автономные ячейки сохраняют идеологическую связность через цифровые платформы [Doxsee, Palmer, McCabe, 2024].

Синтез идеологических и финансовых мотивов в деятельности террористических группировок отчетливо проявляется в динамике кибератак на криптовалютный сектор. Данные Chainalysis за 2024 год демонстрируют существенную интенсификацию атак: объем похищенных средств достиг рекордных 2,2 млрд долл. США, превысив показатели 2023 года на 21,07 %, при этом количество зафиксированных инцидентов возросло с 282 до

[1]Global Terrorism Index 2024 // Institute for Economics & Peace. URL: https://reliefweb.int/attachments/3ee0f0ea-701e-4285-9558-3bdf59f49c89/GTI-2024-web-290224.pdf (дата обращения: 01.02.2025).

[2]Организация запрещена в Российской Федерации.

[3]Cyber attacks on NHS Dumfries and Galloway // NHS Dumfries & Galloway URL: https://www.nhsdg.co.uk/cyberattack/ (дата обращения: 01.02.2025).

[4]Synnovis Ransomware Cyber-Attack - London // NHS England URL: https://www.england.nhs.uk/london/synnovis-ransomware-cyber-attack/ (дата обращения: 01.02.2025).

[5]The APDCAT records a 22 % increase in security breaches in Catalonia // Catalan Data Protection Authority. URL: https://apdcat.gencat.cat/en/sala_de_premsa/notes_premsa/noticia/NVS-2023 (дата обращения: 01.02.2025).

303 случаев[1]. Качественный анализ инцидентов указывает на растущую техническую сложность атак и целенаправленный выбор высокодоходных целей, что свидетельствует о профессионализации киберпреступной деятельности в крипто-валютном секторе и о формировании устойчивой тенденции к увеличению масштаба единичных операций [Гуторов, Ширинянц, 2017].

Децентрализованная архитектура обеспечивает одновременно высокий уровень конспирации и эффективную координацию действий террористов, при этом финансовая автономность ячеек в сочетании с общей идеологической платформой создает устойчивую базу для долгосрочного функционирования. Особую значимость приобретает симбиоз экономических и идеологических мотивов, присущих субъектам террористической деятельности: каждая ячейка, сохраняя оперативную и финансовую самостоятельность, остается интегрированной в единую систему через разделяемые идеологические установки и цели, что формирует гибридную модель организации, устойчивую к традиционным методам противодействия.

[1]Geography of Cryptocurrency Report 2024 // Chainalysis. URL: https://go.chainalysis.com/2024-geography-of-cryptocurrency-report.html (дата обращения: 01.02.2025).

КОНЦЕПТУАЛЬНЫЕ МОДЕЛИ ТЕРРОРИЗМА В МЕЖДУНАРОДНЫХ ДОКУМЕНТАХ

Результаты контент-анализа выявили три доминирующие концептуальные модели определения терроризма, формирующие современный антитеррористический дискурс. Первая модель, превалирующая в 78 % резолюций СБ ООН (2020–2023), акцентирует правовые аспекты, связывая терроризм с нарушением базовых принципов международного права. Типичным примером служит резолюция 2565 (2021), где террористические акты определяются как «преднамеренные нападения на гражданское население, противоречащие Женевским конвенциям и Уставу ООН». Данная трактовка подчеркивает универсальный характер угрозы, но оставляет неразрешенными вопросы дифференциации между терроризмом и национально-освободительной борьбой, что становится источником правовых коллизий в Совете Безопасности (см. табл. 1).

Таблица 1

СРАВНИТЕЛЬНЫЙ АНАЛИЗ КОНЦЕПТУАЛЬНЫХ МОДЕЛЕЙ ОПРЕДЕЛЕНИЯ ТЕРРОРИЗМА В МЕЖДУНАРОДНЫХ ДОКУМЕНТАХ[1]

Критерий анализа	Правовая модель	Политическая модель	Операционная модель	Страновые кластеры
Ключевые характеристики	Ссылки на нормы международного права (Женевские конвенции, Устав ООН)	Акцент на идеологическую / религиозную мотивацию	Классификация методов (кибератаки, использование дронов)	Группировка по парадигмам противодействия терроризму
Примеры документов	Резолюции СБ ООН №2565 (2021), №2678 (2023)	Стратегия США (2021), Стратегия Ирана (2021) (силовая парадигма)	Стратегия Германии (2021), Резолюция СБ ООН №2678 (2023)	США, Франция, Израиль
Региональная специфика	78 % резолюций СБ ООН	65 % западных стратегий vs 89 % ближневосточных трактовок (правозащитная ориентация)	23% документов учитывают гибридные угрозы	Германия, Канада, ЮАР
Концептуальные противоречия	Неразрешенность вопроса о национально-освободительной борьбе	Бинарность «государственный терроризм» vs «экстремизм» (контекстуальный подход)	Пробелы в определении когнитивных атак	Бразилия, Индия, Турция
Динамика терминологии	Снижение использования «международный терроризм» на 37 %	Рост упоминаний «трансграничный терроризм» (12 → 41)	Включение систематических миграций (58% в 2023 vs 12% в 2020)	Расхождения в классификации организаций (9 / 15 стран)
Статистические показатели	12 запрещенных действий в резолюциях 2020 → 17 в 2023	41 случай термина «трансграничный терроризм» в 2023	17 методов в таксономии Резолюции №2678	41 % синхронизация национальных стратегий с СБ ООН
Географические акценты	Универсальный характер угрозы	Европа: миграционные каналы (68%)	Азия: морские коридоры и киберпространство	Ближний Восток: «государственный терроризм» (89 % ссылок)

[1]*Источник*: составлено автором на основании данных Резолюций Совета Безопасности ООН № 2501, 2510, 2532, 2565, 2585, 2597, 2610, 2621, 2635, 2657, 2678, 2699 (2020–2023), а также Стратегий национальной безопасности США (2022), КНР (2023), РФ (2021), Франция (2020), Германия (2021), Индия (2020), Турция (2020), Сауд. Аравия (2022), Иран (2021), Бразилия (2020), ЮАР (2021), Австралия (2023), Канада (2021), Великобритания (2021), Израиль (2022).

Вторая модель, представленная в 65 % национальных стратегий (США, Великобритания, Канада, Австралия), сфокусирована на идеологической мотивации терроризма. Документ США 2022 года вводит понятие «транснационального терроризма с религиозно-экстремистской идеологией», акцентируя необходимость борьбы с радикальными нарративами. Однако подобные определения демонстрируют региональную асимметрию: в стратегиях Ирана (2021) и Турции (2020) акцент смещается на «государственный терроризм», подразумевая политику западных стран на Ближнем Востоке.

Так, в Иране определение терроризма часто связано с политическими и религиозными контекстами. Иран может рассматривать действия, направленные против государства, как «государственный терроризм», особенно если они исходят от оппозиционных групп или иностранных государств. Экстремизм в Иране также может включать в себя действия, которые угрожают исламским ценностям или национальной безопасности. Таким образом, в языковом поле Ирана присутствует акцент на идеологических аспектах терроризма.

В Турции определение терроризма может быть связано с внутренними конфликтами, особенно с курдскими группами, которые правительство считает террористическими. В данном случае «государственный терроризм» может рассматриваться как ответ на угрозы национальной безопасности. Меж тем экстремизм может включать как внутренние, так и внешние угрозы, в том числе исламский экстремизм.

Бразильский феномен «государственного терроризма» может содержать акцент на социальных и экономических факторах, способствующих насилию. Он может рассматриваться в контексте борьбы с преступностью и насилием, особенно в фавелах. Бразильское общество также может акцентировать внимание на экстремизме, связанном с политическими или идеологическими движениями, включая протесты и демонстрации.

Эта бинарность концепций создает системное противоречие в международных отношениях, затрудняя формирование единого правового поля.

Третья модель, получившая развитие в документах 2022–2023 годов, определяет терроризм через классификацию методов. Резолюция СБ ООН № 2678 (2023) содержит расширенный перечень из 17 запрещенных действий, включая кибератаки на критическую инфраструктуру и использование дронов. Аналогичный подход к терроризму прослеживается в германской стратегии (2021), где впервые к терроризму отнесены «когнитивные атаки, направленные на дестабилизацию демократических институтов». Подобная конкретизация, однако, не устраняет концептуальных пробелов: только 23 % проанализированных документах учитывается взаимосвязь терроризма с гибридными угрозами.

Динамика терминологических изменений демонстрирует рост частотности понятия «трансграничный терроризм»: с 12 упоминаний в документах 2020 года до 41 случая в 2023 году. Параллельно наблюдается снижение использования термина «международный терроризм» на 37 %, что отражает переход к более конкретным видовым формулировкам. Географическая привязка определений терроризма в национальных стратегиях раскрывает поле восприятия рисков: если европейские страны акцентируют миграционные каналы проникновения террористов (68 % упоминаний), то азиатские государства фокусируются на морских коридорах (Китай, Индия) и киберпространстве (Южная Корея, Япония). Рост терминов «трансграничный терроризм» (+241,7 %) и «гибридные угрозы» (+262,5 %) отражает сдвиг в восприятии терроризма как многомерного явления, выходящего за рамки традиционных военных действий. Резкое увеличение упоминаний «климатической миграции» (+650 %) и «продовольственных кризисов» (+600 %) свидетельствует о включении нестандартных факторов в антитеррористический дискурс. При этом снижение частотности «международного терроризма» (-60,3 %) и «религиозного экстремизма» (-46,7 %) указывает на пересмотр концептуальных рамок терроризма в пользу его более конкретизированных определений (см. табл. 2).

Сравнительный анализ нормативных акцентов позволил выявить три кластера государств: страны с силовой парадигмой (США, Франция, Израиль) – 89 % определений связывают терроризм с необходимостью превентивных военных операций; страны с правозащитной ориентацией (Германия, Канада, ЮАР) – 72 % дефиниций включают ссылки на соблюдение прав человека при антитеррористических операциях; государства с контекстуальным подходом (Бразилия, Индия, Турция) – 64 % определений увязывают терроризм с историческими конфликтами и территориальными спорами [Рахимов и др., 2022].

Противоречия в концептуальных моделях проявляются в механизмах реализации резолюций СБ ООН: только 41 % национальных стратегий полностью синхронизированы с международными определениями. Наибольшие расхождения касаются классификации организаций: 9 из 15 стран включают в перечни террористических группировок структуры, не признанные таковыми СБ ООН. Например,

Таблица 2

ДИНАМИКА ИСПОЛЬЗОВАНИЯ ТЕРМИНОВ, СВЯЗАННЫХ С ТЕРРОРИЗМОМ, В МЕЖДУНАРОДНЫХ ДОКУМЕНТАХ[1]

Термин	2020	2021	2022	2023	Динамика (%)	Контекст использования
Трансграничный терроризм	12	19	32	41	+241.7	Увязка с миграционными потоками, киберпространством, неконтролируемыми территориями
Международный терроризм	58	47	39	23	-60.3	Постепенное замещение термином "трансграничный"
Международный терроризм	58	47	39	23	-60.3	Постепенное замещение термином "трансграничный" в контексте локализации угроз
Гибридные угрозы	8	14	21	29	+262.5	Включение кибератак, информационных кампаний, климатических факторов
Кибератаки	5	11	18	27	+440.0	Упоминание в контексте критической инфраструктуры и социальной дестабилизации
Когнитивные атаки	0	3	7	12	+1200.0	Новый термин в стратегиях ЕС и НАТО (2022-2023)
Климатическая миграция	2	6	9	15	+650.0	Связь с террористическим рекрутингом в зонах экологических катастроф
Морские коридоры	4	7	10	13	+225.0	Акцент в азиатских стратегиях на нелегальные перевозки оружия
Религиозный экстремизм	45	38	31	24	-46.7	Снижение частотности в западных документах, рост в ближневосточных (Сауд. Аравия: +18%)
Государственный терроризм	9	15	22	28	+211.1	Преимущественно в документах Ирана, Турции, Венесуэлы
Превентивные операции	34	29	25	19	-44.1	Сокращение в стратегиях ЕС, рост в США и Израиле (+12% к 2023)
Продовольственные каналы	3	8	14	21	+600.0	Увязка с финансированием терроризма через контроль ресурсов
Миграционные каналы	11	17	23	30	+172.7	Доминирующий термин в европейских стратегиях (68% упоминаний)

[1] *Источник*: составлено автором на основании данных Резолюций Совета Безопасности ООН №2501, 2510, 2532, 2565, 2585, 2597, 2610, 2621, 2635, 2657, 2678, 2699 (2020–2023), а также Стратегий национальной безопасности США (2022), КНР (2023), РФ (2021), Франция (2020), Германия (2021), Индия (2020), Турция (2020), Сауд. Аравия (2022), Иран (2021), Бразилия (2020), ЮАР (2021), Австралия (2023), Канада (2021), Великобритания (2021), Израиль (2022).

саудовская стратегия 2022 года относит к террористам «все организации, финансируемые Катаром», что противоречит резолюции 2657 (2022) о необходимости доказательной базы.

ЗАКЛЮЧЕНИЕ

Современный терроризм, трансформируясь под влиянием технологических инноваций и глобальных политических сдвигов, утвердился как многомерный дестабилизирующий фактор, изменяющий архитектуру международных отношений. Эмпирический анализ резолюций СБ ООН и национальных стратегий безопасности выявил три ключевых аспекта этой трансформации. *Во-первых*, превращение угрозы в конкретные действия с помощью интеграции цифровых инструментов: 40 % террористических актов 2024 года включали элементы кибератак, а 78 % транзакций Аль-Каиды осуществлялись через анонимные криптоплатформы. *Во-вторых*, географическая релокация эпицентров активности: регион Сахель, где зафиксировано 68-процентное увеличение смертности от терроризма в 2023 году, демонстрирует связь между климатическими миграциями и рекрутингом экстремистов. *В-третьих*, институционализация террористических групп как квазигосударственных акторов – контроль ИГ (*запрещена в Российской Федерации*) над территориями с населением 11 млн человек и внедрение налоговых систем «Аш-Шабаб» в Сомали подчеркивают их способность формировать параллельные системы власти.

Концептуальные противоречия в определении терроризма, выявленные в документах, усложняют формирование единой антитеррористической стратегии. Если резолюции СБ ООН акцентируют правовые нормы (78 % случаев), то национальные стратегии расходятся в трактовках: западные государства фокусируются на идеологической мотивации, тогда как Иран и Турция используют термин «государственный терроризм» для критики внешней политики конкурентов. Расхождения, наряду с технологической асимметрией (затраты на киберзащиту в 4–7 раз превышают бюджеты террористических групп), создают устойчивые риски для глобальной безопасности.

Новые дестабилизационные риски связаны с гибридизацией методов. Примеры включают использование ИИ-платформ группировкой Lazarus для атак на энергосети Балкан, а также генерацию deepfake-контента «Исламским государством» с целью манипуляции общественным мнением. Подобные тактики трансформируют природу угрозы: терроризм перестает быть исключительно физическим насилием, становясь инструментом системного воздействия на цифровые экосистемы и социальную стабильность.

Таким образом, терроризм XXI века, эволюционируя в условиях цифровых технологий и региональной локализации, бросает вызов не только системам безопасности, но и самим принципам международного взаимодействия. Ответ на этот вызов требует не столько универсальных определений, сколько адаптивных механизмов, способных учитывать динамику гибридных угроз и парадигмы национальной безопасности, в рамках которых государства определяют терроризм и реагируют на него. Примером положительного сотрудничества государств в борьбе с радикальным исламизмом и его проявлениями является сотрудничество России и Ирана, которое берет начало с заключения Договора об основах взаимоотношений и принципах сотрудничества (2001), заключением Соглашения от сотрудничестве между МВД Ирана и России (2013), заключением Межправительственного соглашения о военно-техническом сотрудничестве (2015). Позднее двустороннее взаимодействие дополнялось региональным сотрудничеством в рамках операций по противодействию контрабанде наркотиков. Большие перспективы в регионе заложены во взаимодействии на платформах Организации исламского сотрудничества, Организации Договора о коллективной безопасности (ОДКБ), Шанхайской организации сотрудничества не только в формате силовых взаимодействий, но и в формате «мягкой силы» через межкультурный и межрелигиозный диалоги. С 2021 года открыто сотрудничество между странами в области кибербезопасности, обмена технологиями, обучения специалистов [Джаббаринасир, 2023].

Таких площадок взаимодействия в мире должно быть значительно больше, чтобы противостоять новым нетрадиционным угрозам.

СПИСОК ИСТОЧНИКОВ

1. Nistorescu G. G. Complex analysis of cryptocurrencies and their implications in the context of money laundering and terrorism financing // International Scientific Conference Strategies XXI. Carol I National Defence University Publishing House. 2024. P. 113–124.
2. Lohmann S. ChatGPT, Artificial Intelligence, and the Terrorist Toolbox // An American Perspective. 2024. P. 23–34.
3. Al Waro M. N. A. L. False Reality: Deepfakes in Terrorist Propaganda and Recruitment // Security Intelligence Terrorism Journal (SITJ). 2024. Vol. 1. № 1. P. 41–59.
4. Казакбаев И. З. Мировой терроризм и экстремизм глобальная проблема современной системы международных отношений // Вестник Международного Университета Кыргызстана. 2023. Т. 2. № 50. С. 93–97.
5. Дуткевич П., Казаринова Д. Б. Страх как политика. М.: МГИМО(У), 2017.
6. Курылев К. П., Курбанов Р. М. Понятие «международный терроризм» согласно конструктивистской школе международных отношений // Журнал политических исследований. 2019. Т. 3. № 1. С. 76–82.
7. Боков Д. К. Терминологический аппарат, используемый при характеристике террористических угроз: критический анализ и направления совершенствования // Вестник Университета прокуратуры Российской Федерации. 2024. № 3 (101). С. 95–104.
8. Абдурахманова И. В., Меженская Г. В. Дефиниция «международный терроризм»: научные подходы и нормативно-правовое содержание // Аграрное и земельное право. 2024. № 10 (238). С. 24–27.
9. Сидоров Б. В. Новое в определении терроризма, международного терроризма, террористического акта и акта международного терроризма и проблемы совершенствования российского уголовного законодательства // Вестник экономики, права и социологии. 2017. № 2. С. 115–122.

10. Лебедева М. Л. Политико-экономическое содержание понятия терроризм // Международный журнал гуманитарных и естественных наук. 2024. № 2–3 (89). С. 102–105.
11. Римский А. В., Лысенко В. А. Специфика экстремизма: политико-правовые и философские определения // Наука. Искусство. Культура. 2023. № 1 (37). С. 115–126.
12. Родачин В. М. Философия безопасности: Энциклопедический словарь категорий, понятий, концептов, идей. СПб.: Наукоемкие технологии, 2024.
13. Ejazi F. Performance of Virtual Terrorism in Cyber Space // Media and Terrorism in the 21st Century. IGI Global, 2022. P. 224–236.
14. Ogele E. P. Terrorist financing in the digital age: an analysis of crypto currencies and online crowd funding // Journal of Terrorism Studies. 2024. Vol. 6. № 2. P. 4–25.
15. Me G., Mucci M. F. Identifying Daesh-Related Propaganda Using OSINT and Clustering Analysis // International Conference on Global Security, Safety, and Sustainability. Cham: Springer Nature Switzerland. 2024. P. 97–146.
16. Andreeva C. The Zerkani Network and the 2015 Paris and 2016 Brussels Attacks: An Illustration of Counter-Terrorism Dysfunction in Europe // Studies in Conflict & Terrorism. 2023. P. 1–29.
17. Atik F., Özdemir M. Paradigms of New Media and Terror Agencies // Turkish Online Journal of Educational Technology-TOJET. 2024. Vol. 23. № 1. P. 76–88.
18. Comprehensive review on cybersecurity: modern threats and advanced defense strategies / Obi O. et al. // Computer Science & IT Research Journal. 2024. Vol. 5. № 2. P. 293–310.
19. Ball D., Montasari R. The Evolution of Terrorism in Digital Era: Cyberterrorism, Social Media, and Modern Extremism // Navigating the Intersection of Artificial Intelligence, Security, and Ethical Governance: Sentinels of Cyberspace. Cham: Springer Nature Switzerland. 2024. P. 159–170.
20. Doxsee C., Palmer A., McCabe R. Global terrorism threat assessment. 2024. Rowman & Littlefield, 2024.
21. Гуторов В. А., Ширинянц А. А. Терроризм как теоретическая и историческая проблема: некоторые аспекты интерпретации // Полис. Политические исследования. 2017. № 3. С. 30–54.
22. Рахимов К. Х. [и др.]. Антитеррористический фокус сближения Индии и Таджикистана / К. Х. Рахимов, С. В. Федина, С. Х. Холов, А. Я. Якуба // Вопросы национальных и федеративных отношений. 2022. Т. 12. № 9 (90). С. 3435–3453.
23. Джаббаринасир Х. Р. Сотрудничество Ирана и России в борьбе с международным терроризмом: состояние, возможности и перспективы // Мировая экономика и международные отношения. 2023. Т. 67. № 1. С. 90–100.

REFERENCES

1. Nistorescu, G. G. (2024). Complex analysis of cryptocurrencies and their implications in the context of money laundering and terrorism financing. In International Scientific Conference Strategies XXI (pp. 113–124). Carol I National Defence University Publishing House.
2. Lohmann, S. (2024). ChatGPT, Artificial Intelligence, and the Terrorist Toolbox. An American Perspective (pp. 23–34).
3. Al Waro, M. N. A. L. (2024). False Reality: Deepfakes in Terrorist Propaganda and Recruitment. Security Intelligence Terrorism Journal (SITJ), 1(1), 41–59.
4. Kazakbaev, I. Z. (2023). World terrorism and extremism is a global problem of the modern system of international relations. Bulletin of the International University of Kyrgyzstan, 2(50), 93–97. (In Russ.)
5. Dutkevich, P., Kazarinova, D. B. (2017). Strah kak politika = Fear as politics. Moscow: MGIMO (U). (In Russ.)
6. Kurylev, K. P., Kurbanov, R. M. (2019). The concept of "international terrorism" according to the constructivist school of international relations. Journal of Political Research, 3(1), 76–82. (In Russ.)
7. Bokov, D. K. (2024). Terminological apparatus used in characterizing terrorist threats: critical analysis and areas of improvement. Bulletin of the University of the Prosecutor's Office of the Russian Federation, 3(101), 95–104.
8. Abdurakhmanova, I. V., Mezhenskaya, G. V. (2024). Definition "international terrorism": scientific approaches and regulatory content. Agrarian and land law, 10(238), 24–27. (In Russ.)
9. Sidorov, B. V. (2017). Novelties in Definition of Terrorism, International Terrorism and Acts of International Terrorism and Problems of Improving Russian Criminal Legislation. Bulletin of Economics, Law and Sociology, 2, 115–122. (In Russ.)
10. Lebedeva, M. L. (2024). Political and economic content of the concept of terrorism. International Journal of Humanities and Natural Sciences, 2–3(89), 102–105. (In Russ.)

11. Rimsky, A. V., Lysenko V. A. (2023). The specifics of extremism: political, legal and philosophical definitions. Science. Art. Culture, 1(37), 115–126.
12. Rodachin, V. M. (2024). Filosofia bezopastnosti: Entsiklopedicheskij slovar' kategorij, ponyatij, idej = Security Philosophy: Encyclopedic Dictionary of Categories, Concepts, Concepts, Ideas. St. Petersburg: Science-intensive technologies. (In Russ.)
13. Ejazi, F. (2022). Performance of Virtual Terrorism in Cyber Space. In Media and Terrorism in the 21st Century (pp. 224–236). IGI Global.
14. Ogele, E. P. (2024). Terrorist financing in the digital age: an analysis of crypto currencies and online crowd funding. Journal of Terrorism Studies, 6(2), 4–25.
15. Me, G., Mucci, M. F. (2024). Identifying Daesh-Related Propaganda Using OSINT and Clustering Analysis. In International Conference on Global Security, Safety, and Sustainability (pp. 97–146). Cham: Springer Nature Switzerland.
16. Andreeva, C. (2023). The Zerkani Network and the 2015 Paris and 2016 Brussels Attacks: An Illustration of Counter-Terrorism Dysfunction in Europe. Studies in Conflict & Terrorism (pp. 1–29).
17. Atik, F., Özdemir, M. (2024). Paradigms of New Media and Terror Agencies. Turkish Online Journal of Educational Technology-TOJET, 23(1), 76–88.
18. Obi, O. C. (Ed.) et al. (2024). Comprehensive review on cybersecurity: modern threats and advanced defense strategies. Computer Science & IT Research Journal, 5(2), 293–310.
19. Ball, D., Montasari, R. (2024). The Evolution of Terrorism in Digital Era: Cyberterrorism, Social Media, and Modern Extremism. In Navigating the Intersection of Artificial Intelligence, Security, and Ethical Governance: Sentinels of Cyberspace (pp. 159–170). Cham: Springer Nature Switzerland.
20. Doxsee, C., Palmer, A., McCabe, R. (2024). Global terrorism threat assessment 2024. Rowman & Littlefield.
21. Gutorov, V. A., Shirinyanc, A. A. (2017). Terrorism as a theoretical and historical problem: some aspects of interpretation. Polis. Political Studies, 3, 30–54. (In Russ.)
22. Rahimov, K. H. et al. (2022). Anti-terrorist focus of rapprochement between India and Tajikistan / Rahimov, K. H., Fedina, S. V., Holov, S. H., Yakuba, A. Ya. Issues of National and Federal Relations, 12(9), 3435–3453. (In Russ.)
23. Jabbarinasir, H. R. (2023). Cooperation between Iran and Russia in the fight against international terrorism: state, opportunities and prospects. World economy and international relations, 67(1), 90–100. (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРЕ

Холов Суруш Холович

аспирант
факультета гуманитарных и социальных наук
Российского университета дружбы народов имени Патриса Лумумбы

INFORMATION ABOUT THE AUTHOR

Kholov Surush Kholovich

Postgraduate Student
Faculty of Humanities and Social Sciences
Patrice Lumumba Peoples' Friendship University of Russia

Статья поступила в редакцию	07.12.2024	The article was submitted
одобрена после рецензирования	12.01.2025	approved after reviewing
принята к публикации	14.03.2025	accepted for publication