

**ПРАВОВАЯ ПРИРОДА И КРИМИНАЛИСТИЧЕСКИЕ ОСОБЕННОСТИ
ФИНАНСИРОВАНИЯ ТЕРРОРИЗМА С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ**

<https://doi.org/10.5281/zenodo.16860808>

Нажмитдинов Нодирхон Амриллохонович

Соискатель Университета общественной безопасности Республики

Узбекистан; E-mail: amrilloxon47@gmail.com

Аннотация. В настоящей статье автором исследуются вопросы осуществления криптовалютных платежей. Особое внимание уделяется децентрализованным контент-сетям, блокчейн-технологиям, криптобиржам, криптообменникам и специальным сервисам с функцией рандомизации как источникам получения криминалистически значимой информации. Предлагаются организационно-тактические и следственные рекомендации по расследованию финансирования терроризма, осуществляемого посредством криптовалютных транзакций.

Ключевые слова: финансирование терроризма, криптовалюта, блокчейн, криптобиржа, криптокошелек, аудит блокчейна, «миксеры».

**THE LEGAL NATURE AND FORENSIC CHARACTERISTICS OF TERRORISM FINANCING
THROUGH THE USE OF CRYPTOCURRENCIES**

Najmitdinov N.A.

Applicant to the University of Public Security

of the Republic of Uzbekistan; E-mail: amrilloxon47@gmail.com

Abstract. This article explores issues related to the execution of cryptocurrency payments. Special attention is given to decentralized content networks, blockchain technologies, crypto exchanges, crypto exchangers, and specialized services with randomization functions as sources of forensically relevant information. The author offers organizational-tactical and investigative recommendations for the investigation of terrorism financing carried out through cryptocurrency transactions.

Keywords: terrorism financing, cryptocurrency, blockchain, crypto exchange, crypto wallet, blockchain audit, "mixers".

В условиях стремительного развития информационных и коммуникационных технологий террористические организации активно адаптируются, используя новые цифровые инструменты для финансирования своей деятельности. Криптовалюта, благодаря своим уникальным техническим свойствам, становится важным средством

для обеспечения финансирования террористических актов, что представляет серьёзную угрозу для глобальной безопасности.

Исторически террористические акты представляли собой «досадную неприятность», контролируруемую международным сообществом. Однако современные угрозы с применением цифровых технологий требуют новых методов противодействия.

Финансовая поддержка необходима террористам для вербовки, обучения, закупки оружия, подкупа и пропаганды. Помимо государств, сегодня ключевую роль играют негосударственные факторы и сбор пожертвований через скрытые каналы. Криптовалюта облегчает сбор и перемещение средств без контроля.

Впервые идея цифровой валюты появилась в 1980-х годах с разработками Дэвида Чаума и его DigiCash. Несмотря на провал централизованной системы, последующие инновации — b-money, Bit Gold, Hashcash — заложили фундамент для появления биткойна, запущенного в 2009 году Сатоши Накамото.

После запуска биткойна в 2009 году технология быстро набирала популярность. Одним из первых пользователей стал Хэл Финни, получивший от Сатоши Накамото первые 50 BTC — первая транзакция в сети. С ростом популярности биткойна и появлением других криптовалют (Ethereum, Litecoin, Dogecoin и др.) компании, такие как WordPress, Microsoft и PayPal, начали принимать криптовалютные платежи [1]. Это свидетельствует о признании криптовалют в легальной экономике.

Финансирование терроризма — это процесс получения, передачи и использования денежных средств и материальных ресурсов, необходимых для планирования и реализации террористических действий. Для успешной деятельности террористам требуются как наличные деньги, так и безналичные средства, особенно те, которые функционируют вне традиционных финансовых систем и контролирующих органов.

Объём и устойчивость финансирования напрямую влияют на масштабы и частоту террористических актов. Источники финансирования могут быть как легитимными (доноры, членские взносы), так и нелегальными, такие как торговля наркотиками, мошенничество, торговля людьми, киберпреступность [2].

Криптовалюта — это цифровая форма денег, существующая в децентрализованной сети, не контролируемая государственными институтами. Примером является биткойн — первая и наиболее известная криптовалюта. FATF (Financial Action Task Force on Money Laundering) определяет криптовалюту как средство обмена, не признанное законной валютой какой-либо страны [3].

При этом обратим внимание, что криптовалюта не тождественна электронным деньгам, например Яндекс-деньги или Киви-кошелек. Последние продолжают использовать для транзакций механизмы реально существующей банковской системы. Биткойны передаются напрямую между сторонами экономических отношений, минуя любые сторонние финансовые институты, а всеохватывающий

масштаб электронной сети делает возможным их мгновенную передачу из одного уголка земного шара в другой.

Необходимо отметить, что Узбекистан является участником FATF. Настоящая организация рекомендует странам устанавливать уголовную ответственность в случае выявления фактов финансирования террористических групп, немедленно замораживать счета и активы, производить арест имущества организаций и частных лиц, причастных к данной противоправной деятельности. В случае возникновения подозрений финансовые организации обязаны предоставлять соответствующую информацию компетентным органам. Все существующие инструменты государственного контроля помогают в борьбе со многими преступлениями, в частности с финансированием терроризма (ст. 155³ УК РУз).

Необходимость развития международной системы противодействия как терроризму, так и финансированию террористической деятельности, в том числе совершаемому посредством криптовалютных транзакций, подтверждается фактическими данными. Так, 22 марта 2024 г. террористы совершили вооруженное нападение в подмосковном «Крокус Сити Холле», в результате которого погибли 145 человек и пострадали более 550. При расследовании теракта были установлены данные, свидетельствующие о его финансировании через многочисленные финансовые организации с использованием различных инструментов, в том числе криптовалюты [4].

Кроме того, ИГИЛ использует даркнет-сайт Isdarat для пропаганды и сбора пожертвований в криптовалюте, а также выпускает блоги с рекомендациями по анонимному использованию биткойна и специальных кошельков, таких как DarkWallet. В 2015 году ФБР заблокировало счет, через который ИГИЛ собирал около 5 BTC [5].

Террористов привлекают особенности криптовалют такие как:

- Трансграничность (мгновенные международные переводы без необходимости посредников);
- Минимальные транзакционные издержки (значительно дешевле традиционных банковских переводов);
- Отсутствие централизованного контроля (нет посредников, которые могли бы блокировать операции);
- Псевдоанонимность (адреса и транзакции сложно связать с реальными лицами, что затрудняет отслеживание денежных потоков).

Из-за этих особенностей криптовалюты активно используются для сокрытия и перевода средств, связанных с террористической деятельностью. Это вызвало ответные меры ряда государств, которые ограничивают или запрещают их использование.

Однако, мы считаем, что при наличии контроля за интернет-пространством трафик денег с использованием криптовалют все равно в какой-то возможно

отслеживать. К примеру, можно видеть, конечно, не конкретные суммы и не конкретного отправителя или получателя, но аргументированно и точно можно назвать так называемые директории – то есть регион отправки и регион получения перевода по использованным IP-адресам.

К сожалению, до настоящего времени существуют и продолжают появляться как криптобиржи, криптобменники и специальные сервисы, находящиеся вне правового поля, позволяющие скрыть происхождение полученного дохода в криптовалюте, так и децентрализованные контент-сети (например, Tron, Steem (Steemit), LBRY). Такие сети работают на основе блокчейн-технологии, позволяя осуществлять обмен и хранение данных без централизованного управления.

В расследовании преступлений, которые совершаются с использованием криптовалют и децентрализованных контент-сетей, участникам доказывания необходимы знания об основах функционирования таких сетей, об обнаружении следов криптовалютных транзакций (цифровых). В этом контексте мы полностью согласны с мнением ученых процессуалистов Ю.В.Гаврилина и И.С.Бедерова о том, что использование для анонимности специальных программ, браузеров «существенно ограничивает возможности правоохранителей по использованию "финансового следа" для установления лиц, причастных к расследуемому преступлению, включая личности получателей подобных активов» [6].

Для подготовки криптовалютной транзакции, в том числе с целью финансирования терроризма, лицо должен обладать крипто-кошельком, который содержит информацию о публичных и приватных ключах. При производстве таких следственных действий, как обыск и осмотр жилища или помещений, следователю необходимо обращать внимание не только на электронные носители, но и знать, как может выглядеть криптокошелек (может быть в виде флешнакопителя, пластиковой карты, может содержаться в ноутбуке и сотовом телефоне, даже обычный распечатанный лист бумаги с набором слов, знаков, цифр может означать приватный ключ к криптокошельку).

Выделяют следующие виды кошельков для криптовалют:

- настольный (десктопный) – программа устанавливается непосредственно на ПК, при этом в компьютере автоматически будет размещен документ, содержащий данные закрытого ключа и адрес, на который можно отправлять или получать средства (wallet.dat);

- онлайн-кошелек – находится на сервисе сети, доступен с любого устройства, способного выйти в сеть (считается самым небезопасным для хранения крупных сумм), чаще всего содержится в телефонах в виде скачанных приложений;

- аппаратный («холодное» хранение) – ключ хранится автономно на устройстве без подключения к сети Интернета (схожи с флешнакопителями, так как подключаются к компьютеру, ноутбуку для транзакции), но также требует введения

пароля; даже если владелец потерял такой кошелек, он может купить новый, ввести свой пароль и снова использовать.

Во всех представленных вариантах при поисковых мероприятиях необходимо обращать внимание на записи владельца (на бумаге, в записной книжке и пр.) в виде номера счета и пароля или qr-кода (символы, цифры, слова, не всегда имеющие смысл). Такие записи могут быть надежно спрятаны владельцем, поскольку являются ключами (паролями) к криптокошелькам.

При регистрации криптокошелька на криптоплатформе необходима подготовка учетных записей отправителей и получателей криптовалюты в обход процедур KYC («Know Your Customer» – знай своего клиента), т.е. верификации. Для верификации по указанной процедуре требуется указать e-mail и номер телефона, паспортные данные, иногда даже осуществляется проверка лица по фотографии-селфи. После этого криптобиржа выдает адрес криптовалютного кошелька, и при необходимости возможно отследить все транзакции через блокчейн-навигатор в рамках процедуры AML («Anti-Money Laundering» – борьба с отмыванием денег). С ее помощью проверяют, не связана ли криптовалюта с преступной деятельностью. Однако, несмотря на ужесточение законодательства о регулировании финансовых организаций, все еще возможно совершить транзакцию без верификации на определенных криптобиржах (например, BingX, LCS, Phemex, Probit, Kuna, SkyCrypto и др.). Децентрализованные биржи (DEX) являются платформами для торговли, обмена и использования финансовых инструментов. Они построены на основе технологии блокчейн, и в отличие от централизованных бирж у них нет администрации, которая управляет платформой и может принять решение о блокировке пользователей. Децентрализованные биржи не требуют прохождения KYC и создания кошелька, который находился бы под контролем биржи. Для подключения требуется только некастодиальный кошелек. Платформа не получает доступа к средствам, поэтому не может забрать их или ограничить их использование.

Чаще всего при выводе средств необходимо подтверждение электронного адреса и номера телефона, иногда – наличие банковской карты.

Если лицо использует номер телефона и банковскую карту, оформленную на подставное лицо, изменяет передаваемые HTTP-заголовки, применяет средства VPN (Virtual Private Network, виртуальная частная сеть), Tor (The Onion Router)¹, P2P анонимайзеры и др., то обнаружить его практически не представляется возможным.

Анализ процесса подготовки к совершению финансирования терроризма с использованием криптотранзакций позволил выделить следующие действия: поиск криптобиржи без процедур KYC; приобретение криптокошелька; поиск абонентского

¹ Свободная (BSD) реализация второго поколения onion router (так называемая «луковая (многослойная) маршрутизация»). Данная система, позволяет пользователям соединяться анонимно, обеспечивая передачу пользовательских данных в зашифрованном виде).

номера (сим-карты), который регистрируется на подставное лицо; подбор и использование программного обеспечения с целью сокрытия IP-адреса.

Непосредственно факт финансирования терроризма с использованием криптовалют связан с обращением к специальным сервисам для транзакций (криптовбиржи, обменники, электронные платежные системы, р2р-биржи, телеграм-боты, криптоматы). Отследить «финансовые» следы переводов между криптовалютными биржами достаточно сложно по следующим причинам:

- регистрация криптовалютных бирж за рубежом, зачастую в странах, не оказывающих правовую помощь в расследовании уголовных дел, или офшорных зонах;
- использование сервисов анонимности, так называемых «миксеров»², затрудняющих (иногда делающих невозможным) отслеживание транзакций криптовалют посредством функции рандомизации, усложнения анализа цепочки блоков.

«Миксеры» работают на браузере Tor, многие из них не ведут логи, удаляя информацию об операциях за сутки. Суть работы «миксера» как раз и заключается в оказании услуги за определенную комиссию (от 0,01 до 10% от суммы транзакции), позволяющей максимально завуалировать (если не удалить) связи между адресом кошелька и местом, куда преступник доставляет криптовалюту. А поскольку такие веб-сайты не хранят историю транзакций и посещений, не требуют регистрации, это позволяет осуществлять мгновенные переводы на различные дополнительные адреса.

Для сокрытия фактов финансирования терроризма с использованием криптовалют лицами, как правило, совершаются следующие действия:

- дробление целевой транзакции на минимальные части для конвертации полученных целевых средств;
- использование «дропов» (неосведомленных о транзакциях и переводах лиц, на которых легально оформлены счета, банковские карты, сим-карты);
- дополнительные транзакции по переводу конвертированных денежных средств на электронные кошельки;
- перевод конвертируемых денег на счета третьих лиц и др.

Каждое из представленных действий само по себе не образует состав преступления или какого-либо нарушения, и, на первый взгляд, может не вызывать подозрений у контролирующего государственного органа. Однако именно на такие действия следователю необходимо обращать внимание, так как, например, с помощью дробления при перечислении денег маскируется сложная цепочка транзакций несколькими трансфертами, в том числе находящимися за пределами государства; банковские карты «дропов», по которым совершают некоторые покупки,

² Биткойн-тумблер, сервис микширования биткойнов; наиболее популярные из них Mixtum, Cryptomixer, ChipMixer, Blender, BitcoinMix, Bitmixer, BitCloak и др.

создают вид использования карты живым человеком в повседневных нуждах и др., чтобы обеспечить функционирование счетов (в противном случае банки блокируют транзакцию из-за подозрительности сделок) [7].

В расследовании финансирования терроризма рассмотренные нами сервисы, а также криптовалютные биржи, обменники и др. являются источником получения криминалистически значимой информации. В ситуации регистрации таковых за пределами государства необходимо использовать возможности международного взаимодействия уполномоченного ведомства с подразделениями финансовой разведки других государств, так как информационный обмен между правоохранительными органами включает в себя взаимодействие при производстве предварительного расследования уголовных дел.

По запросу можно получить следующую информацию: о лицах, которые использовали соответствующие транзакции при совершении торговых операций на валютном рынке, включая статистические данные для IP-адресов, с которых была произведена регистрация, а также последующее администрирование счетов; реквизиты адресов криптовалюты в соответствующей сети, связанных с этими лицами; сведения о совершаемых ими транзакциях; копии документов, предоставленных для идентификации, а также информацию о платежных средствах, используемых для пополнения фиатных счетов. Такая информация может быть приобщена к материалам уголовного дела. Также, полученные электронные данные после соответствующей проверки и согласно постановлению следователя, могут быть признаны цифровыми доказательствами по уголовному делу [8].

Необходимо отметить, что одним из основных инструментов, используемых в сфере противодействия финансированию терроризма с использованием криптовалют, является аудит блокчейна.

Аудит блокчейна – это процесс анализа данных в блокчейне для выявления закономерностей, отслеживания транзакций и определения потенциальной преступной деятельности.

Поскольку блокчейн представляет собой публичную децентрализованную бухгалтерскую книгу аналитического учета, в которую записываются все транзакции в сети и эта книга прозрачна, что означает, что любой может просмотреть данные, но личности участвующих сторон остаются анонимными. Правоохранительные органы ряда стран часто используют специализированное программное обеспечение для анализа блокчейна и выявления подозрительных транзакций. Этот процесс включает в себя сбор и анализ данных о транзакциях, идентификацию адресов кошельков и отслеживание движения средств. После анализа данных блокчейна правоохранительные органы могут определить вовлеченные стороны и отследить движение средств. Программное обеспечение предназначено для выявления закономерностей и тенденций в данных, например, крупных транзакций или нескольких транзакций между одними и теми же сторонами. Программное обеспечение также может быть

использовано для отслеживания движения средств через блокчейн, идентификации адресов кошельков и отслеживания движения средств.

К таким инструментам относятся следующие: **Walletexplorer.com**, **Graphsense.info** (поддерживает BTC, BCH, LTC, ZEC), **Blockchain.com** (BTC, BCH) **Blockchair.com** (BTC, BCH, BSV, ETH, XRP, LTC, DASH, DOGE, GRS) **Etherscan.io** (только ETH), а также, программные продукты «Прозрачный блокчейн 2.0» и АО «Шард» Российского производства [9].

В качестве рекомендаций при производстве следственных действий в расследовании финансирования терроризма, совершенного с помощью криптовалют, считаем целесообразным провести следующее:

- для осмотра, изъятия электронных носителей (телефон, компьютер и др.) необходимо пригласить специалиста, обладающего специальными знаниями не только в области компьютерных технологий, но и в области программного обеспечения для криптовалютных транзакций;

- в ходе осмотра электронного носителя произвести необходимые скриншоты, отражающие криптовалютные транзакции. Также требуется уделять особое внимание: данным о криптокошельках (адреса, ключи, SEED-фразы, логины, пароли); истории посещений сайтов, связанных с криптоактивами; IP-адресам; информации об использовании облачных сервисов; программному обеспечению для работы с криптокошельками; файлам, фото, аудио- и видеозаписям с информацией о криптоактивах;

- в случае извлечения специалистом из электронного носителя и расшифровки сведений об открытых и закрытых ключах криптокошелька принять меры к переводу активов на новый аппаратный кошелек, принадлежащий органам расследования, при этом указав в протоколе следственного действия только открытый ключ нового кошелька (не прописывая пароль для исключения доступа третьих лиц, в том числе обвиняемых и защитников), далее принять меры к хранению криптокошелька как вещественного доказательства и обратиться в суд с ходатайством о наложении ареста на изъятые криптовалютные активы [10].

Криптовалюты представляют собой двойственный феномен: с одной стороны — инновационный финансовый инструмент, способствующий развитию экономики и технологий, с другой — средство обхода контроля и финансирования преступной деятельности, в том числе международного терроризма. Борьба с этим вызовом требует скоординированных международных усилий, развития новых технологий мониторинга и усовершенствования законодательства.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. https://en.wikipedia.org/wiki/History_of_bitcoin
2. Sountra M.A. (2019). Cryptocurrency as a Modern Technique of money Laundering and Terrorism Financing. LGU International Journal for Electronic Crime Investigation, 3(4), 1-16.
3. Irwin A.S., & Milad G. (2016). The use of crypto-currencies in funding violent jihad. Journal of Money Laundering Control, 407-425 pp.
4. Росфинмониторинг раскрыл детали финансирования теракта в «Крокусе» [Электронный ресурс]. URL: <https://www.rbc.ru/rbcfrreenews/662a0b689a794764461ecf79> (дата обращения: 27.04.2024).
5. <https://www.memri.org/cjlab/following-repeated-shutdowns-prominent-website>.
6. Гаврилин Ю.В., Бедеров И.С. Установление личности владельцев цифровой валюты: методологические основы // Труды Академии управления МВД России. 2021. № 4.
7. Нуменко О.А. Некоторые организационно-тактические особенности расследования финансирования терроризма, совершенного с использованием криптовалют // Вестник Краснодарского университета МВД России. 2024. №3(65). С. 58-61.
8. Настольная книга следователя при ведении уголовных дел в области информационных технологий. Методическое пособие. Академия правоохранительных органов. Ташкент. 2025. С. 28-35.
9. Пушкарев В.В., Токолов А.В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют// Вестник экономической безопасности. 2023. №4. С. 88–92.
10. Балашова А. А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: автореф. дис. ... канд. юрид. наук : 12.00.09. М., 2020. С. 14.

REFERENCES:

1. https://en.wikipedia.org/wiki/History_of_bitcoin
2. Sountra M.A. (2019). Cryptocurrency as a Modern Technique of money Laundering and Terrorism Financing. LGU International Journal for Electronic Crime Investigation, 3(4), 1-16.
3. Irwin A.S., & Milad G. (2016). The use of crypto-currencies in funding violent jihad. Journal of Money Laundering Control, 407-425 pp.
4. Rosfinmonitoring revealed the details of the financing of the terrorist attack in Crocus [Electronic resource]. URL: <https://www.rbc.ru/rbcfrreenews/662a0b689a794764461ecf79> (accessed: 04/27/2024).

5. <https://www.memri.org/cjlab/following-repeated-shutdowns-prominent-website>.

6. Gavrilin Yu.V., Bederov I.S. Identification of the owners of digital currency: methodological foundations // Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2021. № 4.

7. Numenko O.A. Some organizational and tactical features of the investigation of terrorist financing committed using cryptocurrencies // Bulletin of the Krasnodar University of the Ministry of Internal Affairs of Russia. 2024. No. 3(65). pp. 58-61.

8. The investigator's desk book for conducting criminal cases in the field of information technology. Methodical manual. Academy of Law Enforcement Agencies. Tashkent. 2025. pp. 28-35.

9. Pushkarev V.V., Tokolov A.V. Fundamentals of the organization of countering crimes committed using cryptocurrencies// Bulletin of Economic Security. 2023. No. 4. pp. 88-92.

10. Balashova A. A. Electronic information carriers and their use in criminal procedural evidence: abstract of the dissertation of the cand. jurid. Sciences : 12.00.09. Moscow, 2020. p. 14.