Дата поступления рукописи в редакцию: 28.08.2026 г.
Дата принятия рукописи в печать: 25.09.2026 г.

DOI: 10.24412/2782-3849-2026-9-118-127

ТАРАСОВ Александр Анатольевич,
старший преподаватель Департамента уголовного права, процесса и криминалистики Факультета права Национального исследовательского университета «Высшая школа экономики» (НИУ ВШЭ), ORCID:0000-0078-9276-5211, ResearcherID: T-8912-2023, Scopus AuthorID: 82640173651, e-mail: tarasov.aa@hse.ru

СОВЕРШЕНСТВОВАНИЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРОТИВОДЕЙСТВИЯ ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА В РАМКАХ СТРАН БРИКС

Аннотация. *В статье проанализированы законодательные противоречия государств-членов БРИКС. Сделан вывод о том, что несогласованность правовых подходов в национальных законодательствах стран-участниц позволяет радикальным группам применять цифровые инструменты и традиционные неформальные системы расчетов для обеспечения финансирования террористических актов.*

В рамках проведенного сравнительно-правового анализа систем финансового контроля государств-участниц БРИКС автор выявляет уязвимости действующих механизмов противодействия легализации преступных доходов. Особое внимание уделяет инструментам отслеживания сомнительных транзакций в цифровой среде.

Внедрение единых стандартов финансового мониторинга и синхронизация уголовной ответственности способствуют устранению правовых пробелов. Позволяют усовершенствовать межведомственный обмен данными и оперативно блокировать трансграничные каналы финансирования терроризма. В рамках исследования выявлены уязвимые места в механизмах противодействию финансированию терроризма и предложены меры по унификации уголовного законодательства стран объединения.

Ключевые слова: *БРИКС, финансирование терроризма, криптовалюта, рекомендации ФАТФ, сравнительное правоведение, уголовная ответственность, гармонизация законодательства, правоприменительная практика.*

TARASOV Aleksandr Anatolyevich,
Senior Lecturer at the Department of Criminal Law, Procedure and Criminology, Faculty of Law, National Research University Higher School of Economics (HSE University)

IMPROVING THE LEGAL REGULATION OF COUNTERING THE FINANCING OF TERRORISM WITHIN THE BRICS COUNTRIES

Annotation. *Legislative discrepancies among the BRICS member states create significant security risks. Divergent legal approaches within national frameworks enable radical groups to exploit digital tools and informal value transfer networks to sustain terrorist financing.*

A comparative analysis of financial control mechanisms across the BRICS bloc reveals key vulnerabilities in current anti-money laundering regimes, particularly regarding the tracking of suspicious transactions in the digital domain.

Implementing unified financial monitoring standards and aligning criminal liability will close existing legal loopholes, enhance cross-border interagency data sharing, and facilitate the swift freezing of illicit funds. Ultimately, this research identifies systemic gaps in countering terrorist financing and outlines concrete steps to unify criminal legislation across the association.

Key words: *BRICS, terrorist financing, cryptocurrency, FATF recommendations, comparative law, criminal liability, legislative harmonization, law enforcement.*

Современная цифровая трансформация применения транснациональным терроризмом сетевых коммуникаций требует от межгосударственных альянсов скоординированных правовых шагов. БРИКС, который объединяет 9 государств и охватывает 37% глобального ВВП и 46% населения мира, занимает центральное место в архитектуре международной безопасности. Следует отметить, что существующая разрозненность национальных законов заметно снижает общую результативность противодействия финансированию терроризма. Даже когда формально законодательство соответствует международным стандартам, на практике правоприменение остается фрагментированным. Юрисдикционные разрывы и отличия в определении терроризма дают радикальным структурам возможность переводить капиталы через криптовалюты и неформальные расчетные системы. Чтобы пройти через эти барьеры, мало просто привести термины к общему виду, нужен еще и общий механизм сквозного мониторинга транзакций. Именно этот переход от формального комплаенса к реальному усилению межведомственного взаимодействия сегодня и задает направление международно-правового сотрудничества [1].

Цель статьи состоит в том, чтобы разработать научно обоснованные решения для сближения правовых систем БРИКС и тем самым ускорить обмен данными и оперативную блокировку каналов снабжения терроризма. Методологическую основу работы составляет сравнительно-правовой анализ национальных законодательств, а также оценка того, как на практике внедряются Рекомендации ФАТФ и резолюции СБ ООН. Данный подход позволяет перевести фокус внимания на системные структурные проблемы осуществляемого странами БРИКС финансового контроля, найти пробелы в регулировании цифровых финансовых экосистем и понять, почему механизмы противодействия финансированию терроризма малоэффективны и не имеют общего синергетического эффекта [2].

Сравнительно-правовой анализ показывает, что ключевые определения и правовые основы механизмов, применяемых для перекрытия каналов финансирования терроризма, в национальных законодательствах России, Китая, Индии, Бразилии и ЮАР имеют существенные расхождения. Оценка имплементации Рекомендаций ФАТФ демонстрирует, что на фоне формального введения в национальные системы международных стандартов не произошло снятие барьеров в межведомственном взаимодействии. В этой связи автором разработаны рекомендации по сближению нормативной базы БРИКС. Предлагается ввести сквозные и общие для стран-участниц альянса подходы к мониторингу сомнительных транзакций, включая операции с виртуальными активами, и синхронизировать меры уголовной ответственности. Реализации данной меры приведет к формированию более прочной правовой основы для совместного своевременного оперативного реагирования и участия в трансграничных расследованиях.

Такая унификация нужна еще и потому, что БРИКС объединяет очень разные правовые системы и социально-политические модели. Это крупные развивающиеся экономики, у каждой свои институциональные возможности, и все они сталкиваются с общими угрозами отмывания доходов и транснациональной организованной преступности, но реагируют на них через собственные правовые традиции [4]. Эта институциональная автономия напрямую влияет на то, как в каждой стране формулируют понятие терроризма, а круг противоправных деяний там сегодня охватывается совершенно по-разному.

В Российской Федерации базовое понятие терроризма закреплено в Федеральном законе № 35-ФЗ «О противодействии терроризму». Законодатель определяет его как «идеологию насилия и практику воздействия на принятие решений органами власти или международными организациями, связанную с устрашением населения» [5], т.е. в отечественной доктрине основной упор традиционно делают на публичный характер угрозы.

В Китайской Народной Республике нормативный подход долгое время был довольно узким и сосредотачивался на конкретных актах физического насилия. Под давлением современных геополитических вызовов, дефиниция расширилась и стала жестко связываться с противодействием сепаратизму и религиозному экстремизму.

У Индии, Бразилии и ЮАР тоже есть свои особенности в нормативно-правовой базе. Индийская модель криминализации терроризма отличается высокой детализацией и широким охватом составов преступлений, и это явно связано с многолетним опытом борьбы с трансграничной и внутренней агрессией. Вместо коротких определений индийский законодатель перечисляет максимально подробно материальные, организационные и финансовые деяния, которые признаются террористическими актами. Внутриструктурные проявления терроризма в Индии делят по идеологическим основаниям: религиозно-экстремистский, сепаратистский и леворадикальный. Кроме того, в отличие от российского уголовного права в индийской доктрине наркотерроризм выделяется как отдельная форма террористической деятельности.

В Бразилии базовое понятие терроризма появилось в Федеральном законе № 13.260 от

16 марта 2016 года. В частности, юридически он определяется как умышленное действие, совершенное по мотивам ксенофобии, расовой, национальной, этнической или религиозной дискриминации, если цель указанных действий состоит в социальном или общем терроре, угрожающем личности, имуществу или общественной безопасности. До 2016 года в бразильском законодательстве не было единой формулировки "терроризма", хотя Конституция 1988 года [9] с самого начала относила террористическую деятельность к числу особо тяжких деяний, которые не подлежат амнистии. Толчком к принятию специального закона стала необходимость обеспечить безопасность перед Олимпийскими играми в Рио-де -Жанейро [10].

Южноафриканский подход, закрепленный в Законе № 33 от 2004 года «О защите конституционной демократии от террористической и связанной с ней деятельности», также имеет свою специфику. Модель ЮАР необычна тем, что она соединяет строгие международные стандарты безопасности с чувствительными механизмами защиты прав человека, что объясняется историей прошедшей через апартеид страны.

Таким образом, имеющийся в национальных законодательствах стран БРИКС нормативный дуализм создает почву для правовой неопределенности и тормозит оперативное взаимодействие правоохранительных органов между странами.

Аналогичный правовой диссонанс у участников БРИКС состоит и в понимании "финансирования терроризма". Российский законодатель идет по сравнительно узкому пути и связывает объективную сторону преступления с умышленным предоставлением или сбором средств для конкретных террористических актов либо для деятельности радикальных организаций. В КНР, наоборот, подход максимально широкий: туда попадает любая материальная поддержка террористических структур, даже если она не привязана к конкретному преступлению. В Бразилии же отдельного состава финансирования терроризма долгое время вообще не было, и из-за этого в правоприменении возникали серьезные пробелы.

Следует отметить, что внедрение международных стандартов ПОД/ФТ не стерло указанных различий. История развития антитеррористического законодательства в Индии и ЮАР показывает, что зачастую страны смешивают узкий и широкий подходы при конструировании составов преступлений лишь для формального соответствия требованиям ФАТФ. Особенно это заметно, когда речь заходит о цифровых валютах. Разные взгляды на сущность финансирования терроризма усложняют трансграничный мониторинг транзакций и межгосударственное взаимодействие.

Разнородность антитеррористического законодательства стран БРИКС снижает эффективность международной правовой помощи, потому что мешает реализации фундаментального принципа двойной криминализации. По этому правилу экстрадиция или исполнение запроса о правовой помощи возможны только тогда, когда инкриминируемое деяние считается преступлением в обеих юрисдикциях. На практике, если в России финансовая поддержка определенной структуры признается преступлением, а в Бразилии состав преступления не образуется, то межведомственное сотрудничество становится невозможным. Бразильская сторона в таком случае будет обязана отказать в официальном запросе, потому что для ее правового поля это действие формально законно. В результате юрисдикционные коллизии блокируют выдачу обвиняемых и останавливают обмен доказательствами.

Реализация процедур идентификации клиентов в странах БРИКС также демонстрирует применения различных подходов. Требования к алгоритмам установления конечных бенефициарных владельцев в Бразилии и России детально и четко регламентированы, а в Индии и КНР этот процесс менее формализован. Из-за различий в правовом регулировании транснациональным финансовым институтам приходится повторять комплаенс-проверки по несколько раз, что приводит к росту операционных издержек и ослабляет контроль. Разница хорошо видна при работе с клиентами из зон повышенной террористической активности. ЮАР и Китай применяют к ним обязательные процедуры усиленной проверки, тогда как в Индии и России такие механизмы выстроены менее системно. Наряду с этим, отсутствует общий для стран БРИКС список террористических организаций, что создает для банков непреодолимые процедурные барьеры, а радикальным структурам помогает скрывать настоящих владельцев преступных активов.

С мониторингом подозрительных транзакций ситуация тоже заметно разнится. Бразилия и Россия установили низкие пороговые значения для обязательного контроля операций, что помогает выявлять скрытые финансовые потоки, несмотря на большое количество ложных срабатываний. Индия и Китай, наоборот, держат пороги высокими. Для комплаенс-служб это снижает административную нагрузку, но у преступников появляется возможность безопасно осуществлять дробные регулярные переводы.

Исследователи считают, что эффективность и результативность мониторинга напрямую зависит от применяемого уровня автоматизации. При современных колоссальных темпах увеличении объема транзакций странам БРИКС необходима интеграция искусственного интеллекта и

машинного обучения в национальные системы финансовой безопасности [11]. В тоже время на практике цифровая трансформация буксует из-за различий в правовых традициях, регуляторных ограничений в сфере оборота данных и нехватки технологических ресурсов. В результате между формальным комплаенсом и реальной работой контроля происходит существенный разрыв.

Значительную долю проблем добавляют и виртуальные активы вместе с неформальными расчетными системами. Криптовалюты позволяют полностью обходить традиционный банковский сектор и дают прямой канал для трансграничной подпитки терроризма. Быстрое расширение этих теневых цифровых маршрутов создает правовые уязвимости в развивающихся экономиках БРИКС. Асимметрия регуляторных подходов в странах альянса дает спонсорам терроризма возможность использовать коллизии между юрисдикциями, обходить запреты и легализовать преступные доходы. Так, КНР держится линии абсолютного запрета на майнинг и коммерческий оборот частных токенов, а Россия перешла к модели жестко контролируемого допуска. Масштабная реформа российского рынка цифровых валют нацелена на то, чтобы вывести цифровые активы из серой зоны и снизить риски ПОД/ФТ [12].

Принятие Федерального закона № 282-ФЗ от 4 августа 2026 года «О цифровых валютах и цифровых правах» перевело оборот криптоактивов в РФ на регулируемую модель, близкую к фондовому рынку. Новые правила требуют обязательного лицензирования Банком России пяти категорий профессиональных участников: бирж, цифровых депозитариев, брокеров, управляющих и крупных обменников. Закон окончательно закрепил за цифровой валютой статус имущества и запретил использовать ее как внутреннее платежное средство. При этом расчеты криптовалютой по внешнеторговым контрактам, то есть в ВЭД, и сделки с российскими ценными бумагами были легализованы. Чтобы защитить розничных инвесторов и сделать рынок менее анонимным, регулятор ввел обязательное тестирование и защитный 48-часовой период охлаждения при крупных транзакциях [13].

Особый нормативный разнобой внутри объединения хорошо видно по стратегиям других участников. Бразилия развивает либеральную, но при этом структурированную правовую модель в рамках специального законодательства, а Индия и ЮАР довольно долго сочетали высокое фискальное давление с медленным формированием базовых правил для бизнеса [14]. Поскольку быстро унифицировать частные криптовалюты не получается, государства БРИКС смещают акцент в сторону интеграции цифровых валют центральных банков. Проекты по технологическому сопряжению цифрового рубля, цифрового юаня и цифровой рупии в единую платежную экосистему рассматриваются как легальная альтернатива традиционным межбанковским сетям и SWIFT, которая может убрать неконтролируемые трансграничные каналы перемещения ценностей [15].

Регуляторный дисбаланс преступные сообщества используют для того, чтобы без особых препятствий выводить капиталы в юрисдикции с мягким режимом комплаенса. Закрыть такие пробелы может только сквозная гармонизация правил обращения цифровых валют, подкрепленная скоординированными действиями государств на пространстве БРИКС. Даже когда национальные законы формально совпадают с глобальными стандартами, правоприменительная практика все равно упирается в системный кризис, а контроль слабеет из-за раздробленности норм. В таких условиях простое декларативное выполнение наднациональных регламентов практически теряет смысл, потому что для реального блокирования финансовых каналов терроризма нужны жесткое укрепление институтов контроля и прямой межведомственный обмен данными.

Рекомендации ФАТФ и резолюции Совета Безопасности ООН, в частности № 1373 и № 2462, задают нормативную основу глобального режима ПОД/ФТ. В основе этой системы лежит риск-ориентированный подход, который требует от государств оценивать внутренние угрозы и заранее направлять ресурсы туда, где риски самые острые [16]. Рекомендации 24 и 25, если говорить проще, требуют обязательно устанавливать конечных бенефициарных владельцев юридических лиц и трастов. Это нужно, чтобы трансграничные транзакции были хоть сколько-то прозрачными [17].

Сравнительно-правовой анализ показывал, что все страны БРИКС формально внедрили указанные международные стандарты в национальное право. В тоже время глубина встроенности в систему и механизмы правоприменения имеют существенные отличия [18]. Так, в рамках исследования автором выявлен разрыв между институциональным комплаенсом и реальной эффективностью правоприменения. Происходит утрата силы национальных законов из-за внутренней несогласованности норм, нехватки ресурсов у контролирующих и правоохранительных ведомств стран БРИКС, слабого технического оснащения и плохого взаимодействия между компетентными органами на международном уровне.

Практика правоприменения демонстрирует, что в случаях, если национальные нормативные базы концептуально расходятся, межведомственное взаимодействие в рамках БРИКС не осуществляется. Такой подход, в частности, при-

меняется при уголовном преследовании группировок, действующих на Ближнем Востоке или в Африке, в том числе филиалов ИГИЛ. Так, в России и Индии сбор денежных средств для таких структур безоговорочно квалифицируется как финансирование терроризма. При этом в Бразилии долгое время не существовало юридических оснований, позволяющих блокировать такие транзакции. Причина в том, что статья 2 бразильского Закона № 13.260 [8] требует обязательного наличия мотива ксенофобии либо расовой дискриминации и полностью исключает из состава преступления политические и идеологические цели. Такой терминологический вакуум создает почву для правового арбитража и позволяет преступным сетям вполне легально накапливать активы в «мягких» юрисдикциях.

Для решения выявленной проблемы, странам БРИКС необходимо выйти за рамки декларативного комплаенса. Единая дефиниция терроризма должна охватывать и насильственные действия, направленные на дестабилизацию власти, и их идеологическое обоснование. При этом следует держать баланс и учитывать национальную специфику, чтобы не спровоцировать конфликт с внутренним правопорядком государств. Согласованное определение финансирования терроризма должно включать и прямые, и косвенные способы передачи активов. Под жесткий контроль должны попадать транзакции через посредников, краудфандинговые платформы и благотворительные организации. Отдельного внимания требуют криптовалюты и неформальные платежные системы вроде "хавалы", которые используют для обхода банковского мониторинга. Если такие каналы будут квалифицированы единообразно, страны БРИКС смогут эффективнее блокировать теневые потоки, снизят уязвимость своих финансовых рынков и создадут прочную нормативную основу для совместной работы правоохранителей.

На практике отсутствие единых стандартов контроля над деятельностью некоммерческих организаций приводит к серьезным регуляторным сбоям. Например, индийское Агентство национальных расследований заблокировало функционирование НКО «Популярный фронт Индии», которая годами собирала средства под видом исламских благотворительных фондов. Указанная структура принимала пожертвования как наличными, так и в криптовалюте. В дальнейшем распределяла средства через сеть посредников для финансирования радикальных ячеек. Индийское законодательство [6] позволило жестко остановить схему внутри страны.

В то же время ЮАР долго находилась под критикой со стороны ФАТФ и была в «сером списке» именно из-за слабого контроля над некоммерческими организациями и цифровыми активами. Посредники использовали южноафриканские криптобиржи, чтобы пропускать средства террористическим группам, действующим в Мозамбике и Центральной Африке. Суды ЮАР не имели оперативного юридического инструмента, чтобы мгновенно арестовывать такие кошельки по запросу зарубежных партнеров, потому что не было синхронизированных дефиниций косвенного финансирования [19].

Для нейтрализации указанных угроз странам БРИКС также необходимы единые критерии подозрительных операций, выстроенные на стандартах ФАТФ. На их основе следует осуществлять автоматизированный мониторинг трансграничных переводов, поскольку при усложнении финансовых инструментов происходит некоторое отставание финансовых регуляторов и на первый план выходят сквозные автоматизированные комплексы, которые в реальном времени выявляют аномальные транзакции [3]. Таким образом, если цифровые индикаторы риска будут унифицированы, то национальные подходы к ПОД/ФТ можно будет согласовать, а превентивные межведомственные меры станут результативнее на всей территории стран БРИКС.

На практике автоматизация мониторинга и выравнивание индикаторов уже приступила к локальной работе в региональных форматах. В рамках Евразийской группы по противодействию отмыванию доходов и финансированию терроризма, куда входят Россия, Китай и Индия, уже разработана единая система криптоанализа. Росфинмониторинг активно использует программный комплекс «Прозрачный блокчейн» [20]. Этот инструмент в реальном времени отслеживает цепочки транзакций в биткоинах и стейблкоинах и маркирует кошельки, связанные с финансированием радикальных ячеек.

Структуры финансового мониторинга Индии внедрили платформу FINnet 2.0. Этот модернизированный комплекс использует искусственный интеллект и машинное обучение, чтобы автоматически собирать данные через субсистему FINGate и глубоко анализировать транзакции через FINCore. Система в реальном времени считает индексы рисков для физических и юридических лиц, сверяя банковские отчеты и данные криптобирж с внешними государственными базами [21].

Синхронизация процедур обмена данными между подразделениями финансовой разведки стран БРИКС требует унификации каналов связи и форматов отчетности. Необходима стандартизация отчетности, создание защищенных каналов связи и расширение прямых межведомственных соглашений. Если внедрить аналитические платформы на базе искусственного интел-

лекта, они смогут обрабатывать массивы разнородных данных из смежных юрисдикций и быстрее выявлять трансграничные цепочки подозрительных операций. При этом нехватка ресурсов у ведомств требует серьезной модернизации институциональной базы и перехода подразделений финансовой разведки стран БРИКС на единые цифровые стандарты.

Международные расследования показывают, что сквозной обмен информацией позволяет разрывать сложные теневые схемы. Так, результаты бразильской операции «Автомойка» это хорошо показали. Во время расследования масштабной коррупционной сети вокруг государственной нефтегазовой компании Petrobras правоохранительные органы столкнулись с запутанной цепочкой вывода активов через офшорные зоны. Положительный результат стал возможен лишь после того, как Федеральная полиция Бразилии и национальный Совет по контролю за финансовой деятельностью наладили прямую связь с финансовыми разведками других стран. Так удалось без лишней бюрократии отследить движение цифровых денежных средств и арестовать счета посредников за рубежом [22].

Массовое изъятие криптовалютных активов правоохранительными органами Сингапура в деле об отмывании доходов на сумму более 2,8 млрд долларов США тоже показало, насколько нужна технологическая унификация [23]. Преступная сеть скрывала конечных бенефициаров, используя децентрализованные платформы, но полиция Сингапура раскрыла схему благодаря мгновенному обмену цифровыми индикаторами и блокчейн-адресами с международными партнерами. Для стран БРИКС этот пример прямо говорит, что без единых форматов кодирования криптотранзакций невозможно эффективно преследовать технологически развитый криминалитет.

Установление согласованных правовых оснований для замораживания счетов требует баланса между суверенитетом национальных юрисдикций и международными обязательствами стран объединения. В основе указанных обеспечительных мер должны быть надежные механизмы, которые не только криминализируют финансовые преступления, но и обеспечивают оперативное отслеживание, арест и конфискацию теневых доходов. Отдельно необходимо регулировать виртуальные активы, потому что их трансграничное использование создает скрытые каналы для подпитки радикальных ячеек, пока правовая база в БРИКС остается фрагментированной. Если национальные процедуры блокирования активов будут синхронизированы, совместные расследования станут результативнее, каналы вывода капитала сузятся, а риски правового арбитража в слабоконтролируемых юрисдикциях снизятся.

На практике такие механизмы работают нормально только тогда, когда в законе есть четкие алгоритмы мгновенного действия. В Российской Федерации ключевым инструментом здесь выступает Федеральный закон № 115-ФЗ [24]. По его нормам Межведомственная комиссия по противодействию финансированию терроризма может мгновенно замораживать счета и блокировать любое имущество лиц, причастных к радикальной деятельности, во внесудебном порядке. Росфинмониторинг за считаные минуты доводит обновленные перечни до банков и криптобирж, и это фактически перекрывает вывод средств со счетов.

Международный стандарт, в частности Резолюция СБ ООН 1373, требует от государств замораживать средства террористов «без промедления», то есть в течение нескольких часов после запроса или обновления санкционного перечня. Но в таких странах БРИКС, как ЮАР или Бразилия, судебная процедура наложения ареста исторически требовала долгих межведомственных согласований. Из-за этого преступники успевали конвертировать фиатные деньги в анонимные криптовалюты и уводить их из-под удара [19]. Если внутри БРИКС синхронизировать внесудебные регламенты экстренной блокировки, ведомства смогут действовать зеркально и убрать этот временной лаг. Необходимо сблизить подходы к уголовной и административной ответственности за финансирование терроризма через унификацию составов преступлений, размеров санкций и процедур конфискации теневых доходов.

Различия в правоприменении и строгости наказания сильно мешают трансграничному возврату активов. Отслеживание преступных капиталов усложняется многослойными транзакциями, фирмами-однодневками и несовпадением юридических дефиниций, так что здесь нужно серьезно усиливать судебный и правоохранительный потенциал, в том числе через расширение соглашений о полицейском сотрудничестве. Этот межсистемный дисбаланс хорошо виден на примере привлечения к ответственности юридических лиц. Так, в России за финансирование терроризма предусмотрена строгая уголовная ответственность физических лиц (ст. 205.1 УК РФ), а к корпоративным структурам применяются жесткие административные санкции (ст. 15.27.1 КоАП РФ) вплоть до конфискации всего имущества.

В Бразилии же уголовная ответственность юридических лиц ограничена лишь экологическими преступлениями. Причастность к финансовым махинациям и террористическим сетям регулируется административным и гражданским правом в рамках Закона о чистой компании [22]. Из-за отсутствия уголовно-правового статуса у таких правонарушений бразильские ведомства долго

сталкивались с процедурными уязвимостями при трансграничном взыскании активов. Это осложняет исполнение международных следственных запросов и мешает арестовывать имущество подставных фирм за рубежом.

В индийском антитеррористическом праве, которое регулируется Законом о предотвращении отмывания денег [26], по ряду тяжких составов почти нет классических сроков давности для привлечения к ответственности. Это дает индийским правоохранительным органам возможность начинать конфискацию активов даже спустя много лет после совершения преступления. В других же юрисдикциях БРИКС строго регламентируемые процессуальные сроки давности позволяют блокировать исполнение старых индийских запросов, что также демонстрирует необходимость выравнивания материальных норм уголовного права.

Для устранения недостатков трансграничного сотрудничества, необходимо модернизировать механизмы взаимной правовой помощи и экстрадиции. Внутренняя фрагментация норм и коррупционные риски снижают результативность расследований, даже если национальные законы формально соответствуют стандартам ФАТФ. Совершенствование соглашений о правовой помощи ускорит уголовное преследование транснациональных преступных сетей. Для устранения пробелов необходима конвергенция законодательных систем, прозрачность, рост оперативных возможностей ведомств и укрепление взаимного доверия через прямые договоры о полицейском сотрудничестве. Результативность взаимодействия прямо зависит от того, готовы ли государства быстро реагировать на запросы коллег. Отдельное значение имеет расширение сети многосторонних соглашений с учетом специфики финансирования терроризма. Для лиц, которые подозреваются в финансировании радикальных структур, стоит предусмотреть упрощенные процедуры экстрадиции.

Страны БРИКС также сталкиваются с проблемой суверенного контроля над данными. По исследованию профессора Л. Белли, различие подходов к трансграничной передаче информации замедляет следствие. Оперативный обмен цифровыми уликами, такими как IP-адреса, логи блокчейн-транзакций и метаданные, требует выделенной защищенной сети [27]. Успешным примером преодоления такого рода барьеров является взаимодействие между Россией и Китаем, а также Индией и ЮАР. Прямые соглашения между Следственным комитетом РФ, МВД РФ и Министерством общественной безопасности КНР позволяют передавать данные о транзитных счетах хакеров и спонсоров экстремизма в течение нескольких часов, минуя громоздкие судебные процедуры [28]. Внедрение таких регламентов экспресс-экстрадиции и экспресс-выемки данных на уровне всей стран-участниц БРИКС критически важно для противодействия сетевому криминалитету.

Таким образом, проведенный сравнительно-правовой анализ национальных законодательств стран БРИКС выявил существенные расхождения в базовых дефинициях терроризма и механизмах финансового мониторинга. По мнению автора, именно терминологическая рассинхронизация порождает критические юрисдикционные разрывы. Из-за этого общая эффективность взаимодействия государств в рамках БРИКС заметно снижается. Когда квалификация преступлений расходится, базовое уголовно-процессуальное условие двойной криминализации деяния просто не выполняется. Это делает невозможной экстрадицию обвиняемых и блокирует передачу материалов уголовных дел между ведомствами. В частности, статья 2 бразильского Закона № 13.260 требует обязательного наличия мотива ксенофобии или расовой дискриминации и полностью исключает политические цели. Из-за этого суды Бразилии долго не могли блокировать счета лиц, связанных с ближневосточными террористическими структурами. Такой правовой вакуум позволяет преступным сетям использовать юрисдикционные разрывы для обхода регуляторных запретов, просто переводя деньги в страны со слабым или специфическим антитеррористическим законодательством.

Анализ имплементации международных стандартов показал, что формальное соответствие законов требованиям ФАТФ и резолюциям Совбеза ООН еще не означает реальной безопасности. Между декларативными нормами и практикой по-прежнему остается устойчивый разрыв. На практике внешняя легитимация национальных законов под международные стандарты часто носит декларативный характер, а децентрализация нормативного поля разрушает систему контроля финансовых транзакций.

Странам БРИКС уже пора переходить к тому, чтобы укреплять свои контролирующие структуры не на бумаге, а по-настоящему, и налаживать прямое трансграничное сотрудничество между ведомствами.

С учётом изложенного, автором сформулированы предложения по созданию общей правовой платформы для объединения.

Во-первых, необходима единая для стран БРИКС дефиниция терроризма и его косвенного финансирования. Такое согласованное определение должно охватывать и прямую, и косвенную передачу активов, в том числе через краудфандинговые платформы и благотворительные организации. Опыт Индии, где скрытое финан-

сирование радикальных ячеек через исламские фонды «Популярного фронта Индии» удалось пресечь, показывает, что за некоммерческим сектором нужен жесткий контроль.

Во-вторых, во всех юрисдикциях БРИКС следует ввести зеркальные механизмы мгновенной внесудебной блокировки счетов и ареста имущества. Если смотреть на российский опыт внесудебных решений по линии Росфинмониторинга, предусмотренный ФЗ № 115-ФЗ, то в ЮАР длительные судебные процедуры согласования исторически приводили к тому, что средства уходили в адрес террористических групп, действующих в Мозамбике. Если выровнять эти регламенты, ведомства БРИКС смогут работать без бюрократических проволочек.

В-третьих, разный подход стран БРИКС к цифровым валютам создает почву для правового арбитража. Китай придерживается жесткой запретительной политики, а Россия законом № 282-ФЗ перешла к модели контролируемого допуска с 48-часовым «периодом охлаждения» для крупных транзакций. Чтобы противостоять технологически развитому криминалитету, нужны единые цифровые стандарты контроля.

В-четвертых, обычный контроль должен уступать место автоматизированным аналитическим системам с искусственным интеллектом, которые обрабатывают трансграничные потоки данных в реальном времени. Внедрение сквозных цифровых индикаторов, по примеру российской системы «Прозрачный блокчейн» или индийской платформы «ФинНет», значительно повысят эффективность и результативность противодействия финансированию терроризма.

Список литературы:

[1] Ангриаван Р. Режимы противодействия отмыванию денег и мера возврата активов в борьбе с транснациональной организованной преступностью в контексте БРИКС-АСЕАН // Право. Журнал Высшей школы экономики. 2026. Т. 19, № 2. С. 273–297. DOI: 10.17323/2072-8166.2026.2.273.297..

[2] Lee B., Sims J., Lee Y.-T. BRICS expansion: threat or opportunity for ASEAN? // India Quarterly. 2025. Vol. 81, no. 2. Pp. 130–157. DOI: 10.1177/09749284251328226..

[3] Aksenova M. Legal Support of Artificial Intelligence in Countering Anti-Money Laundering and Terrorism Financing Regimes in the BRICS Plus Countries // BRICS Law Journal. 2024. Vol. 11, no. 3. Pp. 92–116. DOI: 10.21684/2412-2343-2024-11-3-92-116..

[4] Arnone G. Regulating the crypto-laundering chain: a comparative study of scam compounds and money mule mechanisms within criminal networks // Risks. 2026. Vol. 14, no. 4. Art. 96. Pp. 1–21. DOI: 10.3390/risks14040096.

[5] Российская Федерация. Законы. О противодействии терроризму : Федеральный закон № 35-ФЗ от 6 марта 2006 г. // Собрание законодательства Российской Федерации. 2006. № 11. Ст. 1146.

[6] Индия. Законы. О предотвращении противоправной деятельности : Федеральный закон № 37 от 30 декабря 1967 г. (с изм. и доп.) : [ориг. текст: The Unlawful Activities (Prevention) Act, 1967]. Section 15. URL: indiacode.nic.in (дата обращения: 25.08.2026). Режим доступа: электронный.

[7] Hoffman B. Inside terrorism. New York : Columbia University Press, 2006. 432 p. ISBN 978-0231126984.

[8] Бразилия. Законы. О противодействии терроризму : Федеральный закон № 13.260 от 16 марта 2016 г. : [ориг. текст: Lei № 13.260, de 16 de março de 2016] // Diário Oficial da União. 2016. 17 março (№ 52). Seção 1. P. 1.

[9] Бразилия. Конституция (1988). Конституция Федеративной Республики Бразилия : принята 5 октября 1988 г. : [ориг. текст: Constituição da República Federativa do Brasil de 1988] // Diário Oficial da União. 1988. 5 outubro (№ 191-A). Seção 1. P. 1–32.

[10] Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 : Act № 33 of 2004 // Government Gazette. 2005. 11 February (Vol. 476, № 27266). P. 1–58. URL: www.gov.za (дата обращения: 25.08.2026). Режим доступа: электронный.

[11] Belli L., Gaspar W. B., Jaswant S. S. Data sovereignty and data transfers as fundamental elements of digital transformation: lessons from the BRICS countries // Computer Law & Security Review. 2024. Vol. 54. Art. 106017. DOI: 10.1016/j.clsr.2024.106017..

[12] Jangirala S., Verma D. C., Yadav J. K., Srivastava S. K., Mandal A. Cryptocurrency Policy Stance of BRICS Countries // ICT Systems and Sustainability. Springer, 2025. Pp. 225–236. DOI: 10.1007/978-981-97-8591-9_20..

[13] Russia Is Launching a Legal Crypto Market: What Investors Need to Know / S. why NOT // Binance Square. 2026. 25 August. URL: binance.com (дата обращения: 25.08.2026). Режим доступа: электронный.

[14] Chudinovskikh M., Sevryugin V. Cryptocurrency regulation in the BRICS Countries and the Eurasian Economic Union // BRICS Law Journal. 2019. Vol. 6, iss. 1. Pp. 63–81. DOI: 10.21684/2412-2343-2019-6-1-63-81..

[15] Dulatova N., Abd Razak A. The Ecosystem of Cryptocurrency as an Object of Civil Rights in BRICS Countries // BRICS Law Journal. 2020. Vol. 7, iss. 2. Pp. 37–65. DOI: 10.21684/2412-2343-2020-7-2-37-65..

[16] The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation / Financial Action Task Force. Paris : FATF, 2012–2025. 140 p. URL: fatf-gafi.org (дата обращения: 25.08.2026). Режим доступа: электронный.

[17] Stankevičiūtė G. 40 Recommendations of the FATF — Overview // iDenfy. 2026. 20 August. URL: idenfy.com (дата обращения: 25.08.2026). Режим доступа: электронный.

[18] Staying Ahead of Financial Crime: Adhering to FATF Recommendations for Financial Institutions // Financial Crime Academy. 2026. 17 July. URL: financialcrimeacademy.org (дата обращения: 25.08.2026). Режим доступа: электронный.

[19] Mavhuru L., Chitimira H. An analysis of impact of the risk-based approach to combat money laundering and the financing of terrorism on financial inclusion in South Africa // Potchefstroom Electronic Law Journal. 2025. Vol. 28, no. 1. Pp. 1–30. DOI: 10.17159/1727-3781/2025/v28i0a21305..

[20] Резник О. Финансовая разведка (мониторинг) как эффективный способ в сфере борьбы с отмыванием денег / О. Резник [и др.] // Journal of Money Laundering Control. 2023. Т. 26, № 1. С. 94–105. DOI: 10.1108/JMLC-09-2021-0102..

[21] Financial Intelligence Unit arms itself with AI, ML tools to check money laundering // The Times of India. 2024. 5 May. URL: indiatimes.com (дата обращения: 25.08.2026). Режим доступа: электронный.

[22] Binotto A. Corporate liability after Car Wash: spillovers to Brazilian corporate law on liability // Oñati Socio-Legal Series. 2025. Vol. 15, no. 3. Pp. 85–94. DOI: 10.35295/osls.iisl.2292.

[23] Zhou H. Y. Regulating crypto money laundering: an assessment of current regulatory responses and potentials for technology-based solutions // Stanford Journal of Blockchain Law & Policy. 2025. Vol. 8, no. 1. Pp. 142–176. URL: stanford.edu (дата обращения: 25.08.2026). Режим доступа: электронный.

[24] Российская Федерация. Законы. О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма : Федеральный закон № 115-ФЗ от 7 августа 2001 г. // Собрание законодательства Российской Федерации. 2001. № 33. Ст. 3418.

[25] Бинотто А. Корпоративная ответственность после операции «Автомойка»: влияние на бразильское корпоративное право в сфере деликтной ответственности // Oñati Socio-Legal Series. 2025. Т. 15, № 3. С. 85–94. DOI: 10.35295/osls.iisl.2292.

[26] Баджпаи Г. С., Пал Г. Отсутствие срока давности в Законе Индии о предотвращении отмывания денег 2002 года: анализ влияния на правовую определенность и фундаментальные права // Journal of Illicit Trade, Financial Crime, and Compliance. 2025. Т. 1, № 1. С. 27–36. DOI: 10.65879/3070-6122.2025.1.04..

[27] Белли Л., Гаспар В. Б., Джасвант С. С. Цифровой суверенитет и трансграничная передача данных как фундаментальные элементы цифровой трансформации: опыт стран БРИКС // Computer Law & Security Review. 2024. Т. 54. Ст. 106017. DOI: 10.1016/j.clsr.2024.106017..

[28] Тьебо Р. Роль транснационального правового процесса в продвижении повестки устойчивого развития в рамках БРИКС // Journal of Law and Sustainable Development. 2024. Т. 12, № 10. С. e3997. DOI: 10.55908/sdgs.v12i10.3997..

References:

[1] Angriawan R. Anti-money laundering regimes and asset recovery measures in the fight against transnational organized crime in the context of BRICS-ASEAN // Law. Journal of the Higher School of Economics. 2026. VOL. 19, NO. 2. S. 273-297. DOI: 10.17323/2072-8166.2026.2.273.297. .

[2] Lee B., Sims J., Lee Y.-T. BRICS expansion: threat or opportunity for ASEAN? // India Quarterly. 2025. Vol. 81, no. 2. Pp. 130–157. DOI: 10.1177/09749284251328226..

[3] Aksenova M. Legal Support of Artificial Intelligence in Countering Anti-Money Laundering and Terrorism Financing Regimes in the BRICS Plus Countries // BRICS Law Journal. 2024. Vol. 11, no. 3. Pp. 92–116. DOI: 10.21684/2412-2343-2024-11-3-92-116..

[4] Arnone G. Regulating the crypto-laundering chain: a comparative study of scam compounds and money mule mechanisms within criminal networks // Risks. 2026. Vol. 14, no. 4. Art. 96. Pp. 1–21. DOI: 10.3390/risks14040096.

[5] Russian Federation. Laws. On countering terrorism: Federal Law No. 35-FZ of March 6, 2006 // Collection of legislation of the Russian Federation. 2006. № 11. Art. 1146.

[6] India. Laws. On the prevention of illegal activities: Federal Law No. 37 of December 30, 1967 (amended and supplemented): [orig. текст: The Unlawful Activities (Prevention) Act, 1967]. Section 15. URL: indiacode.nic.in (access date: 25.08.2026). Access mode: electronic.

[7] Hoffman B. Inside terrorism. New York : Columbia University Press, 2006. 432 p. ISBN 978-0231126984.

[8] Brazil. Laws. On countering terrorism: Federal Law No. 13.260 of March 16, 2016: [orig. текст: Lei № 13.260, de 16 de março de 2016] // Diário Oficial da União. 2016. 17 março (№ 52). Seção 1. P. 1.

[9] Brazil. Constitution (1988). Constitution of the Federative Republic of Brazil: Adopted on

October 5, 1988: [orig. текст: Constituição da República Federativa do Brasil de 1988] // Diário Oficial da União. 1988. 5 outubro (№ 191-A). Seção 1. P. 1–32.

[10] Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 : Act № 33 of 2004 // Government Gazette. 2005. 11 February (Vol. 476, № 27266). P. 1–58. URL: www.gov.za (access date: 25.08.2026). Access mode: electronic.

[11] Belli L., Gaspar W. B., Jaswant S. S. Data sovereignty and data transfers as fundamental elements of digital transformation: lessons from the BRICS countries // Computer Law & Security Review. 2024. Vol. 54. Art. 106017. DOI: 10.1016/j.clsr.2024.106017..

[12] Jangirala S., Verma D. C., Yadav J. K., Srivastava S. K., Mandal A. Cryptocurrency Policy Stance of BRICS Countries // ICT Systems and Sustainability. Springer, 2025. Pp. 225–236. DOI: 10.1007/978-981-97-8591-9_20..

[13] Russia Is Launching a Legal Crypto Market: What Investors Need to Know / S. why NOT // Binance Square. 2026. 25 August. URL: binance.com (access date: 25.08.2026). Access mode: electronic.

[14] Chudinovskikh M., Sevryugin V. Cryptocurrency regulation in the BRICS Countries and the Eurasian Economic Union // BRICS Law Journal. 2019. Vol. 6, iss. 1. Pp. 63–81. DOI: 10.21684/2412-2343-2019-6-1-63-81..

[15] Dulatova N., Abd Razak A. The Ecosystem of Cryptocurrency as an Object of Civil Rights in BRICS Countries // BRICS Law Journal. 2020. Vol. 7, iss. 2. Pp. 37–65. DOI: 10.21684/2412-2343-2020-7-2-37-65..

[16] The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation / Financial Action Task Force. Paris : FATF, 2012–2025. 140 p. URL: fatf-gafi.org (access date: 25.08.2026). Access mode: electronic.

[17] Stankevičiūtė G. 40 Recommendations of the FATF — Overview // iDenfy. 2026. 20 August. URL: idenfy.com (access date: 25.08.2026). Access mode: electronic.

[18] Staying Ahead of Financial Crime: Adhering to FATF Recommendations for Financial Institutions // Financial Crime Academy. 2026. 17 July. URL: financialcrimeacademy.org (access date: 25.08.2026). Access mode: electronic.

[19] Mavhuru L., Chitimira H. An analysis of impact of the risk-based approach to combat money laundering and the financing of terrorism on financial inclusion in South Africa // Potchefstroom Electronic Law Journal. 2025. Vol. 28, no. 1. Pp. 1–30. DOI: 10.17159/1727-3781/2025/v28i0a21305..

[20] Reznik O. Financial intelligence (monitoring) as an effective way to combat money laundering/O. Reznik [et al.] // Journal of Money Laundering Control. 2023. T. 26, NO. 1. S. 94-105. DOI: 10.1108/JMLC-09-2021-0102..

[21] Financial Intelligence Unit arms itself with AI, ML tools to check money laundering // The Times of India. 2024. 5 May. URL: indiatimes.com (access date: 25.08.2026). Access mode: electronic.

[22] Binotto A. Corporate liability after Car Wash: spillovers to Brazilian corporate law on liability // Oñati Socio-Legal Series. 2025. Vol. 15, no. 3. Pp. 85–94. DOI: 10.35295/osls.iisl.2292.

[23] Zhou H. Y. Regulating crypto money laundering: an assessment of current regulatory responses and potentials for technology-based solutions // Stanford Journal of Blockchain Law & Policy. 2025. Vol. 8, no. 1. Pp. 142–176. URL: stanford.edu (access date: 25.08.2026). Access mode: electronic.

[24] Russian Federation. Laws. On combating the legalization (laundering) of proceeds from crime and the financing of terrorism: Federal Law No. 115-FZ of August 7, 2001 // Collection of Legislation of the Russian Federation. 2001. № 33. Art. 3418.

[25] Binotto A. Corporate Responsibility after Operation Car Wash: Impact on Brazilian Corporate Law in the Area of Tort Liability // Oñati Socio-Legal Series. 2025. VOL. 15, NO. 3. S. 85-94. DOI: 10.35295/osls.iisl.2292.

[26] Bajpayee GS, Pal G. No Statute of Limitations in the Indian Money Laundering Prevention Act, 2002: An Analysis of the Impact on Legal Certainty and Fundamental Rights // Journal of Illicit Trade, Financial Crime, and Compliance. 2025. T. 1, NO. 1. S. 27-36. DOI: 10.65879/3070-6122.2025.1.04..

[27] Belli L, Gaspar WB, Jaswant S. S. Digital sovereignty and cross-border data transfer as fundamental elements of digital transformation: the experience of the BRICS countries // Computer Law & Security Review. 2024. T. 54. Art. 106017. DOI: 10.1016/j.clsr.2024.106017..

[28] Tjebo R. The role of the transnational legal process in advancing the BRICS sustainable development agenda // Journal of Law and Sustainable Development. 2024. T. 12, NO. 10. C. e3997. DOI: 10.55908/sdgs.v12i10.3997..