УДК 343.9.01
ББК 67.73

РОЛЬ КРИПТОВАЛЮТ В ФИНАНСИРОВАНИИ ТЕРРОРИЗМА

А. В. Рощупкина
Орловский юридический институт МВД России имени В. В. Лукьянова (Орёл, Россия)
ORCHID0009–0002–9325–1601

Развитие сети Интернет и электронных устройств радикально изменили все сферы жизни человека, помимо положительного аспекта, цифровизация привелаи к увеличению количества преступлений, совершаемых с использованием интернета. Одними из первых внедрили новые технологии террористы, которые воспользовались преимуществами цифровизации для повышения своей прибыли. Террористы обратили внимание на криптовалюту, рассматривая ее как цифровое платежное средство. Для них она имеет ряд привлекательных функций, таких как: псевдоанонимность, доступность, высокая скорость транзакций, легкое хранение и перевод. В настоящее время, правоохранительные органы используют прямую и косвенную деанонимизацию, анализ распространения, количественный анализ, анализ времени и анализ транзакционных сетей. В статье рассматривается криптовалюта как инструмент финансирования терроризма с приведением примеров положительного опыта работы правоохранительных органов, который может помочь в совершенствовании законодательной системы и оказать помощь в раскрытии подобных преступлений.

Ключевые слова: криптовалюта, цифровая валюта, финансирование терроризма, криптобиржа, терроризм, раскрытие преступлений, деанонимизация.

THE ROLE OF CRYPTOCURRENCIES IN TERRORIST FINANCING

A. V. Roshchupkina
Oryol Law Institute of the Ministry of Internal Affairs of Russia named after V. V. Lukyanov (Oryol, Russia) ORCHID0009–0002–9325–1601

The development of the Internet and electronic devices has radically changed all spheres of human life, in addition to the positive aspect, digitalization has led to an increase in the number of crimes committed using the Internet. Terrorists were among the first to introduce new technologies, who took advantage of digitalization to increase their profits. Terrorists have turned their attention to cryptocurrency, considering it as a digital means of payment. For them, it has a number of attractive features such as: pseudonymity, accessibility, high transaction speed, easy storage and translation. Currently, law enforcement agencies use direct and indirect deanonymization, distribution analysis, quantitative analysis, time analysis, and transactional network analysis. The article examines cryptocurrency as a tool for financing terrorism, giving examples of positive experience of law enforcement agencies, which can help in improving the legislative system and assist in solving such crimes.

Keywords: cryptocurrency, digital currency, terrorist financing, crypto exchange, terrorism, crime detection, deanonymization.

Doi: https://doi.org/10.14258/ralj(2024)4.12

Появление виртуальных активов и виртуальных поставщиков услуг по управлению активами принесли значительные позитивные изменения в наш мир, стимулируя инновации, повышая эффективность и способствуя расширению доступа к финансовым услугам. Тем не менее определенные характеристики виртуальных активов также делают их привлекательными для преступников, особенно с развитием сложных цифровых инструментов, таких как микшеры, тумблеры

и анонимайзеры, которые предназначены для сокрытия транзакционных связей с первоначальными владельцами валюты.

Стоит отметить, что число преступлений, совершенных с использованием информационно-телекоммуникационных технологий в России, возросло на 73,4%, в том числе с использованием сети Интернет — на 91,3%, при помощи средств мобильной связи — на 88,3% [1, с. 3]. Аналогичная картина наблюдается и по всему миру.

В докладе Содружества наций от 3 февраля 2016 г. говорится, что главные риски оборота виртуальных валют связаны с финансированием терроризма, совершением киберпреступлений и легализацией преступных доходов, полученных преступным путем. К их криминогенным признакам относят полную анонимность, скорость, дешевые, невозвратные переводы, сложные цепочки транзакций [2, с. 1].

Анонимность, скорость и неограниченность возможностей виртуальных активов и поставщиков услуг по управлению активами позволяют достигать поставленных преступных целей. Хотя число доказанных случаев использования террористами этих цифровых инструментов остается относительно небольшим, имеющиеся данные свидетельствуют о том, что это число неуклонно растет.

Под терроризмом законодатель понимает идеологию насилия и практику воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий [3, с. 2].

Финансирование терроризма — предоставление, сбор средств или оказание финансовых услуг с пониманием того, что они предназначены для финансирования организации, подготовки и совершения преступлений террористического характера, либо для обеспечения организованной группы, незаконного вооруженного формирования, преступного сообщества, созданных или создаваемых для совершения указанных преступлений.

Изначально террористические организации использовали фиатную валюту для своих целей, использование которой вызывало множество проблем (контроль за отмыванием денег, банковская политика и т. д.). В настоящее время террористы значительно повысили свое внимание к криптовалюте, в частности к биткоину. Использование криптовалюты помогает террористам обходить финансовые организации и их оперативные инструменты, разработанные специально для борьбы с финансированием терроризма. Собранные средства идут непосредственно на организацию и повышение эффективности конкретных атак, формирование штаба и подразделений, которые уже в процессе своей деятельности, путем хакерских атак, вымогательств, продажи наркотических средств и подобного добывают новые финансовые ресурсы, которыми зачастую выступает криптовалюта.

Росфинмониторинг России указал, что неоднократно фиксировались факты финансирования терроризма с использованием таких криптовалют, как: Bitcoin, Ethereumи Monero [4, с. 4].

Резолюция 2463 о противодействии финансирования терроризма, принятая Советом Безопасности ООН 28 марта 2019 г., определяет сбор, перемещение, передачу и предоставление доступа к средствам террористическим организациям как практическое понимание финансирования терроризма. В то же время, Группа разработки финансовых мер борьбы с отмыванием денег (ФАТФ) фокусирует внимание на целевом использовании средств «финансировании террористических актов, а также деятельности террористов и террористических организаций» [5, с. 88]. Актуальные научные труды на данную тему позволяют разрешить вышеуказанный спор посредством объединения мер, предпринимаемых лицами, финансирующими терроризм, и целями, преследуемыми ими, для формирования более наглядного представления процесса финансирования терроризма. Мартин Навиас идентифицирует три основных категории действий [6, с. 49] (создание фондов, перевод и использование средств) — в то время как Джессика Дэвис [7, с. 5] дополняет его еще тремя ключевыми видами деятельности: сбор, использование, хранение, перемещение и сокрытие средств, а также управление фондами. Данная интерпретация обращает внимание на то, что финансирование терроризма — это не просто кратко- и среднесрочные виды деятельности (привлечение, использование и перемещение средств), а также и долгосрочные соображения о надзоре и управлении финансовыми ресурсами. Помимо этого, исследователи акцентируют внимание на операционном и организационном финансировании. Первое направлено на поддержку готовящихся и потенциальных атак (включая процессы

подготовки боевиков, проведение исследований и разведывательной деятельности, приобретение оружия и иных материалов) [8, с. 20].

Различные международные организации и страны сосредотачиваются на определении финансирования терроризма в соответствии со своими собственными административными нормами и финансовой практикой. Согласно Организации Объединенных Наций средства для финансирования терроризма относятся ко всем видам активов, юридических документов или сертификатов, будь то материальные или нематериальные активы, движимые или недвижимые активы, полученные любым путем, подтверждающие права собственности или интересы таких активов в любом виде, включая электронные или цифровые формы, а также банковские кредиты, дорожные чеки, почтовые переводы, акции, ценные бумаги, облигации, переводные векселя и аккредитивы.

Группа разработки финансовых мероприятий (ФАТФ) и Организация Объединенных Наций (ООН) создали важнейшие механизмы, направленные на снижение рисков, связанных с использованием виртуальных активов и поставщиков сервисов для преступных целей и финансирования терроризма.

Эти методы предполагают:

1. Совершенствование нормативно-правовой базы. Государствам — членам ЕАГ рекомендуется внедрять законы, нормативные акты и практику в соответствии с международными стандартами, включая рекомендации ФАТФ и в соответствии с международным правом, в частности международным гуманитарным правом, международным законодательством в области прав человека и международным законодательством о беженцах.

2. Укрепление международного сотрудничества. Государствам –членам ЕАГ рекомендуется сотрудничать между собой и с международным сообществом для содействия в области обмена информацией, касающейся эффективных методов борьбы с неправомерным использованием виртуальных активов.

3. Поощрение партнерства между государственным и частным секторами. Государствам — членам ЕАГ предлагается развивать сотрудничество с междугосударственным сектором и поставщиками услуг по управлению виртуальными активами для понимания рисков и обеспечения соблюдения нормативных требований.

Кроме того, крайне важно проводить программы по наращиванию потенциала и обучению правоохранительных органов для расширения их возможностей в сфере противодействия терроризма, совершаемого с использованием криптовалют. Разработка специализированных инициатив по обучению, обеспечит подготовленность правоохранительных органов к мониторингу, раскрытию, расследованию и эффективному реагированию на неправомерные действия, связанные с виртуальными активами. Такие программы жизненно важны для того, чтобы опережать возникающие угрозы, связанные со злоупотреблением виртуальными активами, в том числе, и для финансирования терроризма.

Эффективное регулирование виртуальных активов и виртуальных поставщиков услуг по управлению активами является обязательным условием защиты финансовых систем от использования террористами. Внедряя согласованную практику в соответствии с международными правом и стандартами ФАТФ, а также укрепляя международное сотрудничество, можно значительно снизить риски, связанные с анонимностью и неограниченным характером виртуальных активов.

Помимо эффективного регулирования, большую роль в борьбе с данной категорией преступлений является своевременное предупреждение и раскрытие финансирования терроризма с использованием виртуальных активов. При раскрытии преступлений, связанных с использованием криптовалют, стоит уделять внимание деталям, поскольку потеря важной информации может сделать невозможным раскрытие преступления, а также изъятие и конфискацию криптовалюты. При раскрытии финансирования терроризма важно найти и надежно сохранить все электронные устройства вовлеченных лиц, а также все соответствующие электронные и физические следы любых носителей секретных ключей криптовалютных кошельков. Сотруднику важно понимать, как замораживать, арестовывать и конфисковать криптовалюты, полученные незаконным путем и предназначенные для финансирования терроризма или другой преступной деятельности. Предполагается, что для эффективного и своевременного раскрытия и расследования данного вида преступности сотрудник пра-

воохранительных органов должен иметь четкое представление о типах кошельков, бирж или трейдеров, о которых идет речь.

Также немаловажным тактическим шагом в раскрытии является планирование мер по предотвращению удаления улик владельцами устройств. Современное программное обеспечение обладает многочисленными возможностями для удаленного доступа к данным и управления устройствами, что позволяет перевести криптовалюту на другой кошелек, контролируемый сообщником, всего за несколько секунд. Поэтому важно убедиться, что подозреваемый не имеет возможности воспользоваться своим устройством даже на короткое время или промежуток времени между началом действия и физическим изъятием устройства, а также выключать изъятое устройство или переводить его в «режим полета» сразу после изъятия.

Большинство персональных устройств защищаются с помощью булавок, рисунков или касаний, распознавания лиц или отпечатков пальцев. Если нет возможности разблокировать устройство на месте происшествия, такое устройство может быть отправлено в специальное подразделение для взлома системы безопасности и извлечения данных.

Записи об открытых и закрытых ключах к криптовалютным кошелькам могут храниться в электронном виде на персональных электронных устройствах или носителях данных, на бумажном носителе и может быть обнаружен в ходе обыска в доме, на рабочем месте или в месте временного пребывания подозреваемого.

Типичными способами хранения ключа от кошелька являются компьютерный файл, «заметка» на смартфоне или строка символов, записанная в блокноте или на стикере, прикрепленном к дисплею компьютера или иным образом расположенном поблизости.

Общепринятой практикой среди правоохранительных органов, работающих по данному направлению преступности, является изъятие всех электронных устройств, обнаруженных у подозреваемого, в ходе обыска при нем, в месте его жительства или работы. При проверке электронного устройства сотрудник правоохранительного органа должен обращать внимание именно на следы использования и владения криптовалютного кошелька или сервиса. На владение или использование лицом криптокошелька могут указывать: электронные письма от криптовалютных бирж или трейдеров, подтверждающие доступ к криптовалютному кошельку; записи о транзакциях; поисковые запросы, связанные с криптовалютой, в истории браузера.

Подводя итог, можно сказать, что постепенный рост числа киберпреступлений демонстрирует применимость новых технологий в преступной деятельности. Основными характеристиками, привлекающими преступников к киберпреступности, являются высокая скорость действий, доступность, неограниченность, неопределенная юрисдикция государств и сложность расследования. Биткоин и другие криптовалюты изменили не только финансовую систему, но и способы и средства преступной деятельности. Одноранговые сети, микшеры и другие средства повышения анонимности позволили скрыть финансовые транзакции. Цифровая инфраструктура создала благоприятную среду международного финансирования террористических организаций и других преступлений.

Для успешного предупреждения использования криптовалют в качестве финансирования терроризма необходимо предпринять ряд комплексных действий. К ним относятся принятие международных стандартов регулирования виртуальных активов, обеспечение соответствия поставщиков услуг по управлению виртуальными активами нормативным актам и создание механизмов, основанных на оценке рисков, для выявления подозрительных операции.

Международное сотрудничество в обмене информацией о преступных транзакциях и владельцах кошельков имеет решающее значение. Для преодоления проблем, связанных с их децентрализованным и трансграничным характером, необходимо создать правовую базу для изъятия и конфискации криптовалют. Кроме того, немаловажными стали усилия по деанонимизации владельцев и противодействию смешиванию криптовалют, а также инвестиции в обучение сотрудников правоохранительных органов для повышения их возможностей в эффективной борьбе с цифровыми финансовыми преступлениями.

Анонимность криптовалют, ее собственности, опора на децентрализованные услуги, провайдеры, отсутствие целостной системы профилактики способствуют ее использованию для преступной деятельности. Чтобы эффективно снизить эти риски, страны должны инвестировать в надежные ка-

налы связи между правительствами и поставщиками услуг, а также расширять возможности обмена информацией.

На национальном уровне необходимо создать межведомственные «объединенные целевые группы», где опытные сотрудники, обладающие знаниями и навыками, необходимыми для противодействия преступлениям, связанным с использованием криптовалют, смогут осуществлять деятельность по противодействию преступности в данной сфере. На уровне ведомства, учитывая специфические проблемы, связанные с такими преступлениями, особенно их связь с финансированием терроризма, необходимо рассмотреть возможность создания специальных подразделений и оказать им поддержку со стороны государства.

Немаловажным остается и тот факт, что террористические организации используют комплексный подход, объединяя социальные сети, мессенджеры и криптовалюты для международного сбора средств. Таким образом, в этом контексте правоохранительные органы должны постоянно повышать свою осведомленность о быстро развивающихся криптовалютах и способах их использования.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Статистические сведения по преступлениям, совершенным с использованием сети Интернет. Официальные данные, предоставленные Порталом правовой статистики Генеральной прокуратуры РФ. URL: https//www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.

2. Доклад Содружества наций от 3 февраля 2016 г. // The commonwealth. URL: http://thecommonwealth.org/sites/default/files/pressrelease/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf.

3. О противодействии терроризму: Закон Российской Федерации от 6 марта 2006 г. №35-ФЗ // Российская газета. 2006.

4. Росфинмониторинг фиксирует факты финансирования терроризма с использованием криптовалют. 21.03.2021. Интервью заместителя руководителя Росфинмониторинга Германа Негляда. URL: https://tass-ru.turbopages.org/tass.ru/s/ekonomika/10978989.

5. Мелкумян К. С. ФАТФ в противодействии финансированию терроризма (специфика подхода) // Вестник МГИМО-Университета. 2014. 88 с.

6. Martin S Navias, Finance & Security: Global Vulnerabilities, Threats and Responses. London: C Hurst & Co., 2019.

7. Jessica Davis, Illicit Money: Financing Terrorism in the 21st Century. London: Lynne Rienner, 2021.

8. Nick Ridley, Terrorist Financing: The Failure of Counter Measures. Cheltenham: Edward Elgar, 2012.