Дата поступления рукописи в редакцию: 30.07.2026 г.
Дата принятия рукописи в печать: 06.08.2026 г.
DOI: 10.24412/2224-9133-2026-7-224-229

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

ЦИФРОВЫЕ И КВАЗИФИНАНСОВЫЕ КАНАЛЫ СОДЕЙСТВИЯ ТЕРРОРИЗМУ: ГОСУДАРСТВЕННО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ

Аннотация. *В статье приведены результаты авторского исследования особенностей трансформации ресурсной базы обеспечения террористической деятельности. Рассматриваются актуальные проблемы уголовно-правовой квалификации финансирования терроризма, осуществляемого с использованием цифровых децентрализованных платежных инструментов. Сделан вывод о том, что современный технологический сектор предопределил качественную эволюцию способов оказания содействия террористической деятельности, при которой традиционные фиатные расчеты замещены скрытой цифровой и квазифинансовой инфраструктурой. Действующая правоприменительная практика, основанная на консервативных подходах, сталкивается с трудностями при фиксации преступлений, совершаемых с использованием анонимизированных виртуальных активов, трансграничных расчетных систем и неверифицируемых банковских карт. Автор ретроспективно прослеживает эволюцию обеспечительных механизмов радикальных структур. В результате приходит к обоснованному выводу о необходимости внедрения критерия «цифровой заведомости» для эффективного доказывания прямого умысла. Авторский алгоритм оценки действий жертвы в сочетании с предлагаемыми изменениями в диспозицию статьи 205.1 УК России позволит сформировать единообразную правоприменительную практику на фоне современных угроз национальной безопасности.*

Автор аргументированно утверждает, что, несмотря на тотальный контроль в глобальной банковской сфере, радикальные структуры до сих пор находят лазейки для финансового обеспечения террористической деятельности. В качестве ключевого инструмента задействуются возможности децентрализованных сетей и сервисы анонимизации криптовалют. Для эффективного пресечения террористических квазифинансовых схем государству необходимо расширять рамки криминологического контроля. Очевидно, что противодействовать необходимо не только с координаторами финансовых сборов. Контроль должен охватить всю цепочку посредников, вплоть до номинальных держателей карт и счетов, которые обеспечивают техническую сторону перевода денежных средств.

Ключевые слова: *содействие террористической деятельности; финансирование терроризма; ст. 205.1 УК России; судебная практика; криптоактивы; система «хавала»; дроп-карты; ИТ-мошенничество; квалификация преступлений; виктимологическая профилактика.*

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)

DIGITAL AND QUASI-FINANCIAL CHANNELS OF COMPLICITY IN TERRORISM: STATE-LEGAL REGULATION AND PROBLEMS OF CRIME QUALIFICATION

Annotation. *The article, which develops a series of studies on the transformation of the resource base of organized crime, deals with the problems of criminal law and criminological qualification of terrorist financing through modern decentralized payment tools. It was the technological sector that predetermined the qualitative evolution of methods of assisting terrorist activity, in which traditional fiat settlements are replaced by a hidden digital and quasi-financial infrastructure. Current investigative practice, based on conservative approaches, faces serious difficulties in capturing crimes committed using anonymized virtual assets, transborder settlement systems ("hawala") and proxy bank cards (drop-cards). Author retrospectively traces the evolution of the securing mechanisms of radical structures and substantiates the necessity of introducing the "digital knowledge standard" for effective proof of direct intent. The developed algorithm for assessing the actions of the subject in combination with the doctrinal project of amendments to Article 205.1 of the Criminal Code of the Russian Federation is intended to serve as a great help for the formation of uniform judicial practice against the background of modern threats to national security.*

Why, in conditions of total control and transparency of the global banking system, decentralized shadow networks and cryptocurrency mixers are still unhindered used by international terrorist organizations for accumulation and cross-border movement of colossal capitals? The law enforcer intends to expand the scope of preventive criminological control — not only regarding the organizers of fundraising, but also regarding the entire network of technical intermediaries, including nominee cardholders.

Key words: *assisting terrorist activity; terrorist financing; Article 205.1 of the Criminal Code of the Russian Federation; judicial practice; crypto-assets; hawala system; drop-cards; IT fraud; qualification of crimes; victimological prevention.*

Обеспечение национальной безопасности Российской Федерации в условиях беспрецедентного внешнего давления требует постоянного пересмотра уголовно-правовых подходов к пресечению каналов материального обеспечения организованной преступности и террористических структур. Сегодня экономическая основа терроризма претерпевает серьезные изменения. Привычные банковские переводы и наличные расчеты уступают место скрытой цифровой инфраструктуре. Затрагиваемая проблема имеет важное значение для теории и практики уголовного права. Проблемы материального обеспечения террористической деятельности традиционно находятся в фокусе внимания отечественных исследователей.

Базовые вопросы соучастия в преступлениях заложены в трудах Ю. А. Клименко. Исследователь выявил критерии классификации преступного взаимодействия по формам, сформулировал авторское определение данного понятия и систематизировал варианты совместного совершения преступлений, в том числе террористического характера, выделив пять форм соучастия в Общей части УК РФ и десять его видов в Особенной части [1, с. 157]. Проблемы квалификации специальных форм содействия такой деятельности и участия в групповых структурах террористической направленности детально исследованы в работах Д. К. Бокова [2, с. 25].

В свою очередь, актуальные проблемы противодействия сопутствующему теневому перемещению капиталов и современные стандарты финансового мониторинга изучены в работах В. В. Красинского [3, с. 15], который сфокусировался на высокотехнологичных угрозах, проведя глубокий криминологический анализ блокчейн-платформ, систем отслеживания криптовалютных транзакций и современных механизмов финансирования терроризма. Риски цифровой трансформации для уголовного права и проблемы обеспечения безопасности в информационной среде подробно исследованы Е. А. Капитоновой [4, с. 96], уделившей особое внимание уголовно-правовым рискам новых форм девиантных действий в интернет-пространстве (пранков, треш-стримов и нелегальных онлайн-трансляций). При этом специфика современного виктимологического анализа и снижения рисков латентной вовлеченности потенциальных жертв в террористическую активность, в том числе с учетом психологических, социальных и информационных факторов цифровизации, системно раскрывается в новейших интегративных исследованиях А. Г. Черявко и М. В. Майбороды [5].

Безусловно, эти исследования имеют колоссальное значение для науки. Однако новейшие технологические тренды объективно остались за рамками прежних дискуссий. Точно так же и действующий текст статьи 205.1 Уголовного кодекса

Российской Федерации [6] и вместе устоявшимися разъяснения Пленума Верховного Суда Российской Федерации [7] создавались в то время, когда правоприменитель имел дело исключительно с традиционными, классическими финансовыми расчетами.

Современная криминологическая ситуация характеризуется масштабным использованием преступниками анонимных электронных кошельков, трансграничных внебанковских сетей взаимных расчетов, подставных банковских карт и схем телефонного мошенничества. На фоне глобальной цифровизации правоохранительные органы сталкиваются с трудностями при правовой оценке высокотехнологичных противоправных явлений. При этом отсутствие единого подхода к фиксации подобных технологических «цифровых следов» затрудняет реализацию принципа неотвратимости наказания и требует адаптации уголовно-правовых подходов к современным реалиям.

Проводимый авторский анализ позволяет взглянуть на институт соучастия в террористической деятельности шире, отказавшись от консервативного понимания финансирования исключительно как материального обеспечения. Для описания этих процессов целесообразно использовать понятие «квазифинансовой инфраструктуры терроризма», обозначающее латентную, функционирующую вне государственного контроля систему децентрализованных институтов передачи ценностей (в том числе виртуальных) умышленно используемую террористическими организациями для обхода защитных фильтров национальных мониторинговых структур. Введение этой дефиниции создаст возможность более точно дифференцировать ответственность технических посредников и детально описать современные бесконтактные механизмы ресурсного обеспечения терроризма.

Результаты анализа показывают, что внутри современной структуры квафинансирования терроризма прослеживается деление участников на два основных уровня. К первому относятся организаторы и координаторы сборов, выполняющие организационно-управленческие задачи. Второй уровень формируют технические посредники. К ним относятся всевозможные операторы систем неформальных расчетов, предоставляющие инструменты анонимизации, а также номинальные владельцы банковских счетов («дропперы»). Такая дифференциация позволяет точнее определить характер содействия преступным группам, степень осведомленности каждого соучастника и индивидуализировать ответственность по статье 205.1 УК России.

Чтобы правильно разделить ответственность теневых посредников, необходимо точно определить, чего именно они хотели и что осознавали. Для этого предлагается ввести в научный оборот и использовать критерий «цифровой заведомости». Он работает как технический алгоритм. Если человек в момент перевода денег специально использует программы для сокрытия своих платежей, то является прямым доказательством наличия у него противоправного умысла.

На фоне внедрения криптовалюты в криминальный оборот у правоприменителей возникают сложности в определении точного момента окончания финансирования терроризма, поскольку цифровые денежные средства проходят многоэтапные цепочки подставных кошельков и криптообменники. Для квалификации преступления по статье 205.1 УК России принципиален сам факт того, что человек безвозвратно отдал деньги или имущество, прекрасно понимая, кому и зачем они пойдут. Если речь идет о цифровых платежах, то финансирование терроризма возможно считать оконченным в момент, когда фиксация транзакции о переводе появляется в блокчейне. По мнению автора, именно в данный момент отправитель теряет контроль над находившейся в его распоряжении криптовалютой. При этом получатель (или связанные с ним посредники) этот контроль приобретают.

Последующая конвертация цифровой валюты в наличные деньги лежит за пределами объективной стороны данного состава преступления и относится к стадии реализации преступных доходов[3].

Специфика функционирования внебанковской системы «хавала» заключается в том, что трансграничный перевод ценностей осуществляется на основе клирингового взаимозачета между крипто-брокерами, в результате чего физического перемещения денег через государственную границу не происходит. Передача наличных средств посреднику внутри страны влечет автоматическую выдачу эквивалентной суммы в целевом регионе, что полностью выводит транзакцию из-под контроля органов финансового мониторинга.

Сложность квалификации действий указанных брокеров связана с определением их роли в соучастии финансирования терроризма. Вменение статьи 205.1 УК России теневому спонсору обоснованно только при наличии прямых доказательств его осведомленности о конечном деструктивном векторе движения денег. Если же посредник действует вслепую, обеспечивая лишь транзит в рамках общего теневого бизнеса, его деяние подпадает под признаки состава преступления, предусмотренного статьей 172 УК России, т.е. квалифицируется как незаконная банковская деятельность. В этом случае отправитель средств несет самостоятельную ответственность за финансирование терроризма через квазифинансо-

вый институт. Данный подход соотносится с международным опытом [8], где режимы контроля за неформальными платежными системами встроены в общую структуру противодействия отмыванию доходов.

Сходные проблемы возникают при оценке деятельности номинальных владельцев счетов, чьи карты используются как базовый низовой элемент для сбора средств. Правоохранительные органы нередко автоматически рассматривают «дропперов» в качестве соучастников финансирования терроризма. В тоже время разграничение составов здесь, по мнению автора, также должно проводиться через оценку направленности умысла. Если лицо передает платежное средство за вознаграждение без понимания специфики его дальнейшего использования, содеянное образует состав неправомерного оборота средств платежей, предусмотренный статьей 187 УК России. Если же доказано, что лицо предоставляло банковские карты, достоверно зная, что их реквизиты используются интернет-ресурсами террористических организаций, его действия подлежат прямой квалификации по части 1.1 статьи 205.1 УК России.

Серьезным вызовом последних лет стала интеграция инструментов социальной инженерии в схемы ресурсного обеспечения терроризма. Денежные средства граждан, похищаемые под видом перевода на «безопасные счета», транзитом направляются на материально-техническое обеспечение запрещенных военизированных формирований. Правовой статус лица, ставшего жертвой психологического воздействия и лично переведшего денежные средства, зависит от наличия умысла. Отсутствие осознания лицом общественно опасного характера своих действий исключает субъективную сторону преступления, предусмотренного статьей 205.1 УК России. Обманутый гражданин должен рассматриваться в качестве потерпевшего от мошенничества (статья 159 УК России). Напротив, действия организаторов таких мошеннических колл-центров обладают повышенной общественной опасностью. Требуют вменения по совокупности преступлений и привлечению к ответственности за хищение чужого имущества путем обмана и последующее умышленное финансирование террористической деятельности.

Одной из наиболее сложных проблем на практике остается доказывание прямого умысла, когда сбор денежных средств маскируется под легитимную благотворительность или гуманитарную помощь. Для преодоления этих трудностей предлагается также использовать критерий «цифровой заведомости». Он более точно позволит сделать вывод о намерениях лица на основе анализа объективно оставляемых им электронных следов.

Наличие прямого умысла на финансирование террористической деятельности можно считать доказанным при фиксации судом четкой цепочки взаимосвязанных факторов. В качестве отправной точки выступает сам факт транзакции на адрес крипто-кошелька или счет, который на момент перевода уже находился в так называемых «черных списках» Росфинмониторинга. Далее суду необходимо оценить технологическое маскирование платежа, при котором отправитель осознанно прятал свой сетевой след с помощью VPN-сервисов, защищенных браузеров или криптомиксеров. Логическим завершением этой цепочки является фиксация конспиративного характера общения перед переводом, когда переписка велась исключительно в «секретных чатах» мессенджеров с функцией автоматического удаления сообщений.

Такая последовательность действий позволит обоснованно констатировать наличие умысла и исключить версию подсудимого о якобы добросовестном заблуждении. Использование данного формата позволит заменить оценку противоречивых устных показаний анализом объективных, материально фиксируемых технических данных.

Перспективным направлением в правоприменении также видится адаптация классических институтов уголовного права для точной индивидуализации ответственности лиц, ставших объектом технологического манипулирования.

Для нормативного закрепления выработанных подходов предлагается расширить понятие финансового обеспечения преступной деятельности, изложив Примечание 1 к статье 205.1 УК РФ в следующей редакции:

«Под финансированием терроризма в настоящем Кодексе понимается предоставление или сбор средств либо оказание финансовых услуг, а равно предоставление, сбор, обмен, смешивание или перемещение цифровых финансовых активов, цифровой валюты, электронных денежных средств, равно как и использование неформальных расчетно-клиринговых систем, с осознанием того, что они предназначены для финансирования организации, подготовки или совершения хотя бы одного из преступлений, предусмотренных настоящей статьей…»

Введение данной дефиниции позволит однозначно зафиксировать на законодательном уровне, что виртуальные активы и неформальные расчеты признаются полноценным предметом и способом совершения преступления, независимо от их физической формы или легального статуса.

Автор также считает, что обоснованная в исследовании дифференциация ответственности технических посредников требует нормативного закрепления. В этих целях предлагается допол-

нить части 1 и 1.1 статьи 205.1 УК РФ квалифицирующим признаком, предусматривающим повышенную ответственность за совершение преступления «с использованием сети Интернет, цифровых валют, анонимных платежных инструментов или с привлечением номинальных владельцев средств платежа».

Реализация данных предложений в правоприменительной сфере унифицирует подходы к определению момента окончания преступления, совершаемого через бесконтактные распределенные платформы. Суды и органы предварительного расследования получат четкие нормативные ориентиры, что позволит минимизировать риски ошибочного вменения смежных составов и исключит уклонение от ответственности виновных лиц под предлогом отсутствия фиатных денег в транзакциях. В сфере предупреждения преступлений криминологический контроль использования подставных карт и анонимных систем расчетов окажет сдерживающее воздействие на лиц, предоставляющих свои платежные инструменты теневому сектору экономики, разрушая обеспечительную инфраструктуру преступных организаций на ее начальном, низовом уровне.

Выделение цифровой и квазифинансовой инфраструктуры в качестве самостоятельного объекта уголовно-правовой защиты открывает новые перспективы для научного развития понятия «соучастие». Практическое внедрение предложенного в работе стандарта «цифровой заведомости» в сочетании с проектом изменений в статью 205.1 УК РФ будет способствовать повышению эффективности деятельности правоохранительных органов в квалификации преступлений, обеспечивая единообразие и укрепление национальной безопасности России.

Список литературы:

[1] Клименко, Ю. А. Классификация соучастия: формы, виды, значение для уголовно-правовой оценки преступления / Ю. А. Клименко. — DOI 10.17803/1729-5920.2016.114.5.156-168 // Lex russica (Закон русской науки). — 2016. — № 5 (114). — С. 156–168. — URL: https://doi.org/10.17803/1729-5920.2016.114.5.156-168 (дата обращения: 28.07.2026).

[2] Боков, Д. К. Финансирование терроризма: спорные вопросы квалификации / Д. К. Боков. — DOI 10.18572/1812-3783-2024-12-25-28 // Российский следователь. — 2024. — № 12. — С. 25–28. — URL: https://lawinfo.ru/articles/8764/finansirovanie-terrorizma-spornye-voprosy-kvalifikacii (дата обращения: 28.07.2026).

[3] Красинский, В. В. Борьба с финансированием терроризма и экстремизма : монография / В. В. Красинский. — Москва : ИНФРА-М, 2021. — 184 с. — (Научная мысль). — ISBN 978-5-16-015843-3. — URL: https://znanium.ru/catalog/document?id=358941 (дата обращения: 28.07.2026).

[4] Терроризм и современное право: актуальные вопросы противодействия : монография / О. В. Безрукова, Е. А. Капитоновой, Г. П. Кулешова [и др.] ; под ред. Г. Б. Романовского. — Москва : Проспект, 2023. — 176 с. — ISBN 978-5-392-27437-6. — URL: https://book.ru/book/937567 (дата обращения: 28.07.2026).

[5] Черявко Е. Д., Майборода Э. Т. Интегративная модель виктимологии терроризма: междисциплинарный подход // Психология и право. 2026. Т. 16, № 1. С. 223–239. DOI: 10.17759/psylaw.2026160114..

[6] Уголовный кодекс Российской Федерации : федер. закон от 13.06.1996 № 63-ФЗ (ред. от 30.01.2026) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

[7] О некоторых вопросах судебной практики по уголовным делам о преступлениях террористической направленности : Постановление Пленума Верховного Суда РФ от 09.02.2012 № 1 (ред. от 28.10.2021) // Бюллетень Верховного Суда РФ. 2012. № 4.

[8] Central Prevention of Money-Laundering Act, 2002. Financial Intelligence Unit – India, 2022.

References:

[1] Klimenko, Yu. A. Classification of complicity: forms, types, significance for the criminal law assessment of the crime/Yu. A. Klimenko. - DOI 10.17803/1729-5920.2016.114.5.156-168 // Lex russica (Law of Russian Science). — 2016. — № 5 (114). - S. 156-168. - URL: https://doi.org/10.17803/1729-5920.2016.114.5.156-168 (access date: 28.07.2026).

[2] Bokov, D. K. Financing of Terrorism: Controversial Qualification Issues/D. K. Bokov. - DOI 10.18572/ 1812-3783-2024-12-25-28 // Russian investigator. — 2024. — № 12. - S. 25-28. — URL: https://lawinfo.ru/articles/8764/finansirovanie-terrorizma-spornye-voprosy-kvalifikacii (дата обращения: 28.07.2026).

[3] Krasinsky, V.V. The fight against the financing of terrorism and extremism: monograph/ V.V. Krasinsky. - Moscow: INFRA-M, 2021. - 184 p. - (Scientific thought). — ISBN 978-5-16-015843-3. - URL: https://znanium.ru/catalog/document?id=358941 (access date: 28.07.2026).

[4] Terrorism and modern law: topical issues of counteraction: monograph/O. V. Bezrukova, E. A. Kapitonova, G. P. Kuleshova [and others]; ed. G. B. Romanovsky. - Moscow: Prospekt, 2023. - 176 p. - ISBN 978-5-392-27437-6. - URL: https://book.ru/book/937567 (access date: 28.07.2026).

[5] Cheryavko E. D., Mayboroda E. T. Integrative model of victimology of terrorism: interdisciplinary approach // Psychology and law. 2026. VOL. 16, NO. 1. S. 223-239. DOI: 10.17759/psylaw.2026160114..

[6] Criminal Code of the Russian Federation:

feder. Law of 13.06.1996 No. 63-FZ (as amended by 30.01.2026) // Collection of Legislation of the Russian Federation. 1996. № 25. Art. 2954.

[7] On some issues of judicial practice in criminal cases of terrorist crimes: Resolution of the Plenum of the Supreme Court of the Russian Federation of 09.02.2012 No. 1 (ed. 28.10.2021) // Bulletin of the Supreme Court of the Russian Federation. 2012. № 4.

[8] Central Prevention of Money-Laundering Act, 2002. Financial Intelligence Unit – India, 2022.