Красинский Владислав Вячеславович,

Аппарат Правительства Московской области,

доктор юридических наук, доцент,

Krasinsky Vladislav V.,

Moscow region government apparatus,

Doctor of Law, associate Professor

ПРОТИВОДЕЙСТВИЕ ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

*Красинский В.В.* Противодействие финансированию терроризма с использованием криптовалют // Современное право. 2022. № 9. С. 108-116. **DOI 10.25799/NI.2022.58.84.018**

Финансирование террористической деятельности является важной основой функционирования любой террористической организации, ячейки или террориста-одиночки. Денежные средства помогают международным террористическим организациям (далее-МТО) вербовать и рекрутировать новых сторонников, готовить и проводить теракты, обеспечивают ресурсную поддержку и информационно-пропагандистское сопровождение террористической деятельности. В то же время пресечение правоохранительными органами финансовой подпитки позволяет уменьшить масштабы и интенсивность террористических акций, снизить активность организационного ядра, функционеров и пособнических сетей террористического бандподполья.

В течение 5 последних лет в арсенале террористических организаций появились качественно иные финансовые инструменты, основанные на новых информационных технологиях, - криптовалюты[[1]](#footnote-1).

Использование виртуальных валют (криптовалют) существенно повлияло на систему финансирования и ресурсного обеспечения терроризма, открыло новые возможности для отмывания преступных доходов и финансирования терроризма[[2]](#footnote-2).

Можно выделить две группы факторов, связанных с использованием террористами виртуальных валют и активов: препятствующие использованию криптовалют и цифровых активов и способствующие этой деятельности.

Среди основных факторов, препятствующих использованию криптовалют в террористических целях, следует назвать недостаточное количество подготовленных технических специалистов МТО в данной сфере и необходимость устойчивого интернет-доступа. Таким образом для террористических группировок и их сторонников, находящихся в отдаленных регионах с неустойчивым покрытием или отсутствием Интернета данный инструмент финансирования мало пригоден. Кроме того, в государствах, где криптовалюты запрещены в качестве платежных или расчетных средств, виртуальные активы приходится конвертировать в фиатные деньги, что создает для преступников дополнительные риски идентификации участников операций.

В числе способствующих использованию криптовалют факторов:

относительная анонимность операций при отсутствии централизованной системы перевода криптовалют и должной идентификации владельца виртуальных активов[[3]](#footnote-3);

возможности быстрого первичного выпуска криптовалют, а также проведения операций по обмену криптовалют на территории государств, в которых ни плательщик, ни получатель не находятся[[4]](#footnote-4);

беспрепятственный и оперативный трансграничный перевод криптовалют;

возможности обналичивания криптовалют в системе неформальной («теневой») экономики;

размывание ответственности лиц, осуществляющих переводы и совершение платежей[[5]](#footnote-5);

относительно слабый общий потенциал подразделений финансовой разведки и правоохранительных органов по контролю операций в криптокошельках, своевременному пресечению подозрительных операций и сделок с виртуальными активами.

Не случайно, по данным опроса 550 респондентов из финансовых учреждений, правоохранительных и надзорных органов, страховых и юридических компаний, проведенного в сентябре 2020 г. аналитическим центром Royal United Services Institute и Ассоциацией специалистов по борьбе с отмыванием денег (Association of Anti-Money Laundering Specialists), представители финансового сектора в подавляющем большинстве считают криптовалюты рискованными активами[[6]](#footnote-6).

Все респонденты признали, что криптовалюты уязвимы для преступников. Почти 90% опрошенных заявили, что их тревожит использование криптовалют для отмывания денег. Более 80% выразили обеспокоенность тем, что находящиеся под санкциями субъекты используют цифровые валюты для обхода формальной финансовой системы. Лишь 20% респондентов считают виртуальные активы перспективным финансовым средством[[7]](#footnote-7).

В проекте Азиатско-Тихоокеанской группы противодействия отмыванию денег и Ближневосточной и Североафриканской ФАТФ (MENAFATF) «Социальные медиа и финансирование терроризма» использование иностранными боевиками-террористами новых платежных продуктов и сервисов, включая криптовалюты, указывается в числе рисков финансирования терроризма[[8]](#footnote-8).

В отчете Группы финансовых мер борьбы с отмыванием денег (ФАТФ) «Виртуальные активы. Признаки отмывания денег и финансирования террористов (2020)» отмечается: «Возможность совершать быстрые трансграничные операции позволяет преступникам не только приобретать, перемещать и хранить активы в цифровом виде, часто за пределами регулируемой финансовой системы, но и скрывать отправителя и получателя средств, и затруднять своевременное выявление подозрительной деятельности»[[9]](#footnote-9).

Данные факторы обусловили широкое распространение виртуальных активов в преступной и террористической деятельности.

Одним из первых джихадистских сторонников использования криптовалюты для финансирования терроризма был Бахрун Наим (Bahrun Naim), индонезийский боевик ИГИЛ[[10]](#footnote-10), воевавший в Сирии. В 2016 г. Наим назвал биткоин одним из инструментов перемещения средств для отмывания доходов от кардинга и посоветовал своим последователям отмывать деньги через цепочку криптовалютных счетов[[11]](#footnote-11). Впоследствии, по данным финансовой разведки Индонезии (Indonesian Financial Transaction Reports and Analysis Centre), Наим использовал биткоины для финансирования теракта в полицейском управлении Соло (Ява, июль 2016 г.)[[12]](#footnote-12).

Наиболее распространенной схемой финансирования терроризма с помощью виртуальных валют является использование аккаунтов подставных благотворительных организаций для размещения реквизитов криптокошельков и сбора средств.

Так, анализ финансовых кампаний центральноазиатских группировок боевиков, связанных с Аль-Каидой[[13]](#footnote-13), показывает, что они регулярно собирали пожертвования в криптовалюте через благотворительные организации «Аль-Садака» и «Закят»[[14]](#footnote-14). Первые рекламные объявления о краудфандинговых кампаниях центральноазиатских террористических группировок, принимавших биткоин для джихадистских целей в Сирии, появились в Telegram-канале «Аль-Садака» в 2017 году. Лидеры МТО тогда призвали своих сторонников анонимно и безопасно делать пожертвования братьям-моджахедам через «кошелек биткоина», пользуясь «способностью криптовалюты запутать след».

В связи с потребностью в дополнительных источниках финансирования группировки «Катиба-ат-Таухид валь-Джихад», «Катиба Имама аль-Бухари» и «Исламская партия Туркестана»[[15]](#footnote-15) в 2018 г. также включились в кампанию по сбору средств в биткоинах.

В октябре 2018 г. индонезийская благотворительная организация Фонд Абу Ахмада (Abu Ahmed Foundation) задействовала краудфайндинговые инструменты (GoFundme.com, Youcaring.com, Kickstarter.com) для сбора криптовалюты в поддержку МТО «Хайат Тахрир аш-Шам»[[16]](#footnote-16). Фонд призывал «благотворителей» делать пожертвования с помощью криптовалют Bitcoin, Monero, Dash и Verge[[17]](#footnote-17).

18 июня 2020 года боевики группы «Катиба-ат-Таухид валь-Джихад» опубликовали в Telegram мнение известного салафитского идеолога современного джихадизма Абу Катады Аль-Фаластини (Abu Qatada al-Falastini), у которого спросили, противоречит ли краудфандинговая кампания сбора биткоинов в целях джихада Исламу[[18]](#footnote-18). Абу Катада обосновал приемлемость использования биткоина для защиты исламской уммы и ведения джихада, но вместе с тем предостерег от полного доверия к биткоину. По его мнению, «враги ислама» могут уничтожить эту криптовалюту; если она потеряет свою стоимость в связи с волатильностью, то правоверные мусульмане, вложившие свои сбережения в биткоин, могут обанкротиться[[19]](#footnote-19).

В рамках расследования в августе 2020 г. схемы финансирования терроризма с использованием криптовалют Министерство юстиции США установило, что аффилированные с МТО «Аль-Каида»[[20]](#footnote-20) структуры, действовавшие в Сирии, содержали профессиональную сеть отмывания биткоинов, которая с помощью платформы Telegram получала пожертвования в виртуальной валюте. Сбор средств на нужды Аль-Каиды проводила Telegram-группа «Tawheed Jihad Media», начиная с апреля 2019 г. Использовались 155 криптокошельков, средства с которых направлялись на биржи подарочных карт и др. платформы[[21]](#footnote-21).

В сентябре 2020 г. аналогичная группа отмывателей была арестована во Франции. По данным Национального центра по борьбе с терроризмом Франции (PHAT), задержанные входили в отмывочную сеть, которая с использованием криптовалют перевела деньги террористическим группам, связанным с МТО «Аль-Каида» и «ИГИЛ»[[22]](#footnote-22).

В июле 2021 г. в Израиле было конфисковано 84 криптокошелька, связанных с ХАМАС. По данным аналитической компании Elliptic, в них находилось 7,7 млн долларов[[23]](#footnote-23).

Следует выделить несколько особенностей финансирования терроризма с использованием криптовалют:

массовое использование платформы Telegram (социальных сетей) для размещения реквизитов криптокошельков на аккаунтах подставных благотворительных организаций[[24]](#footnote-24);

открытая целевая или псевдоблаготворительная ориентация краудфайндинговых кампаний (указание целевого назначения пожертвований: закупка полевой формы одежды, тактического снаряжения, средств связи, вооружения, боеприпасов, токсичных реактивов и др.);

использование бирж виртуальных активов или сервисов перевода денег в высокорисковой стране или территории с минимальными требованиями ПОД/ФТ, а также отсутствием регулирования виртуальных активов[[25]](#footnote-25);

использование услуг незарегистрированных провайдеров / обменников виртуальных активов («внебиржевых брокеров»);

использование «втемную» третьих лиц (присвоение средств от пожертвований, первичного размещения коинов и инвестиций в криптовалюты);

периодичность массового сбора пожертвований, замаскированных под благотворительные сборы (наиболее активное поступление средств отмечается в священный месяц Рамадан, в честь окончания Рамадана (праздник Ид-аль-Фитр (Ураза-байрам)) и в преддверии праздника Курбан-байрам) [[26]](#footnote-26).

В целях конспирации и противодействия правоохранительным органам техническими специалистами МТО создаются запасные/резервные группы в социальных сетях и мессенджерах (Telegram, Whatsapp, Wickr, WeChat, Snapchat, Surespot, Chat Secure и др.) для предотвращения блокировки аккаунтов сбора средств[[27]](#footnote-27), осуществляется дробление финансовых операций и переводов криптовалюты, используются одноразовые кошельки Electrum и динамические схемы генерации неповторяющихся биткоин-адресов для каждого пожертвования на нужды террористической организации[[28]](#footnote-28).

В условиях активизации блокировки аккаунтов, связанных с терроризмом и отмыванием доходов, сокращения масштабов финансовой поддержки терроризма с использованием условно «легальных» источников доходов (пожертвования частных лиц и различных неправительственных фондов под видом благотворительности) ключевым инструментом финансирования и ресурсного обеспечения МТО становится добывание денежных средств незаконными способами.

Так, на фоне пандемии коронавируса финансовыми институтами фиксируется резкое увеличение числа случаев кибермошенничества с использованием методов социальной инженерии и фишинговых атак. Эксперты указывают на риски получения криптовалют в результате хакерских атак и мошеннических схем[[29]](#footnote-29). Известны факты имитации мошенниками рассылки от Всемирной организации здравоохранения, а также благотворительных кампаний Всемирного банка и МВФ[[30]](#footnote-30).

13 августа 2020 г. в США были арестованы около 300 криптовалютных счетов, предназначенных для сбора средств на нужды МТО ИГИЛ, Аль-Каиды и ХАМАС[[31]](#footnote-31). Часть средств была получена преступниками мошенническим способом, в том числе путем продажи медицинских препаратов для лечения коронавирусной инфекции[[32]](#footnote-32).

Активизировались и незаконные схемы, связанные с оптимизацией налогообложения (tax fraud) и инвестированием в криптовалюты (fraud involving cryptocurrency investments).

Связанные с МТО группы программистов прибегают к вредоносным программным продуктам для хищения средств у граждан и организаций.

К числу регионов повышенной активности программ-вымогателей относится Восточная Европа, где аккумулируется и обращается около ¼ объема незаконных средств, полученных с адресов программ-вымогателей[[33]](#footnote-33).

В целях продажи оружия, взрывчатых веществ и отмывания доходов от продажи наркотиков преступными сообществами и террористическими организациями используются возможности рынков даркнета. Крупнейшим теневым рынком в Восточной Европе является рынок Hydra Marketplace, который является шестым по объему транзакций сервисом в регионе. Доход Hydra в период с июня 2019 г. по июль 2020 г. составил более 1,2 млрд долларов в криптовалюте[[34]](#footnote-34). Ни в одном другом регионе мира среди популярных площадок обслуживания криптовалютных транзакций нет ни рынков даркнета, ни других незаконных финансовых сервисов.

После появления виртуальных активов и криптовалют компетентные правоохранительные и надзорные органы предприняли ряд мер по минимизации рисков отмывания доходов и финансирования терроризма. С одной стороны, данный сегмент финансовой деятельности во многих странах был введен в правовой оборот, разработаны требования к использованию виртуальных валют, контролю деятельности провайдеров; с другой стороны, - для расшифровки и отслеживания транзакций с криптовалютами стали применяться методики анализа блокчейна[[35]](#footnote-35).

Первые рекомендации по управлению рисками ОД/ФТ, связанными с виртуальной валютой, были разработаны ФАТФ и опубликованы в июне 2015 г. (Руководство 2015 г.)[[36]](#footnote-36). Сфера применения Руководства 2015 г. ограничивалась конвертируемой виртуальной валютой и провайдерами услуг по обмену конвертируемой виртуальной валюты.

30 мая 2018 г. Европарламентом и Советом ЕС была утверждена Директива 2018/843 по противодействию отмыванию денег и финансированию терроризма (the fifth anti-money laundering directive – 5 AMLD, т.н. Пятая директива ЕС по ПОД/ФТ). Положения Пятой директивы были в том числе направлены на ограничение анонимности при использовании виртуальных валют, а также усиление контроля деятельности провайдеров услуг в сфере виртуальных активов. На основании требований Пятой директивы в список субъектов первичного финансового мониторинга внесены лица, предоставляющие услуги по конвертации виртуальных валют, а также администрированию кошельков[[37]](#footnote-37).

В октябре 2018 г. ФАТФ актуализировала свои стандарты применительно к деятельности в сфере виртуальных активов. В частности, Рекомендация 15 «Новые технологии» дополнена положением о том, что страны в целях управления рисками ОД/ФТ и их снижения должны обеспечить регулирование деятельности провайдеров услуг в сфере виртуальных активов, их лицензирование или регистрацию, а также контроль.

В отличие от Руководства 2015 г. ФАТФ распространила зоны риска не только на операции обмена виртуальных валют на фиатные, но и на сделки по обмену виртуальных активов между собой.

Глоссарий к Рекомендациям ФАТФ дополнен определениями «провайдеров услуг в сфере виртуальных активов» и «виртуальных активов».

В июне 2019 г. ФАТФ утвердила обновленное Руководство по риск-ориентированному подходу в отношении виртуальных активов и провайдеров услуг в сфере виртуальных активов[[38]](#footnote-38). В соответствии с Руководством 2019 г. государства-члены ФАТФ должны проводить проверку клиентов в отношении операций с криптовалютой на сумму свыше 1 тыс. долларов или евро, хранение записей (в течение 5 лет) и сообщение о подозрительных операциях отправителей и получателей виртуальных активов.

В декабре 2020 г. вступила в силу Шестая директива о борьбе с отмыванием денег (the sixth anti-money laundering directive – 6 AMLD). Новая директива унифицирует конструкцию составов легализации преступных доходов во всех государствах-членах ЕС, распространяет уголовную ответственность на юридических лиц, расширяет сотрудничество между государствами в расследовании финансовых преступлений. Предусмотрен единый перечень предикатных правонарушений, введены новые составы преступлений в сфере ПОД/ФТ: содействие и пособничество, подстрекательство и покушение.

В России сегмент виртуальных активов и криптовалют длительное время оставался неурегулированным. В целях совершенствования правовой регламентации механизмов цифровой экономики, противодействия легализации преступных доходов и финансированию терроризма 31.07.2020 г. принят Федеральный закон от № 259-ФЗ, в соответствии с которым в правовой оборот и легальную экономику введены цифровая валюта и виртуальные финансовые активы. Под цифровыми финансовыми активами законодатель понимает цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, право участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг. Цифровой валютой признается совокупность электронных данных, содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной или расчетной единицей, или в качестве инвестиции[[39]](#footnote-39).

В соответствии с Указанием Банка России от 20.10.2020 г. № 5599-У внесены изменения в правила внутреннего контроля кредитных организаций. При этом перечень признаков подозрительных операций в целях противодействия отмыванию преступных доходов и финансированию терроризма был дополнен кодами признаков: «операции, связанные с обращением цифровых прав, которые характеризуются однонаправленностью, регулярностью, на крупные суммы» (код 1137) и «операции, связанные с оборотом цифровой валюты» (код 1190)[[40]](#footnote-40).

Совершенствование в соответствии со стандартами ФАТФ правил внутреннего контроля кредитных организаций направлено на усиление мониторинга операций с виртуальными активами и криптовалютами на этапе использования банковских счетов и обмена криптовалют на фиатные валюты.

В целях противодействия финансированию терроризма осуществляется выявление и мониторинг финансовых операций, совершенных в зоны повышенной террористической активности и приграничные к регионам вооруженных конфликтов территории. В качестве сомнительных рассматриваются операции клиентов, их контрагентов, представителей, выгодоприобретателей, бенефициаров или участников организаций, зарегистрированных в государствах (на территории) с высокой террористической или экстремистской активностью. Особый интерес представляют операции организаций и граждан иностранных государств, поддерживающих экстремистские движения антироссийской направленности[[41]](#footnote-41).

Традиционное внимание уделяется контролю за операциями по переводу средств, поступающих от зарубежных этнических диаспор и аффилированных с ними финансово-экономических и криминальных структур.

На системной основе организованы выявление и мониторинг операций с участием лиц, находящихся в розыске, осужденных за терроризм, отбывших наказание за совершение преступлений террористической направленности, и их близких связей.

В н.в. для мониторинга криптовалютных транзакций используются цифровые платформы Chainanalysis (создана в 2014 в США, охват – 59 стран, 89 криптовалют), Elliptic (создана в 2013 в Великобритании, охват – 29 стран, 97% криптоактивов)[[42]](#footnote-42), Cipher (создана в США, 29 стран, более 700 криптоактивов)[[43]](#footnote-43), Crystal (создана в 2018 в Нидерландах, 8 криптовалют, более 60 DeFi-протоколов), TRM (основана в США в 2017, анализ 20 блокчейнов) Scorechain (основана в Люксембурге в 2015, мониторинг транзакций биткоина) и Coinfirm (создана в 2016 в Великобритании).

В целях повышения эффективности взаимодействия в сфере противодействия легализации преступных доходов и финансирования терроризма Росфинмониторингом разработан цифровой сервис «Прозрачный блокчейн». Данный ресурс позволяет правоохранительным и контрольно-надзорным органам осуществлять проверку подозрительных аккаунтов участников криптовалютной среды, цепочек криптовалютных транзакций и цифровых финансовых активов. В отличие от бесплатных ресурсов (blockchain.com, blockchair.com, walletexplorer.com и др.), «Прозрачный блокчейн» позволяет проводить кластеризацию адресов, детализацию разметки, экспресс-оценку кошельков, устанавливать участников криптовалютных транзакций и рассчитывать риски. Сервис прошел успешную апробацию в сфере противодействия незаконному обороту наркотиков на площадке обслуживания криптовалютных транзакций в даркнете[[44]](#footnote-44).

Представляет интерес зарубежный опыт контроля и пресечения криптовалютных транзакций на нужды террористической деятельности.

В 2021 году финансовая разведка Канады выпустила руководство по индикаторам отмывания денег и финансирования терроризма с использованием криптовалютных транзакций[[45]](#footnote-45).

К признакам отмывания и финансирования терроризма отнесены:

преобладание в портфеле коинов повышенной анонимности;

большие объемы обмена биткоинов на коины повышенной анонимности;

регистрация на криптовалютной бирже нескольких человек под одним идентификатором (мобильный, IP-адрес и др.) в течение короткого периода времени;

кошелек / адрес виртуальной валюты фигурирует в «черных списках»;

операции в одно и то же время суток, переводы из фиата в крипту и обратно;

сложные переводы через длинные цепочки адресов / кошельков за короткий период;

криптовалюта поступает от внебиржевого брокера, который рекламирует свою анонимность.

Среди новых тенденций отмывания доходов/финансирования терроризма можно выделить:

- активный переход на коины повышенной анонимности (Monero, Dash, Zcash, Komodo). Вымогатели переходят на требования выплат в Monero;

- внедрение инструментов децентрализованного финансирования DeFi и взаимозаменяемых токенов NFT;

- использование криминальных сервисов блокчейн-аналитики. В 2019 г. в даркнете появился AML-бот, а в июле 2021 г. сервис Antinalysis, которые дают возможность анализировать применение транзакций с точки зрения правоохранительных органов. Пользователь получает скоринг-оценку вероятности блокировки его криптовалютных активов. Таким образом преступники получили возможность протестировать свои методы отмывания доходов/финансирования терроризма.

Криптовалюты и инфраструктура их обслуживания постоянно развиваются, что требует гибкого реагирования регуляторов, контрольно-надзорных органов, правоохранительных структур и финансовых институтов.

Перспективными направлениями дальнейшей разработки вопросов противодействия финансированию терроризма с использованием виртуальных активов и криптовалют представляются:

разработка современных типологий и схем финансирования терроризма с использованием новейших информационных технологий и децентрализованного управления финансами (DeFi);

централизованный мониторинг благотворительных акций, реализуемых в социальных сетях и интернет-мессенджерах, где размещаются реквизиты криптокошельков;

разработка реестра адресов/кошельков виртуальной валюты организаций и лиц, причастных к терроризму и экстремизму;

разработка реестра адресов/кошельков виртуальных валют, размещенных на онлайн-платформах террористической и экстремистской направленности (тематические группы соцсетей, сайты даркнета, сайты сбора средств, мессенджеры);

совершенствование методики и тактики выявления, раскрытия и расследования преступлений в сфере финансирования терроризма с использованием виртуальных активов и криптовалют;

вовлечение в антиотмывочную систему участников криптоиндустрии, организующих или осуществляющих выпуск и обращение цифровой валюты;

разработка профилей и реестров провайдеров услуг виртуальных активов, имеющих высокую риск-оценку;

законодательное регулирование отнесения цифровой валюты к имуществу в целях признания ее предметом преступления, а также ареста и конфискации виртуальных активов и криптовалюты;

обмен зарубежным опытом и совершенствование международного сотрудничества в сегменте криминальных операторов криптовалют и мониторинга транзакций виртуальных валют внутри блокчейнов.

СПИСОК ЛИТЕРАТУРЫ:

1. Dr. Dr. *Fabian Teichmann, Elena Park*. Terrorismusfinanzierung durch Kryptowaehrungen // ZRFC.2018. № 2.

Over 13% of Bitcoin Crime Proceeds Laundered Through Privacy Wallets: Elliptic // https://www.coindesk.com/over-13-of-bitcoin-crime-proceeds-laundered-through-privacy-wallets-elliptic

*Глотов В.И., Кржечковскис И.* Меры по снижению рисков отмывания денег и финансирования терроризма при осуществлении операций с виртуальными валютами, установленные в правовых актах ЕС и государств-членов ЕС // Финансовая безопасность. 2020. № 27. С. 62-70.

Руководство по применению риск-ориентированного подхода. Виртуальные валюты. Париж, ФАТФ, 2015. 86 с.

Financial firms and governments deeply skeptical of cryptocurrencies: Survey/ https://www.reuters.com/article/us-crypto-currencies/financial-firms-and-governments-deeply-sceptical-of-cryptocurrencies-survey

Social Media and Terrorism Financing. Asia/Pacific Group on Money Laundering /Middle East and North Africa Financial Action Task Force. January 2019. P. 4 //www.apgml.org.

How Terrorists use Cryptocurrency in Southeast Asia //https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia

Central Asian Jihadists use of cryptocurrencies in Bitcoin/https://moderndiplomacy.eu/2020/09/11/central-asian-jihadists-use-of-cryptocurrencies-in-bitcoin/

US Prosecutors Seize Bitcoin Allegedly Tied to Al Qaeda, ISIS, Hamas / https://www.coindesk.com/us-prosecutors-attempt-to-seize-bitcoin-allegedly-tied-to-al-qaeda; US Prosecutors Announce Historic Takedown of Global Terrorists Crypto Networks / https://www.moneylaundering.com/news/us-prosecutors-announce-historic-takedown-of-global-terrorists-crypto-networks/type=free

Eight charged in France for using cryptocurrency to finance terror / https: //amlintelligence.com/2020/10/eight-charged-in-france-for-using-cryptocurrency-tofinance-terror

US seizes $2 Million in Cryptocurrency From Terrorist Groups / [https://www.bankinfosecurity.com/us-seizes-2 million-in-cryptocurrency-from-terrorist-groups-a-14823](https://www.bankinfosecurity.com/us-seizes-2%20million-in-cryptocurrency-from-terrorist-groups-a-14823).

*Красинский В.В.* Методика работы в социальных сетях по выявлению экстремистского и иного противоправного контента // Современное право. 2020. № 2. С. 65-69 DOI 10.25799/NI.2020.83.61.008

*Юров А.А.* Важность международной интеграции в расследовании преступлений с использованием криптовалют // Финансовая безопасность. 2020. № 28. С. 55.

*Мозгов Е.А., Першина О.О.* Риски отмывания доходов и финансирования терроризма, связанные с пандемией COVID-19, и меры реагирования: Российский и зарубежный опыт // Финансовая безопасность. 2020. № 27. С.11-12.

Eastern Europe High Grassroots Adoption, Outsized Darknet Market and Ransomware Activity // https://blog.chainanalysis.com/reports/eastern-europe-cryptocurrency-market-2020

Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers //fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

Федеральный закон от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Рос. газ. 2020. 6 августа.

1. *Красинский В.В.* Финансирование терроризма преступными организациями и осужденными исправительных учреждений // Современное право. 2016. № 4. С. 88-92.
2. Указание Банка России от 20 октября 2020 г. № 5599-У «О внесении изменений в Положение Банка России от 2 марта 2012 г. № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // http://www.cbr.ru

Росфинмониторинг разработает систему слежения за сделками с криптовалютой/ Tass.ru/ekonomika/9169821

Эксперты оценили идею слежки за сделками с биткоинами /iz.ru/1046878/2020-08-11/eksperty-otcenili-ideiu-slezhki-za-sdelkami-s-bitcoinami

*Красинский В.В.* Противодействие финансированию терроризма с использованием криптовалют // Современное право. 2022. № 9. С. 108-116. **DOI 10.25799/NI.2022.58.84.018**

1. Первая криптовалюта (биткоин) была запущена еще в 2009 г, однако устойчивые риски финансирования терроризма с использованием криптовалют стали фиксироваться правоохранительными органами, начиная с 2015-2016 гг. [↑](#footnote-ref-1)
2. Криптовалюта – децентрализованная виртуальная валюта, которая не эмитируется и не обеспечивается ни одной юрисдикцией. Виртуальная валюта отличается от фиатной (национальной) валюты, представляющей собой монеты и банкноты, которые являются законным средством платежа, обращаются и принимаются в качестве средства обмена в стране-эмитенте. Понятие «цифровая валюта» используется в работе в качестве синонима виртуальной валюты. [↑](#footnote-ref-2)
3. Dr. Dr. *Fabian Teichmann, Elena Park*. Terrorismusfinanzierung durch Kryptowaehrungen // ZRFC.2018. № 2. По данным аналитической компании Elliptic, в 2020 г не менее 13% (по сравнению с 2% в 2019 г.) всех преступных доходов в биткоинах «отмыто» с помощью криптокошельков повышенной конфиденциальности, затрудняющих отслеживание транзакций (privacy wallets). См. Over 13% of Bitcoin Crime Proceeds Laundered Through Privacy Wallets: Elliptic // https://www.coindesk.com/over-13-of-bitcoin-crime-proceeds-laundered-through-privacy-wallets-elliptic [↑](#footnote-ref-3)
4. *Глотов В.И., Кржечковскис И.* Меры по снижению рисков отмывания денег и финансирования терроризма при осуществлении операций с виртуальными валютами, установленные в правовых актах ЕС и государств-членов ЕС // Финансовая безопасность. 2020. № 27. С. 62-70. [↑](#footnote-ref-4)
5. Руководство по применению риск-ориентированного подхода. Виртуальные валюты. Париж, ФАТФ, 2015. 86 с. [↑](#footnote-ref-5)
6. Financial firms and governments deeply skeptical of cryptocurrencies: Survey/ https://www.reuters.com/article/us-crypto-currencies/financial-firms-and-governments-deeply-sceptical-of-cryptocurrencies-survey [↑](#footnote-ref-6)
7. Там же. [↑](#footnote-ref-7)
8. См. Social Media and Terrorism Financing. Asia/Pacific Group on Money Laundering /Middle East and North Africa Financial Action Task Force. January 2019. P. 4 //www.apgml.org. [↑](#footnote-ref-8)
9. http: // www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html [↑](#footnote-ref-9)
10. Запрещена на территории России. [↑](#footnote-ref-10)
11. Кардинг (англ. carding) – мошенничество с платежными картами. [↑](#footnote-ref-11)
12. How Terrorists use Cryptocurrency in Southeast Asia //https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia [↑](#footnote-ref-12)
13. Запрещена на территории России. [↑](#footnote-ref-13)
14. Central Asian Jihadists use of cryptocurrencies in Bitcoin/https://moderndiplomacy.eu/2020/09/11/central-asian-jihadists-use-of-cryptocurrencies-in-bitcoin/ [↑](#footnote-ref-14)
15. Запрещены на территории России. [↑](#footnote-ref-15)
16. Запрещена на территории России. [↑](#footnote-ref-16)
17. How Terrorists use Cryptocurrency in Southeast Asia //https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia [↑](#footnote-ref-17)
18. Среди ведущих исламских теологов до сих пор продолжается полемика, можно ли считать криптовалюты совместимыми с шариатом. [↑](#footnote-ref-18)
19. Central Asian Jihadists use of cryptocurrencies in Bitcoin/https://moderndiplomacy.eu/2020/09/11/central-asian-jihadists-use-of-cryptocurrencies-in-bitcoin [↑](#footnote-ref-19)
20. Запрещена на территории России. [↑](#footnote-ref-20)
21. US Prosecutors Seize Bitcoin Allegedly Tied to Al Qaeda, ISIS, Hamas / https://www.coindesk.com/us-prosecutors-attempt-to-seize-bitcoin-allegedly-tied-to-al-qaeda; US Prosecutors Announce Historic Takedown of Global Terrorists Crypto Networks / https://www.moneylaundering.com/news/us-prosecutors-announce-historic-takedown-of-global-terrorists-crypto-networks/type=free [↑](#footnote-ref-21)
22. Eight charged in France for using cryptocurrency to finance terror / https: //amlintelligence.com/2020/10/eight-charged-in-france-for-using-cryptocurrency-tofinance-terror [↑](#footnote-ref-22)
23. Bits.media, 08.07.2021 [↑](#footnote-ref-23)
24. Использование Telegram-групп для финансирования терроризма отмечалось в сообщениях финансовых разведок США, Австралии, Малайзии, Кувейта и др. См. Social Media and Terrorism Financing. Asia/Pacific Group on Money Laundering /Middle East and North Africa Financial Action Task Force. January 2019. P. 6, 11-14 //www.apgml.org. По данным ближневосточного института медиа-исследований (Middle East Media Research Institute), Telegram-группы предлагали делать пожертвования в криптовалютах для террористических групп вплоть до июля 2020 г. См. US seizes $2 Million in Cryptocurrency From Terrorist Groups / [https://www.bankinfosecurity.com/us-seizes-2 million-in-cryptocurrency-from-terrorist-groups-a-14823](https://www.bankinfosecurity.com/us-seizes-2%20million-in-cryptocurrency-from-terrorist-groups-a-14823). [↑](#footnote-ref-24)
25. Примеры смены регистрации и переноса деятельности провайдеров виртуальных активов в государства с неадекватными нормами ПОД/ФТ см. Отчет ФАТФ. «Виртуальные активы. Признаки отмывания денег и финансирования террористов». Париж, ФАТФ. Сентябрь 2020 г. С. 18. [↑](#footnote-ref-25)
26. Во время мусульманских праздников верующие платят закят (обязательный налог) и садаку (добровольную милостыню). В 2018-2020 гг. в период Рамадана фиксировалось существенное пополнение бюджетов террористических структур «Катиба-ат-Таухид валь-Джихад», «Катиба Имама аль-Бухари», «Исламская партия Туркестана» и группировки «Лива аль-Мухаджирин валь-Ансар» для помощи братьям по вере, пленным мусульманским сестрам, поддержки исламского призыва. [↑](#footnote-ref-26)
27. *Красинский В.В.* Методика работы в социальных сетях по выявлению экстремистского и иного противоправного контента // Современное право. 2020. № 2. С. 65-69 DOI 10.25799/NI.2020.83.61.008 [↑](#footnote-ref-27)
28. US Prosecutors Seize Bitcoin Allegedly Tied to Al Qaeda, ISIS, Hamas / <https://www.coindesk.com/us-prosecutors-attempt-to-seize-bitcoin-allegedly-tied-to-al-qaeda>. [↑](#footnote-ref-28)
29. *Юров А.А.* Важность международной интеграции в расследовании преступлений с использованием криптовалют // Финансовая безопасность. 2020. № 28. С. 55. [↑](#footnote-ref-29)
30. *Мозгов Е.А., Першина О.О.* Риски отмывания доходов и финансирования терроризма, связанные с пандемией COVID-19, и меры реагирования: Российский и зарубежный опыт // Финансовая безопасность. 2020. № 27. С.11-12. [↑](#footnote-ref-30)
31. Запрещены на территории России. [↑](#footnote-ref-31)
32. US seizes $2 Million in Cryptocurrency From Terrorist Groups / [https://www.bankinfosecurity.com/us-seizes-2 million-in-cryptocurrency-from-terrorist-groups-a-14823](https://www.bankinfosecurity.com/us-seizes-2%20million-in-cryptocurrency-from-terrorist-groups-a-14823); US Prosecutors Seize Bitcoin Allegedly Tied to Al Qaeda, ISIS, Hamas / <https://www.coindesk.com/us-prosecutors-attempt-to-seize-bitcoin-allegedly-tied-to-al-qaeda>; US Prosecutors Announce Historic Takedown of Global Terrorists Crypto Networks / https://www.moneylaundering.com/news/us-prosecutors-announce-historic-takedown-of-global-terrorists-crypto-networks/type=free [↑](#footnote-ref-32)
33. Eastern Europe High Grassroots Adoption, Outsized Darknet Market and Ransomware Activity // https://blog.chainanalysis.com/reports/eastern-europe-cryptocurrency-market-2020 [↑](#footnote-ref-33)
34. Eastern Europe High Grassroots Adoption, Outsized Darknet Market and Ransomware Activity // https:// blog.chainanalysis.com/reports/eastern-europe-cryptocurrency-market-2020 [↑](#footnote-ref-34)
35. В настоящее время для расшифровки и отслеживания криптовалютных транзакций, как правило, используются аналитические средства Chainanalysis и Excygent. В России для этих целей применяется цифровой сервис «Прозрачный блокчейн». [↑](#footnote-ref-35)
36. Руководство по применению риск-ориентированного подхода. Виртуальные валюты. Париж, ФАТФ, 2015. 86 с. [↑](#footnote-ref-36)
37. *Глотов В.И., Кржечковскис И.* Меры по снижению рисков отмывания денег и финансирования терроризма при осуществлении операций с виртуальными валютами, установленные в правовых актах ЕС и государств-членов ЕС // Финансовая безопасность. 2020. № 27. С. 65. [↑](#footnote-ref-37)
38. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers //fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html [↑](#footnote-ref-38)
39. Ст.1 Федерального закона от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Рос. газ. 2020. 6 августа. [↑](#footnote-ref-39)
40. Указание Банка России от 20 октября 2020 г. № 5599-У «О внесении изменений в Положение Банка России от 2 марта 2012 г. № 375-П «О требованиях к правилам внутреннего контроля кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». [↑](#footnote-ref-40)
41. *Красинский В.В.* Финансирование терроризма преступными организациями и осужденными исправительных учреждений // Современное право. 2016. № 4. С. 88-92. [↑](#footnote-ref-41)
42. Сотрудничает с ФБР и ЦРУ США, используется Европолом. [↑](#footnote-ref-42)
43. Создана при участии АНБ США. [↑](#footnote-ref-43)
44. Росфинмониторинг разработает систему слежения за сделками с криптовалютой/ Tass.ru/ekonomika/9169821; Эксперты оценили идею слежки за сделками с биткоинами /iz.ru/1046878/2020-08-11/eksperty-otcenili-ideiu-slezhki-za-sdelkami-s-bitcoinami [↑](#footnote-ref-44)
45. https://www.fintrac-canafe.gc.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc\_mltf-eng [↑](#footnote-ref-45)