UDC 327.57
IRSTI 11.25.41
https://doi.org/10.48371/ISMO.2025.62.4.009

НАЦИОНАЛЬНОЕ ГОСУДАРСТВО В БОРЬБЕ С ТРАНСНАЦИОНАЛЬНЫМИ УГРОЗАМИ (НА ПРИМЕРЕ ТЕРРОРИЗМА)

* Жанысова К.Н.[1]
*[1] Казахский университет международных отношений и мировых языков имени Абылай хана, Алматы, Казахстан

Аннотация. Статья посвящена анализу транснационального терроризма и роли государства по обеспечению безопасности. На примере Израиля, Казахстана и Южной Кореи показано, что государство остаётся ключевым актором в борьбе с терроризмом, поскольку именно оно обладает полномочиями по криминализации угроз, регулированию цифровых, финансовых потоков, а также координации силовых и аналитических структур. В условиях цифровизации терроризм приобретает сетевую форму, используя криптофинансирование, онлайн-коммуникации и нелегальные логистические каналы, что требует от государства внедрения новых механизмов контроля: цифрового мониторинга, анализа данных, платформ информационной безопасности и финансового надзора. В статье показано, что Израиль развивает технологически-разведывательный подход, Казахстан усиливает институциональную координацию и аналитический мониторинг, а Южная Корея формирует модель функционального суверенитета, основанную на управлении данными и цифровыми потоками. Автор приходит к выводу, что транснациональный терроризм не ослабляет национальное государство, а наоборот делает его более аналитическим, технологичным и стратегически ориентированным.

Ключевые слова: национальное государство, транснациональные угрозы, международный терроризм, Израиль, Казахстан, Южная Корея, государственное регулирование, безопасность

Введение

В условиях глобальной взаимозависимости и цифровизации, природа транснациональных угроз, таких, как, например, терроризм, выходит за пределы территориальных границ, одновременно затрагивает финансовую, цифровую, коммуникационную сферы, тем самым требуя расширения функций государственности и углубления её аналитического, цифрового и нормативного потенциала.

Терроризм, обладая сетевой и идеологической природой, является одной из наиболее показательных угроз, выявляющих сущность функциональной трансформации государства. Он сочетает цифровую

пропаганду, криптофинансирование, координацию через нелегальные коммуникационные платформы и скрытые логистические маршруты, образуя устойчивую инфраструктуру, не привязанную к конкретному пространству. В научной дискуссии появляются две конкурирующие позиции: одни исследователи указывают на ослабление национального государства перед лицом транснациональных акторов, другие на адаптацию и институциональную трансформацию государственности в ответ на новые вызовы. Таким образом, возникает потребность в анализе того, как государство перестраивает механизмы безопасности, какие инструменты использует и какие новые функции приобретает в условиях сетевого терроризма.

Выбор Израиля, Казахстана и Южной Кореи обусловлен тем, что именно эти страны демонстрируют различные модели государственно-ориентированного противодействия терроризму. Каждая из этих стран показывает различные модели государственного реагирования: Израиль делает упор на разведку и технологии, Казахстан укрепляет роль государства через координацию и анализ угроз, а Южная Корея на цифровое регулирование и контроль данных.

Цель данного исследования заключается в том, чтобы проанализировать трансформацию роли государства в борьбе с терроризмом как транснациональной угрозой, определить, как государственные институты интегрируют цифровой мониторинг, финансовый контроль, правовое регулирование и межведомственную координацию, а также выявить, какие элементы новой модели безопасности формируются в результате этой трансформации.

Описание материалов и методов

В основе исследования лежат несколько теоретико-методологических подходов, позволяющих раскрыть роль государства в борьбе с терроризмом как транснациональной угрозой.

Прежде всего, используются идеи Барри Бузана и Оле Уэвера, которые подчёркивают, что государство сохраняет право определять, какие явления становятся угрозами национальной безопасности, переводя их в категорию секьюритизированных. Это объясняет, почему именно государство инициирует правовые, силовые и организационные меры против терроризма [1].

С позиций политического реализма, Ганс Моргентау рассматривает государство как основной актор международных отношений, обладающий легитимной монополией на силу и ответственностью за выживание политического сообщества. Согласно его подходу, главная задача государства защита национальных интересов и поддержание безопасности, что делает борьбу с терроризмом не только вопросом внутренней стабильности, но и стратегической необходимостью [2].

Мануэль Кастельс рассматривает транснациональный терроризм

как сетевую структуру, действующую через цифровые, финансовые и логистические каналы. Это позволяет объяснить, почему борьба с терроризмом требует от государств создания гибких, аналитических и технологически оснащенных институтов [3].

Джозеф Най и Роберт Кеохейн показывают, что несмотря на наличие негосударственных акторов, государство остаётся главным субъектом, способным координировать нормативные, финансовые и силовые механизмы борьбы с терроризмом. Их взгляды обосновывают применение неолиберального институционализма, где государство не исчезает, а меняет характер своего влияния [4].

Стивен Краснер вводит идею функционального суверенитета, объясняя, что государство сохраняет стратегическую власть, когда контролирует не только границы, но и потоки, как информационные, цифровые, финансовые и миграционные [5]. Это позволяет рассматривать контртеррористическую политику Израиля, Казахстана и Южной Кореи как подтверждение трансформации, а не ослабления государства.

В исследовании применялся институциональный анализ, который позволил выявить, как государство формирует и трансформирует специализированные структуры безопасности, распределяет полномочия между разведывательными, финансовыми и цифровыми ведомствами, а также как эти институты обеспечивают координацию в условиях транснациональных угроз. Через контент-анализ официальных документов были изучены стратегии национальной безопасности, нормативные акты и аналитические сводки, что позволило определить, каким образом государства формализуют угрозу терроризма, закрепляют её в правовом поле и определяют механизмы реагирования. Применение case study дало возможность рассмотреть конкретные примеры предотвращения террористических актов, отслеживания цифровых каналов финансирования, выявления криптоактивов и нейтрализации сетевых групп, что показало, как государственные органы используют цифровую аналитику и межведомственное взаимодействие на практике. Policy analysis позволил интерпретировать государственные меры не только как реакцию на угрозу, но как инструмент формирования государственной политики безопасности, когда государство переходит от силового реагирования к управлению рисками через прогнозирование, цифровое регулирование и межведомственную интеграцию.

Результаты

Концепция секьюритизации, описанная Барри Бузаном и Оле Уэвером, находит отражение в официальных документах трех государств, где борьба с терроризмом рассматривается не как эпизодическая угроза, а как угроза национальной безопасности, оправдывающая расширение полномочий государства [1].

В Национальной стратегии безопасности Израиля терроризм рассматривается как экзистенциальная угроза, «которая требует постоянной готовности государства, укрепления разведывательных служб, цифрового наблюдения и стратегической мобилизации общества». В документе подчёркивается, что государство обладает ключевой координационной ролью в противодействии терроризму, поскольку именно оно уполномочено формировать правовую основу борьбы, организовывать контртеррористические операции, обеспечивать межведомственное взаимодействие, контролировать цифровые коммуникационные сети, пресекать каналы вербовки и инициировать международное сотрудничество в разведывательной сфере [6]. Такой подход отражает логику, описанную вышеуказанными авторами, согласно которой государство не только реагирует на угрозу, но институционально определяет её как угрозу национальной безопасности. Таким образом, государство не просто фиксирует наличие угрозы, а переводит её в сферу государственной политики, придавая ей правовой статус, легитимируя применение специальных мер безопасности и обеспечивая межведомственную консолидацию.

В Стратегии национальной безопасности Республики Казахстан терроризм отнесён к числу приоритетных угроз, подрывающих конституционный строй, стабильность общества и безопасность граждан. В документе подчёркивается, что защита государства от терроризма «обеспечивается через развитие национальной системы противодействия экстремизму и терроризму, включающей правоохранительные органы, спецслужбы, финансовый мониторинг, информационные механизмы, миграционный контроль и международное сотрудничество» [7]. Исходя из этого, в стратегии прослеживается предположение, что государство выступает ключевым организатором и координатором механизмов безопасности, способным объединять различные инструменты реагирования - от правового и силового до цифрового и гуманитарного.

В Национальной стратегии кибербезопасности Республики Корея подчёркивается, что современный терроризм приобретает цифровую форму, проявляясь через онлайн-радикализацию, дистанционные механизмы вербовки, шифрованные коммуникационные каналы и криптофинансирование. В документе акцентируется, что государство выполняет центральную координирующую роль, обеспечивая не только защиту критической инфраструктуры, но и мониторинг цифровых коммуникаций, регулирование потоков данных и пресечение использования нелегальных платформ [8]. Эта логика соответствует идеям Мануэля Кастельса о том, что власть в условиях сетевого общества концентрируется не вокруг контроля над территорией, а вокруг контроля над информационными потоками, инфраструктурой данных и цифровыми каналами, через которые распространяются угрозы [3].

Как видно из данных Таблицы 1, с 2015 года в Израиле, Казахстане

и Южной Корее появились новые специализированные органы, которые отражают переход государства от классической силовой модели к аналитико-цифровому и финансовому контролю над терроризмом.

Таблица 1. Новые государственные структуры по борьбе с терроризмом (2015 - 2024 гг.)

Страна	Наименование структуры	Год создания / реформирования
Израиль	National Bureau for Counter-Terror Financing	2018
	Joint Cyber Defense Authority	2021
Казахстан	Комитет по кибербезопасности при Министерстве цифрового развития	2016
	Центр анализа и расследования кибератак (TSARKA)	2017
	Национальный центр по противодействию терроризму (КНБ)	2021
	Оперативный штаб по борьбе с терроризмом	2019
Южная Корея	Cyber Terror Response Center (KNPA)	2015
	National Cybersecurity Center (NIS)	2015
	Counter-Terror Intelligence Integration Platform	2020

(Составлено автором)

В Казахстане борьба с терроризмом постепенно трансформировалась из силового реагирования в модель функционально-институционального контроля, основанную на цифровой аналитике, межведомственной координации и мониторинге критических инфраструктур. В рамках Министерства цифрового развития действует Комитет по кибербезопасности, который обеспечивает государственный контроль над цифровыми платформами, отслеживает интернет-ресурсы с экстремистским содержанием, фиксирует попытки вербовки в закрытых онлайн-сообществах и выявляет подозрительные криптофинансовые транзакции. Центр анализа и расследования кибератак (TSARKA) осуществляет техническую фиксацию цифровых следов, включая IP-логи, сетевые маршруты, криптокошельки, шифрованные каналы коммуникации и цифровые следы денежных переводов. В свою очередь, Национальный центр по противодействию терроризму (КНБ) и Оперативный штаб по борьбе с терроризмом выполняют аналитически-координационную функцию, объединяя данные из миграционного контроля, финансового мониторинга, киберразведки, судебных органов и силовых структур. Практическая база подтверждает, что государство использует не только силовые операции, но и цифровые, финансовые и аналитические инструменты управления угрозами. Согласно официальным данным КНБ, в 2024 году в Казахстане

было предотвращено четыре готовившихся террористических акта, при этом большинство угроз были выявлены на стадии планирования через мониторинг коммуникаций, отслеживание криптовалютных переводов и анализ поведения пользователей в закрытых мессенджерах [9]. В октябре 2025 года в Алматы был пресечён теракт, подготовленный иностранными гражданами, использовавшими Telegram-каналы, зашифрованные VPN-маршруты и цифровые переводы для координации действий. Спецслужбами была прослежена цепочка коммуникаций, включая IP-активность, геолокацию устройств, транзит денежных средств между гражданами Казахстана и зарубежными посредниками [10]. В ноябре 2025 года задержаны шесть человек в Алматы, Шымкенте, Конаеве и Актобе по подозрению в вербовке через анонимные онлайн-платформы. TSARKA зафиксировал цифровую активность, включающую создание сетевых группировок в WhatsApp и Discord, использование облачных сервисов для распространения инструкций, а также попытки криптофинансового сбора средств на зарубежных краудфандинговых площадках [11]. Параллельно Комитет по финансовому мониторингу выявил «рассыпанную модель микро-платежей», когда небольшие суммы перечислялись через цифровые кошельки в пользу неформальных структур на территории Ближнего Востока. Механизмы, используемые государством, включают не только блокировку экстремистских ресурсов (в 2023–2024 гг. заблокировано более 2 500 сайтов и аккаунтов), но и использование алгоритмов поведенческой аналитики, позволяющих фиксировать признаки деструктивной активности: резкие изменения поисковых запросов, участие в закрытых группах, скачивание подозрительных файлов, контакты с иностранными аккаунтами [12]. Эти действия отражают переход от реактивной модели к модели превентивного управления рисками, где государство осуществляет контроль не только над физической территорией, но и над информационными, финансовыми, цифровыми и коммуникационными.

Израильская система противодействия терроризму характеризуется разведывательно-технологической направленностью, при которой государство выстраивает превентивную, а не реактивную модель, основанную на цифровой аналитике, финансовом мониторинге и межведомственной интеграции. Ключевым компонентом этой модели выступает National Bureau for Counter-Terror Financing, который обладает правом отслеживать, блокировать и замораживать криптовалютные активы, финансирующие экстремистские сети. По состоянию на март 2024 года этим органом было идентифицировано и заморожено 42 криптокошелька, связанных с ХАМАС, «Исламским Джихадом» и транснациональными группировками на Ближнем Востоке [13]. При этом Financial Action Task Force классифицирует израильскую систему финансового мониторинга как «sound and effective», что подтверждает институциональную устойчивость государства в этой сфере [14]. Технологическую составляющую

обеспечивает Joint Cyber Defense Authority, которая выполняет функции цифровой разведки, выявляя шифрованные маршруты коммуникаций, инфраструктуру виртуальных тренировочных лагерей, сетевые ячейки и схемы удалённой логистики. Эта структура анализирует VPN-подключения, метаданные пользователей, криптотранзакции, перемещения информации между мессенджерами, игровыми платформами и закрытыми социальными сетями, что позволяет фиксировать угрозу до её перехода в физическую фазу. Такие меры соответствуют принципу «preemptive intelligence action», лежащему в основе израильской стратегии. По данным Israel Security Agency, около 85 % предотвращённых террористических актов были пресечены именно на стадии подготовки, благодаря цифровому мониторингу коммуникаций, финансовых переводов и поведенческих индикаторов [15]. В 2024 году, по сведениям Institute for National Security Studies, было зарегистрировано 6 828 террористических инцидентов, однако значительная часть попыток была нейтрализована до реализации за счёт интеграции данных, поступающих от Joint Cyber Defense Authority, National Bureau for Counter-Terror Financing и Israel Security Agency (Shin Bet) [16]. Кроме того, Israel National Antiterrorism Headquarters обеспечивает правовую и институциональную координацию между Министерством юстиции, разведывательными органами, финансовыми структурами и военными службами. Именно государство формирует нормативную рамку, инициирует межгосударственное сотрудничество, определяет правовой статус угрозы и легитимирует применение специальных мер безопасности.

В Южной Корее противодействие терроризму опирается на институционально-платформенную модель, основанную на управлении цифровыми, миграционными и финансовыми потоками, а не только на силовом реагировании. Государство обладает возможностью объединять данные из разных ведомств: полиции, разведки, финансовых служб, миграционного контроля и телекоммуникационных операторов, что позволяет выявлять угрозу ещё до перехода к физическому исполнению. Особое значение имеет цифровая разведка. Так, отслеживание шифрованных мессенджеров, IP-маршрутов, VPN-подключений и подозрительных криптовалютных транзакций осуществляется подразделениями Korean National Police Agency через специализированную структуру, которая анализирует цифровые следы, фиксирует попытки онлайн-вербовки, хранение инструкций и удалённые схемы координации. При этом ключевая координационная функция принадлежит разведывательному ведомству, которое управляет системами мониторинга цифровых коммуникаций, блокировки нелегальных платформ и алгоритмами анализа поведения пользователей, что позволяет фиксировать угрозы до того, как они переходят в операционную фазу. Цифрово-аналитический уровень дополняется интегрированной системой отслеживания миграционных данных, криптокошельков, социальных сетей и транзитных финансовых каналов, которая объединяет информацию от

полиции, банков, миграционной службы, операторов связи и специальных служб. Эта платформа позволяет не только фиксировать подозрительные цифровые следы, но и связывать их с реальными перемещениями, финансовыми действиями и коммуникационными связями конкретных лиц. Практика подтверждает эффективность такой модели. В 2024 году в Республике Корея была пресечена группа, использовавшая учебные визы и криптофинансовые операции для поддержки ближневосточной террористической сети; выявление стало возможным благодаря анализу транзитных маршрутов, activity-логов и цифровой переписки в закрытых каналах . В другом случае, зафиксированном в 2023–2024 гг., удалось предотвратить попытку вербовки иностранных студентов через Discord и Telegram: аналитические платформы выявили цифровые паттерны поведения, включая участие в скрытых группах, скачивание инструкций, резкую смену IP-локаций и мелкие криптовалютные пожертвования [17].

Обсуждение

Терроризм, как транснациональная угроза, формирует такие условия безопасности, в которых государство становится центральным субъектом управления рисками, интегрируя правовые, цифровые, финансово-контрольные и гуманитарные механизмы. Как подчёркивал Ганс Моргентау, государство остаётся ключевым актором в обеспечении безопасности, поскольку обладает легитимной монополией на силу, ответственностью за выживание политического сообщества и способностью институционализировать угрозы [2]. Его подход объясняет, почему даже в условиях транснационального терроризма именно государство определяет, что считать угрозой, как на неё реагировать и какие меры применять: силовые, правовые, цифровые или финансовые. Аналитические данные Израиля, Казахстана и Южной Кореи демонстрируют, что именно государство управляет критическими ресурсами: разведывательной информацией, финансовыми потоками, миграционным контролем, цифровыми коммуникациями и инфраструктурными системами, что недоступно негосударственным акторам. Это указывает не на снижение роли государства, а на её усложнение и функциональное расширение.

Израиль демонстрирует модель технологизированной государственности, в которой борьба с терроризмом основана не на механизме реагирования, а на способности государства преобразовывать угрозу в цифровой сигнал, формализуемый через правовые, финансовые и разведывательные каналы. Как подчёркивает Боаз Ганор, государство сохраняет исключительную роль в борьбе с терроризмом именно потому, что обладает монополией на институциональную легитимацию угрозы: оно определяет, классифицирует и переводит потенциальное террористическое действие в юридическую категорию угрозы национальной безопасности [18]. В израильской модели государство не просто фиксирует риск, но управляет

им, формирует цифровую инфраструктуру наблюдения, разрабатывает алгоритмы распознавания угроз, соединяет разведку, финансовый контроль и правовое пресечение в единую систему предотвращения.

Казахстанская модель представляет собой переход от силового реагирования к инфраструктурному управлению угрозами. Как отмечал Мурат Лаумулин, ключевая роль государства заключается в том, что оно способно объединять миграционные, финансовые, информационные и разведывательные потоки, превращая их в инструмент сдерживания гибридных угроз [19]. В отличие от израильской технологической модели, Казахстан демонстрирует институционально-аналитическую, где акцент делается на межведомственном согласовании, нормативном управлении и способности государства адаптироваться к многоуровневым и внутренним кризисам, имеющим признаки террористической или деструктивной координации.

Южная Корея показывает дальнейшее развитие этой логики, формируя платформенную модель безопасности, где государство действует не только как суверен территории, но и как оператор цифровых идентичностей, криптофинансовых перемещений и коммуникационных потоков. Как подчёркивает Д. Ким, борьба с терроризмом в Корее строится на управлении не пространством, а данными: государство контролирует алгоритмы, инфраструктуру цифровой безопасности, прогнозирует угрозы на уровне поведенческих паттернов и сетевой активности, а не только на уровне физических действий [20]. Это демонстрирует смещение государственной власти в сферу платформенной безопасности.

Таким образом, транснациональный терроризм не снижает значимость государственности, а трансформирует её характер. Государство перестает быть только институтом территориального контроля и превращается в инфраструктурного координатора, управляющего потоками данных, коммуникаций, идентичностей и финансов. Эта эволюция демонстрирует формирование новой модели - государство как координирующий центр безопасности, где управление рисками осуществляется не только через силовые меры, но также через анализ, прогнозирование, нормативное регулирование и цифровое управление.

Заключение

Исходя из анализа политики Израиля, Казахстана и Южной Кореи был сделан вывод о том, что главную роль в борьбе с терроризмом играет государство, поскольку именно оно обладает полномочиями криминализировать угрозы, устанавливать правовые рамки реагирования, координировать силовые, цифровые, финансовые и гуманитарные механизмы пресечения, а также обеспечивать легитимность принимаемых мер. В отличие от негосударственных акторов, государство способно объединять разведывательные структуры, финансовый мониторинг,

аналитические центры, правовые институты и технологические системы в единую систему противодействия терроризму, что делает его ключевым координатором национальной и международной безопасности.

Израиль показал наиболее технологически развитую форму контртерроризма, основанную на цифровой разведке, блокировке криптофинансирования, прогнозной аналитике и интеграции правовых инструментов. Казахстан продемонстрировал, что государственное регулирование позволяет не только предотвращать террористические акты, но и управлять кризисами гибридного характера, такими как события января, когда угроза проявилась одновременно в политической, цифровой, криминальной и социальной сферах. Южная Корея подтвердила, что современная борьба с терроризмом требует контроля не только над территорией, но и над цифровыми, финансовыми и миграционными потоками, что является проявлением функционального суверенитета государства.

Показательно, что во всех трёх странах с 2015 года государство не сосредоточилось только на усилении силового компонента, но инициировало создание новых специализированных структур, ориентированных на цифровую безопасность, контроль криптовалют, мониторинг финансовых транзакций, анализ коммуникаций и предотвращение онлайн-радикализации. Это доказывает, что государство трансформирует свою роль, переходя от классической модели защиты границ к архитектуре сетевого управления и цифровой безопасности.

Таким образом, в условиях транснационального терроризма национальное государство не утрачивает своим позиции, а напротив укрепляет стратегические функции, становясь центральным координатором управления потоками, институциональным реформатором, правовым регулятором и цифровым арбитром. Борьба с терроризмом становится не просто сферой безопасности, а пространством, где государство заново утверждает свою значимость, адаптивность и стратегическую необходимость.

ЛИТЕРАТУРА

[1] Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. – Boulder; London: Lynne Rienner Publishers, 1998. – 239 p.

[2] Morgenthau H. J. Politics Among Nations: The Struggle for Power and Peace. – New York: Alfred A. Knopf, 1948.

[3] Castells M. The Power of Identity. – 2nd ed. – Malden, MA; Oxford, UK: Blackwell, 2004. – 592 p.

[4] Nye J. S., Keohane R. O**.** Power and Interdependence: World Politics in Transition. – Boston; Toronto: Little, Brown & Co., 1977. – 334 p.

[5] Krasner S. D. Sovereignty: Organized Hypocrisy. – Princeton: Princeton University Press, 1999. – 269 p.

[6] The State of Israel's National Security // *The Institute for National*

Security Studies (INSS). – 2025. – 4 December. – https://www.inss.org.il/wp-content/uploads/2025/02/SecurityPolicy-Version-ENG_digital-1.pdf.

[7] Закон Республики Казахстан «О национальной безопасности Республики Казахстан» от 06.01.2012 № 527-IV // Юридическая информационная база «Adilet». – 2012. – 17 января. – https://adilet.zan.kz/rus/docs/Z1200000527.

[8] National Cybersecurity Strategy of the Republic of Korea // National Security Office. – 2019. – https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf.

[9] Четыре теракта предотвращено в Казахстане с начала года // *Vlast.kz*. – 2024. – 5 декабря. – https://vlast.kz/novosti/62967-cetyre-terakta-predotvraseno-v-kazahstane-s-nacala-goda-knb.html.

[10] NSC prevents terrorist attack in Almaty // *TengriNews*. – 2025. – 29 октября. – https://en.tengrinews.kz/kazakhstan_news/nsc-prevents-terrorist-attack-in-almaty-269968/.

[11] Шесть религиозных радикалов задержали в Казахстане в ноябре // *Казинформ*. – 2025. – 24 ноября. – https://www.inform.kz/ru/shest-religioznih-radikalov-zaderzhali-v-kazahstane-v-noyabre-fe8bc3.

[12] Более 38 тысяч интернет-ресурсов заблокировали в Казахстане в 2024 году // *Sputnik Казахстан*. – 2025. – 24 ноября. – https://ru.sputnik.kz/20251124/bolee-38-tysyach-internet-resursov-zablokirovali-v-kazakhstane-v-2024-godu-59042113.html.

[13] Israeli authorities link 42 crypto addresses to terrorism // *Elliptic*. – 2024. – 28 March. – https://www.elliptic.co/blog/israeli-authorities-link-42-crypto-addresses-to-terrorism.

[14] Israel – Member since 2018 // *Financial Action Task Force*. – https://www.fatf-gafi.org/en/countries/detail/Israel.html.

[15] Shin Bet reports 40% drop in terrorist successes during 2024 // *Jewish News Syndicate*. – 2024. – 31 December. – https://www.jns.org/shin-bet-reports-40-drop-in-terrorist-successes-during-2024/.

[16] Summary of Terror Attacks in Israel and the West Bank, 2023–2024 // *The Institute for National Security Studies*. – 2025. – 4 February. – https://www.inss.org.il/publication/terror-2023-2024/.

[17] Foreigners caught funding terrorist group using cryptocurrency // *The Korea Times*. – 2023. – 16 February. – https://www.koreatimes.co.kr/southkorea/law-crime/20230216/foreigners-caught-funding-terrorist-group-using-cryptocurrency.

[18] Annual Cybercrime and Counter-Terrorism Report, 2023–2024 / Korea National Police Agency. – https://www.police.go.kr/index.do.

[19] Ganor B. Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? // *Police Practice and Research*. – 2002. – Vol. 3, No. 4. – P. 287–304.

[20] Лаумулин М. Т. Геополитические вызовы и национальная безопасность Казахстана в условиях глобализации. – Алматы: Казахстанский институт стратегических исследований при Президенте Республики Казахстан, 2020. – 256 с.

[21] Kim D. Prediction of terrorism pattern accompanied by cyber-terrorism and the development direction of corresponding legal systems // *arXiv preprint*. – 2022. – arXiv:2203.03620. – March. – 15 p.

REFERENCES

[1] Buzan B., Wæver O., de Wilde J. Security: A New Framework for Analysis. Boulder; London: Lynne Rienner Publishers, 1998, p. 239.

[2] Morgenthau H.J. Politics Among Nations: The Struggle for Power and Peace. New York: Alfred A. Knopf, 1948.

[3] Castells M. The Power of Identity. 2nd ed. Malden, MA; Oxford, UK: Blackwell, 2004, p. 592.

[4] Nye J.S., Keohane R.O. Power and Interdependence: World Politics in Transition. Boston; Toronto: Little, Brown & Co., 1977, p. 334.

[5] Krasner S.D. Sovereignty: Organized Hypocrisy. Princeton: Princeton University Press, 1999, p. 269.

[6] The State of Israel's National Security. The Institute for National Security Studies (INSS), 2025. https://www.inss.org.il/wp-content/uploads/2025/02/SecurityPolicy-Version-ENG_digital-1.pdf.

[7] Zakon Respubliki Kazakhstan «O natsional'noi bezopasnosti Respubliki Kazakhstan» ot 06.01.2012 No. 527-IV [Law of the Republic of Kazakhstan "On National Security of the Republic of Kazakhstan" dated January 6, 2012 No. 527-IV]. Yuridicheskaya informatsionnaya baza «Adilet» [Legal Information Database "Adilet"], 2012, January 17. https://adilet.zan.kz/rus/docs/Z1200000527 [in Russ.].

[8] National Cybersecurity Strategy of the Republic of Korea. National Security Office, 2019. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National%20Cybersecurity%20Strategy_South%20Korea.pdf.

[9] Chetyre terakta predotvrashcheno v Kazakhstane s nachala goda – KNB [Four Terrorist Attacks Prevented in Kazakhstan since the Beginning of the Year – National Security Committee]. Vlast.kz, 2024, December 5. https://vlast.kz/novosti/62967-cetyre-terakta-predotvraseno-v-kazahstane-s-nacala-goda-knb.html [in Russ.].

[10] NSC Prevents Terrorist Attack in Almaty. TengriNews, 2025, October 29. https://en.tengrinews.kz/kazakhstan_news/nsc-prevents-terrorist-attack-in-almaty-269968/.

[11] Shest' religioznykh radikalov zaderzhali v Kazakhstane v noyabre [Six Religious Radicals Detained in Kazakhstan in November]. Mezhdunarodnoe

informatsionnoe agentstvo «Kazinform» [Kazinform International News Agency], 2025, November 24. https://www.inform.kz/ru/shest-religioznih-radikalov-zaderzhali-v-kazahstane-v-noyabre-fe8bc3 [in Russ.].

[12] Bolee 38 tysyach internet-resursov zablokirovali v Kazakhstane v 2024 godu [More than 38,000 Internet Resources Were Blocked in Kazakhstan in 2024]. Sputnik Kazakhstan, 2025, November 24. https://ru.sputnik.kz/20251124/bolee-38-tysyach-internet-resursov-zablokirovali-v-kazakhstane-v-2024-godu-59042113.html [in Russ.].

[13] Israeli Authorities Link 42 Crypto Addresses to Terrorism. Elliptic, 2024, March 28. https://www.elliptic.co/blog/israeli-authorities-link-42-crypto-addresses-to-terrorism.

[14] Israel – Member since 2018. Financial Action Task Force. https://www.fatf-gafi.org/en/countries/detail/Israel.html.

[15] Shin Bet Reports 40% Drop in Terrorist Successes during 2024. Jewish News Syndicate, 2024, December 31. https://www.jns.org/shin-bet-reports-40-drop-in-terrorist-successes-during-2024/.

[16] Summary of Terror Attacks in Israel and the West Bank, 2023–2024. The Institute for National Security Studies, 2025, February 4. https://www.inss.org.il/publication/terror-2023-2024/.

[17] Foreigners Caught Funding Terrorist Group Using Cryptocurrency. The Korea Times, 2023, February 16. https://www.koreatimes.co.kr/southkorea/law-crime/20230216/foreigners-caught-funding-terrorist-group-using-cryptocurrency.

[18] Annual Cybercrime and Counter-Terrorism Report, 2023–2024. Korea National Police Agency. https://www.police.go.kr/index.do.

[19] Ganor B. Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? Police Practice and Research, 2002, Vol. 3, No. 4, pp. 287–304.

[20] Laumulin M.T. Geopoliticheskie vyzovy i natsional'naya bezopasnost' Kazakhstana v usloviyakh globalizatsii [Geopolitical Challenges and National Security of Kazakhstan in the Context of Globalization]. Kazakhstanskii institut strategicheskikh issledovanii pri Prezidente Respubliki Kazakhstan [Kazakhstan Institute for Strategic Studies under the President of the Republic of Kazakhstan]. Almaty, 2020, p. 256 [in Russ.].

[21] Kim D. Prediction of Terrorism Pattern Accompanied by Cyber-Terrorism and the Development Direction of Corresponding Legal Systems. arXiv preprint arXiv:2203.03620, 2022, March, p. 15.

ҰЛТТЫҚ МЕМЛЕКЕТТІҢ ТРАНСҰЛТТЫҚ ҚАУІПТЕРМЕН КҮРЕСУДЕГІ РӨЛІ (ТЕРРОРИЗМ МЫСАЛЫНДА)

*Жанысова К.Н.[1]
*[1] Абылай хан атындағы Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан

Аңдатпа. Мақала трансұлттық терроризм феноменін және қауіпсіздікті қамтамасыз етудегі мемлекеттің рөлін талдауға арналған. Израиль, Қазақстан және Оңтүстік Корея мысалында терроризмге қарсы күресте ұлттық мемлекет негізгі актор болып қала беретіні көрсетілген, өйткені дәл мемлекет қауіптерді криминализациялау, цифрлық және қаржылық ағындарды реттеу, сондай-ақ күштік және аналитикалық құрылымдардың жұмысын үйлестіру өкілеттіктеріне ие. Цифрландыру жағдайында терроризм желілік сипатқа көшіп, криптоқаржыландыруды, онлайн-коммуникацияны және жасырын логистикалық арналары пайдаланады, бұл мемлекеттен бақылаудың жаңа механизмдерін: цифрлық мониторингті, деректерді талдауды, ақпараттық қауіпсіздік платформаларын және қаржылық қадағалауды енгізуді талап етеді. Мақалада Израильдің технологиялық-барлау тәсілді дамытатыны, Қазақстанның институционалдық үйлестіру мен аналитикалық мониторингті күшейткені, ал Оңтүстік Кореяның деректер мен цифрлық ағындарды басқаруға негізделген функционалдық егемендік моделін қалыптастыратыны көрсетілген. Автор трансұлттық терроризм ұлттық мемлекетті әлсіретпей, керісінше оны неғұрлым аналитикалық, технологиялық және стратегиялық бағытталған етеді деген қорытындыға келеді.

Тірек сөздер: ұлттық мемлекет, трансұлттық қауіптер, халықаралық терроризм, Израиль, Қазақстан, Оңтүстік Корея, мемлекеттік реттеу, қауіпсіздік

THE NATION-STATE IN THE FIGHT AGAINST TRANSNATIONAL THREATS (THE CASE OF TERRORISM)

*Zhanyssova K.N.[1]
*[1] Kazakh Ablai khan University of International Relations and World Languages, Almaty, Kazakhstan

Abstract. The article is devoted to the analysis of transnational terrorism and the role of the state in ensuring security. Using the examples of Israel, Kazakhstan, and South Korea, it demonstrates that the nation-state remains the key actor in countering terrorism, as it holds the authority to criminalize threats, regulate digital and financial flows, and coordinate security and analytical institutions. In the context of digitalization, terrorism takes on a networked form, utilizing cryptofinancing, online communication, and clandestine logistical channels, which requires states to implement new mechanisms of control, including

digital monitoring, data analysis, information security platforms, and financial oversight. The article shows that Israel develops a technologically intelligence-driven model, Kazakhstan strengthens institutional coordination and analytical monitoring, while South Korea forms a model of functional sovereignty based on data and digital flow management. The author concludes that transnational terrorism does not weaken the nation-state but rather makes it more analytical, technologically equipped, and strategically oriented.

Key words: nation-state, transnational threats, international terrorism, Israel, Kazakhstan, South Korea, state regulation, security

Received: October 29, 2025
Accepted: December 22, 2025

Сведение об авторе:
Жанысова К.Н. - PhD докторант, Казахский университет международных отношений и мировых языков имени Абылай хана, Алматы, Казахстан, e-mail: kzhanyssovaa@gmail.com

Автор туралы мәліметтер:
Жанысова К.Н. - PhD докторант, Абылай хан атындағы Қазақ халықаралық қатынастар және әлем тілдері университеті, Алматы, Қазақстан, e-mail: kzhanyssovaa@gmail.com

Information about the author:
Zhanyssova K.N. - PhD student, Kazakh Ablai khan University of International Relations and World Languages, Almaty, Kazakhstan, e-mail: kzhanyssovaa@gmail.com