В. Ф. Васюков
Московский государственный университет
международных отношений МИД России (МГИМО)
(Москва)
А. Н. Старжинская
Всероссийский государственный университет юстиции
(РПА Минюста России)
(Москва)

ОБ ОПЕРАТИВНО-РОЗЫСКНЫХ И СЛЕДСТВЕННЫХ МЕРАХ ПРОТИВОДЕЙСТВИЯ ЛЕГАЛИЗАЦИИ ПРЕСТУПНЫХ ДОХОДОВ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

Авторы поднимают вопросы о роли криптовалют в отмывании денежных средств, приводят данные о резком увеличении незаконного оборота криптовалюты. Приводится перечень сведений, которые могут быть получены уполномоченными сотрудниками при проведении оперативно-розыскных мероприятий и при взаимодействии с правоохранительными органами зарубежных стран. Акцентируется внимание на информации, которая может быть особо значима для раскрытия преступлений, связанных с легализацией преступных доходов. Уделяется внимание проведению различных мероприятий при установлении контроля за банкоматами, с помощью которых лица, причастные к преступной деятельности, обналичивают незаконные доходы. Также приводятся примеры раскрытия рассматриваемых преступлений в отдельных юрисдикциях.

Анализируются средства и методы, способствующие раскрытию преступления, связанного с легализацией преступных доходов. Отмечается важность анализа блокчейна с использованием аппаратно-программных комплексов и ресурсов сети Интернет. Изучается возможность применить методы OSINT для аккумулирования и изучения информации, содержащейся в открытых источниках. Делается акцент на том, что благодаря именно этим методам оперативный сотрудник может получить информацию о незарегистрированных криптобиржах. Раскрывается специфика расследования рассматриваемых преступлений в Российской Федерации. Формулируются выводы о том, что использование криптовалют в легализации преступных доходов требует от правоохранительных органов периодически всесторонне оценивать риски и совершенствовать методику раскрытия и расследования преступлений, связанных с цифровыми финансовыми активами этой категории.

Ключевые слова: *раскрытие преступления, выявление преступления, оперативно-розыскная деятельность, криптовалюта, криптопреступление, легализация преступных доходов, блокчейн*

Для цитирования

Васюков В. Ф., Старжинская А. Н. Об оперативно-розыскных и следственных мерах противодействия легализации преступных доходов с использованием криптовалют // Российское право: образование, практика, наука. 2024. № 4. С. 68–78. DOI: 10.34076/2410-2709-2024-142-4-68-78.

УДК 343.1 DOI: 10.34076/2410-2709-2024-142-4-68-78

Введение

В современном мире сложно представить финансирование преступной деятельности вне цифровой плоскости. Механизмы оборота криптовалюты становятся все более привлекательными для организованных преступных формирований, сообществ и синдикатов. Будучи децентрализованным финансовым институтом, криптовалюта стала и новым удобным средством легализации преступных доходов по всему миру.

Преступники в целях анонимизации используют различные методы сокрытия своих деяний, что на практике затрудняет, а то и делает технически невозможным отслеживание маршрута, по которому прошли деньги. Часто используется искусственное усложнение транзакций с целью затруднить отслеживание денег. Одно из системных отличий цифровых транзакций от фиатных заключается в том, что первые могут проводиться очень быстро, в большом количестве и на очень маленькие суммы. Это усложняет отслеживание и позволяет обойти любые ограничения на подачу отчетности по подозрительным операциям, связанным с легализацией преступных доходов.

Также следует упомянуть о том, что с переходом человеческой деятельности из физического мира в виртуальный появились виртуальные активы, понимаемые согласно определению Группы разработки финансовых мер борьбы с отмыванием денег (ФАТФ) как цифровое представление стоимости, которое может быть обменено или передано в цифровой форме и использовано в качестве формы платежа или инвестиционного инструмента[1].

Появление криптовалют, основанных на технологии распределенного реестра (DLT), придало новый вектор развитию финансовой системы государств. Однако, как и многие другие инновации, криптовалюты стали успешно использоваться международными преступными синдикатами в сфере незаконного оборота наркотиков, оружия, финансирования терроризма и т. д. Т. В. Пинкевич справедливо отмечает, что преступления, совершенные в отношении криптовалюты либо с ее использованием, характеризуются высокой степенью общественной опасности, которая определяется ущербом, причиненным личности, обществу и государству, наличием особого субъекта, в качестве которого зачастую выступают представители транснациональной организованной преступности, особенностями предмета и средств совершения таких преступлений, социальными последствиями, высоким уровнем латентности [Пинкевич 2021: 83].

Принято выделять основные факторы, повышающие риск использования криптовалют в преступных целях:

а) анонимность создания виртуальных активов;

б) возможность контроля одним и тем же лицом нескольких десятков (сотен) виртуальных кошельков;

в) децентрализованный характер большинства криптовалют (отсутствие централизованного контролирующего органа);

г) трансграничный диапазон осуществления бесконтрольных транзакций [Пушкарев, Токолов 2023: 88; Зайцев, Сулаева 2021: 28; Самойло 2023: 32].

Проблемы, возникающие в результате расхождений в регулировании, усиливаются из-за обилия криптобирж и их работы сразу в нескольких юрисдикциях. Это существенно увеличивает риски использования виртуальных активов в целях сокрытия противоправной деятельности. Кроме того, в последнее десятилетие международные организации выражали обеспокоенность по поводу возможного использования криптовалют для содействия финансированию терроризма, особенно в качестве средства для анонимного направления пожертвований или взносов в террористические организации.

Тот факт, что операции с криптовалютами происходят в киберпространстве, определяет необходимость изменить оперативную и следственную тактику, значительно усовершенствовать методы и инструменты раскрытия и расследования криптопреступлений. Это, в частности, обосновывается тем, что как таковое место совершения преступления в данном случае определяется множеством критериев и факторов (расположение сервера, адрес криптобиржи, тип кошелька и т. д.).

[1] Guide on Relevant Aspects and Appropriate Steps for the Investigation, Identification, Seizure, and Confiscation of Virtual Assets. 2021 // URL: https://biblioteca.gafilat.org/wp-content/uploads/2024/04/Guide-on-relevant-aspects-and-appropriate-steps-for-the-investigation-identification-seizure-and-confiscation-of-virtual-assets.pdf (дата обращения: 05.10.2024).

В отдельных случаях определить место преступления невозможно в силу технологических особенностей функционирования сети.

Таким образом, эффективность раскрытия и расследования преступлений, связанных с криптовалютами, во многом зависит от того, насколько уполномоченные субъекты смогли адаптироваться к новой технологической реальности, в которой им приходится работать.

Роль криптовалют в легализации преступных доходов

По данным аналитической группы *Chainalysis*, только в 2023 г. 109 адресов обмена депозитов получили незаконной криптовалюты на сумму более 10 млн долл. каждый, а в совокупности они получили 3,4 млрд долл. незаконной криптовалюты[1].

Виртуальные активы стали использоваться для легализации преступных доходов в связи с появлением онлайн-рынков нелегальных товаров и услуг (наркотики, оружие, компьютерные вирусы, хакерские услуги и т. д.) в «Темной сети», или Даркнете. Доступ к Даркнету возможен только с помощью технологических инструментов, обеспечивающих анонимный поиск. Выпуск в 2009 г. биткоина сделал возможным функционирование «темных рынков», основанных на циркуляции платежных средств децентрализованного характера [Сильченко, Васильев 2023: 169].

Появление первого из таких рынков («Шелковый путь») на заре 2011 г. ознаменовало начало новой эры в торговле запрещенными товарами и услугами. Несмотря на то что указанная торговая площадка была заблокирована, на смену ей сразу же пришли другие площадки. Сегодня множество «темных рынков» в Даркнете выступают источником значительной доли незаконных средств, перекачиваемых через виртуальные валюты и связанные с ними сервисы. В исследовании ФАТФ, посвященном анализу криптовалютных транзакций, был сделан вывод о том, что почти все биткоины незаконного происхождения, «отмытые» через платформы обмена криптовалют, поступили с «темных рынков»[2].

Криптовалюты также используются для легитимации средств, полученных от мошенничества, финансовых пирамид, взяточничества, рейдерства, контрабанды товаров, незаконного оборота наркотиков и пр. Например, китайская финансовая пирамида *PlusToken* принесла ее организаторам более 3 млрд долл. незаконной прибыли, большая часть которой была успешно выведена через сервисы конвертации криптовалют. По мнению отдельных специалистов, такая масштабная конвертация криптовалюты в фиатную валюту стала причиной резкого падения стоимости биткоина в августе 2019 г. [Dupuis, Gleason 2020].

Процесс легализации преступных доходов с помощью криптовалюты включает те же три этапа, что и традиционный процесс: «размещение», «наслоение» и «интеграцию». Специфика алгоритмов, применяемых на каждом этапе, обусловлена технологическими особенностями задействованных виртуальных активов.

Так, необходимость этапа «размещения» зависит от того, получены ли незаконные средства в фиатной валюте или непосредственно в криптовалютах. В первом случае необходимо провести конвертацию из одной валюты в другую, а во втором – нет. На этапе «размещения» фигуранты обычно используют платформы обмена криптовалют – для конвертации фиатной валюты в биткоины или другие аналогичные виртуальные активы.

Стадия «наслоения» сводится к «смешиванию» виртуальных активов посредством использования специализированных сервисов – «миксеров», объединяющих поступающие от разных пользователей средства. Пройдя через «миксер», криминальные криптовалюты перемешиваются с легальными, и в итоге обнаружение цифровой цепочки транзакции значительно осложняется.

Основная концепция деятельности «миксеров» напоминает инвестиционные фонды, в которых несколько человек аккумулируют свои средства для получения коллективной выгоды. Разница заключается в том, что «миксеры» используются для осуществления множества криптовалютных транзакций, а выгода состоит в достижении большей анонимности за счет отсутствия «привязки»

[1] Money Laundering Activity Spread Across More Service Deposit Addresses in 2023, Plus New Tactics from Lazarus Group. 2024 // URL: https://www.chainalysis.com/blog/2024-crypto-money-laundering (дата обращения: 05.10.2024).

[2] Virtual Assets and Virtual Assets Service Providers. Guidance for a Risk-Based Approach. 2021 // URL: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf (дата обращения: 05.10.2024).

переводов к конкретным криптовалютным адресам. Владельцы «миксеров», как правило, берут плату за свои услуги, при этом маскируют свою инфраструктуру, работая как «скрытые сервисы» системы TOR (*The Onion Router*).

У различных типов «миксеров» есть общая особенность: смешивание и разделение криптовалют перестает работать, если отдельные пользователи вносят очень крупные суммы, поскольку бóльшая часть этих сумм возвращается к ним. Соответственно перед тем, как пропустить криптовалюту через «миксер», блокчейн дробится на несколько сотен адресов криптокошельков.

На этапе «интеграции» фигуранты переводят криптоактивы (полученные в результате «наслоения») в централизованные и легальные финансовые системы, чтобы узаконить денежные потоки. Через биржи криптовалюты могут быть конвертированы в фиатную валюту как законные средства, которые затем свободно используются для покупки недвижимости, предметов роскоши и иных ценностей. Для «интеграции» все чаще стало использоваться программное и аппаратное обеспечение для майнинга, позволяющее злоумышленникам самостоятельно создавать новые криптомонеты.

Особенности выявления и раскрытия легализации преступных доходов с использованием криптовалют

При выявлении преступлений, связанных с криптовалютами, в распоряжении правоохранительных органов может находиться различная информация, полученная при проведении оперативно-розыскных мероприятий, в результате обмена с другими национальными правоохранительными органами или в результате сотрудничества с коммерческими организациями. Особую значимость для раскрытия рассматриваемых преступлений представляют следующие сведения:

идентификационные данные (псевдонимы / никнеймы), адреса сообщников, электронные адреса социальных сетей, номера телефонов, адреса электронной почты, которые они могли использовать;

записи подозрительных транзакций, осуществляемых через криптобиржи, а также любая другая деятельность с активами;

сводные отчеты по запросу из банковских организаций, налоговых органов, а также органов регулирования ценных бумаг или страхования;

данные из открытых источников, в частности стоимость различных криптовалют, контактная информация, адреса криптобирж, кошельков, ссылки на сайты с рекламой и т. д.;

данные, имеющиеся у оперативных подразделений, специализирующихся на кибербезопасности (отчеты об инцидентах, связанных с финансовым сектором; сведения о вредоносных программах, направленных на хищение личных данных или несанкционированный сбор конфиденциальной и / или финансовой информации).

Сообщения о подозрительных операциях, предоставляемые операторами криптовалют, очень полезны для расследований, поскольку они содержат информацию о транзакциях (клиент-эмитент, бенефициар, адреса кошельков клиентов, баланс в кошельках, дата и время транзакций, тип переданных виртуальных активов, место перевода, отмененные транзакции, зарегистрированные или проверенные банковские счета, тип используемых устройств) и о клиенте (имя, идентификатор пользователя, IP-адрес, физический платежный адрес, адрес электронной почты, дата рождения, национальность, гражданство, экономический профиль и коммерческая деятельность).

Обмен криптовалюты на фиатную валюту может также осуществляться через обменные платформы P2P, которые не подпадают под регулирование ПОД / ФТ (противодействие отмыванию доходов и финансированию терроризма) в соответствии с Рекомендацией 15 ФАТФ. Несмотря на то что в настоящее время такие платформы обрабатывают низкий процент операций, через них могут осуществляться транзакции, затрудняющие отслеживание криптовалют и маскирующие их происхождение (например, *chain hopping*, *coinjoin*). Между тем организации, владеющие криптовалютными киосками или «биткоин-банкоматами», для конвертации криптовалюты в фиатную валюту в соответствии с рекомендациями ФАТФ обязаны получать информацию о своих клиентах и сообщать об операциях, которые считаются подозрительными.

Местонахождение банкоматов, предположительно используемых лицами, представляющими оперативный интерес, может стать отправной точкой для наблюдения за ними либо их возможными сообщниками (как физически, так и с помощью электронных средств) [Каширгов, Семенов 2021: 310]. Если наблюдение за банкоматом позволяет определить точную дату и время обменной операции, осуществленной фигурантом, эти данные (в том числе сведения о сумме, виде криптовалюты и виртуальных адресах участников транзакции) могут быть запрошены у компании, ответственной за эту операцию. На основе указанных данных можно восстановить происхождение и назначение задействованных криптовалют.

Так, в Испании была выявлена и ликвидирована преступная организация, оказывающая услуги по легализации преступных доходов. Фигуранты реализовали схему, включающую конвертацию фиатной валюты в виртуальные активы с использованием криптобанкоматов и «смурфинга» – разделения незаконных доходов на более мелкие суммы и их размещения в многочисленных банковских счетах, чтобы избежать активации сигнала системы выявления подозрительных транзакций. В результате межведомственной операции «Гватузо» было «заморожено» четыре «холодных» кошелька и 20 «горячих» кошельков, на которых находилось 9 млн евро[1].

Одной из ключевых особенностей схемы, которая привлекла внимание испанских оперативных служб, стала активность, проявляемая лицами определенного контингента в районе расположения двух криптобанкоматов. Оперативно-розыскные мероприятия позволили установить, что денежные средства, полученные от наркоторговли, вносились в специальные банкоматы с помощью «денежных мулов», после чего конвертировались в криптовалюту и отправлялись на криптобиржи, зарегистрированные в других государствах. «Денежные мулы» (или просто «мулы») – физические лица, которые получают наличные деньги от членов организованных сообществ, кладут их на свой банковский счет, затем переводят их на счет другому «мулу», образуя «караван». В другой ситуации, не менее распространенной, деньги «мулами» обналичиваются в кассе банка (банкомате) и перевозятся (переправляются) по спланированному маршруту для передачи фигурантам [Клевцов 2023: 55].

Подбор «мулов» осуществляется посредством онлайн-форумов вакансий, электронных писем, социальных сетей через замаскированные объявления о поиске «менеджеров по переводу денег». Чаще всего такими «менеджерами» становятся безработные, студенты и должники по микрозаймам.

В объявлениях о найме «мулов» нет конкретных должностных обязанностей, требований к образованию и опыту работы соискателя, но есть указание на быстрый заработок с минимальными усилиями. Возможность легко заработать деньги преподносится как отсутствие рисков, используются выражения «законные деньги», «100 %-ая гарантия», «наличные в тот же день» и т. п. При согласии кандидат должен заполнить форму, в которой указывает личные данные и контактную информацию (телефон и адрес электронной почты) и к которой прилагает копии документов, удостоверяющих личность, документ, выданный банком (банковский идентификационный номер), а также документ, подтверждающий адрес (копия счета коммунальной компании). Контакты с предполагаемым работодателем всегда поддерживаются по электронной почте или по телефону из-за срочности переводов[2].

Главная цель фигурантов – установить контроль за банковской картой «мула» для регулярной легализации преступных доходов. После каждой транзакции «мулу» остается определенный процент от суммы (0,5–1 %), которая им передается по «каравану» (обналичивается). В отдельных случаях производится фиксированная оплата в зависимости от выполняемой работы.

Так, полиция Индии инициировала расследование крупномасштабного хищения с использованием мобильного приложения, созданного как инвестиционная платформа для майнинга криптовалюты[3]. Приложение

[1] Cryptocurrency Laundering as a Service: Members of a Criminal Organisation Arrested in Spain // URL: https://www.europol.europa.eu/media-press/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain (дата обращения: 05.10.2024).

[2] European Money Mule Action // URL: https://ind.millenniumbcp.pt/en/Particulares/seguranca/Pages/Money-Mule.aspx (дата обращения: 05.10.2024).

[3] Indian Police Nabbed Four for $14 Million Crypto Scam // URL: https://www.financemagnates.com/crypto-

обещало долю в прибыли, полученной от таких инвестиций. В один момент оно перестало работать, а его операторы перестали отвечать на запросы инвесторов. Следователи запросили информацию у Подразделения финансовой разведки Индии, которым были выявлены две организации, управляющие приложением в *Google Play Store*, и 34 организации, с ними связанные. Таким образом, в ходе расследования была обнаружена сеть подставных организаций, занимающихся обманом граждан. Незаконные денежные средства, собранные с жертв, легализовались с помощью банковских счетов «мулов», а часть преступных доходов в итоге конвертировалась в виртуальные активы. Преступные доходы в виде остатков на банковских счетах различных подставных лиц на сумму 865 млн индийских рупий (9,9 млн евро) были обнаружены и заморожены.

Важным источником информации, который помогает отслеживать происхождение и назначение криптовалют, предположительно связанных с незаконной деятельностью, выступает блокчейн. Это источник одновременно актуальный и относительно надежный, поскольку децентрализованная структура криптовалют не позволяет изменять записи в нем [Клевцов, Квык 2020: 60].

Из данных, записанных в блокчейне, оперативные подразделения могут узнать полную историю транзакций адреса цифрового финансового актива, включая адреса всех пользователей, с которыми пользователь проводил транзакции, а также дату, время и точную сумму перевода (что может быть полезно в качестве критерия поиска при анализе многих транзакций одновременно), полную цепочку транзакций, совершенных каждым криптоаккаунтом с момента его создания. Анализ всех этих сведений и их перекрестная проверка с информацией, полученной из других источников (особенно если она осуществляется с помощью аппаратно-программных комплексов), может иметь решающее значение для выявления преступной деятельности с использованием криптовалют, для установления личности преступников и получения изобличающих доказательств.

Чтобы идентифицировать лиц, подозреваемых в незаконной деятельности с использованием криптовалют, важно классифицировать все адреса платформ обмена криптовалюты, «миксеров», онлайн-букмекеров и незаконных рынков в Даркнете.

Для идентификации виртуальных активов и связанных с ними операций могут быть использованы следующие инструменты или методы:

1. *Анализ блокчейна*, который проводится с использованием соответствующих технологических инструментов. Одним из инструментов, который можно найти в свободно распространяемых в Интернете версиях программного обеспечения с открытым исходным кодом, являются сетевые приложения (например, *blockchain explorers*), которые работают как поисковые системы в экосистеме криптовалют, позволяя находить адреса, транзакции и другие связанные с ними данные. Существуют и более сложные компьютерные ресурсы, которые специально разработаны для нужд правоохранительных органов и находятся в распоряжении коммерческих организаций, специализирующихся на анализе блокчейна [Морозова 2022: 245].

Чтобы идентифицировать лиц, подозреваемых в незаконной деятельности с использованием криптовалют, важно классифицировать все адреса платформ обмена криптовалюты, «миксеров», онлайн-букмекеров и незаконных рынков в Даркнете

2. Методы «разведки из открытых источников» (*Open Source Intelligence*, OSINT), которые могут дополнить информацию, полученную в результате анализа блокчейна, и предполагают систематический сбор, обработку и анализ сведений, доступных широкой общественности без ограничений. Например, никнейм пользователя можно найти благодаря поисковым системам сети Интернет, поскольку довольно часто лица, занимающиеся незаконной онлайн-торговлей, размещают свой адрес (связывая его со своим онлайн-профилем и псевдонимом) на форумах (*Reddit*, *4Chan* и *8Chan*) или в разделах комментариев на специализированных криптовалютных сайтах. Кроме того, можно обратиться к сайтам, специально предназначенным для идентификации пользователей виртуальных акти-

currency/news/indian-police-nabbed-four-for-14-million-crypto-scam/ (дата обращения: 05.10.2024).

вов и связанных с ними адресов (например, *walletexplorer.com*) [Колычева 2022: 173].

Тот же прием можно использовать для получения информации в Даркнете, где существует множество форумов (*Dread*, *Darknet Avengers*, *The Hub*, *Exploit.in*), на которых, пользуясь обеспечиваемой TOR-браузером анонимностью, люди свободно делятся информацией о скрытых сервисах, включая их адреса, предлагаемые ими товары и услуги, комментарии о качестве сервиса, никнеймах наиболее (или наименее) успешных трейдеров и т. д. [Wang, Hsieh 2024: 40]. Методы OSINT могут быть эффективны и для получения информации о незарегистрированных криптобиржах, которые предоставляют услуги лицам, занимающимся незаконной деятельностью с криптовалютами, включая «миксеры» или платформы обмена криптовалюты P2P, поскольку они работают на основе той же системы репутации, что и незаконные онлайн-рынки. Наконец, информация из открытых источников может быть полезна, чтобы лучше понять, каков образ жизни подозреваемого, где он проживает и осуществляет свою коммерческую и (или) социальную деятельность.

Чтобы повысить эффективность раскрытия преступлений, связанных с криптоактивами, рекомендуется сочетать изложенные методы и традиционные оперативно-розыскные мероприятия (опрос, наведение справок, наблюдение, отождествление личности и т. д.).

Специфика расследования преступлений, совершаемых с использованием криптовалют

Появление виртуальной реальности, в которой «локализуются» отдельные элементы объективной стороны преступления, требует кардинально изменить подход к сбору и фиксации доказательств.

Так, по ряду уголовных дел, которые расследованы следователями Следственного комитета Российской Федерации и по которым вынесены обвинительные приговоры, установлено множество фактов, когда преступники получили криптовалюту в качестве вознаграждения за сбыт наркотических средств. В последующем фигуранты совершали финансовые операции путем обмена (продажи) криптовалюты (биткоинов, латкоинов) на национальную валюту с использованием интернет-сервисов *Bit-Pay*, «Моментальный обмен 24-7», «Круглосуточный Моментальный Обмен», *4ange.me*, *next24.net*, *Trust*, *Exodus*, *Bit-Bits.net*, *e-obmen.cc*, *Coin-bank.co*, *bestchange.ru*, P2P, *Bitpapa*, а также криптобирж *Binance* и *Bitzlato*.

Например, в ходе расследования установлено, что с 20 марта по 24 июня 2023 г. Н., совершая преступления в сфере незаконного оборота наркотиков и выполняя функции «закладчика», получал вознаграждения в криптовалюте «биткоин», которые перечислялись на открытый им неперсонифицированный электронный кошелек. В дальнейшем Н. конвертировал полученную криптовалюту в рубли на общую сумму более 128 тыс. руб. По результатам рассмотрения уголовного дела в суде в отношении Н. вынесен обвинительный приговор.

Несложный алгоритм конвертации криптовалюты и доступность программного обеспечения для использования криптокошельков позволяют применять такие инструменты в преступных целях и несовершеннолетним. Были выявлены факты легализации ими криптовалюты, полученной в результате совершения преступлений в сфере незаконного оборота наркотиков.

Следует отметить, что отсутствие у криптовалют процессуального статуса порождает проблемы в правоприменении, однако в силу необходимости наложить арест на виртуальные активы при расследовании преступлений должны использоваться наиболее эффективные механизмы, обеспечивающие сохранность арестованных активов.

Так, в 2023 г. в СК РФ расследовано и направлено в суд уголовное дело в отношении лица, совершившего преступление, предусмотренное ч. 2 ст. 273, п. «б» ч. 4 ст. 174.1 УК РФ. Установлено, что с 1 сентября по 26 декабря 2020 г. фигурант, используя компьютерные программы, предназначенные для вмешательства в функционирование средств хранения компьютерной информации, а также «фишинговый» сайт *www.blochchian.ru*, оформленный не осведомленным о его преступных намерениях М., похитил криптовалюту в количестве 8,9999346 биткоинов, принадлежащую Б., который ошибочно перешел по ссылке «фишингового» сайта. В последующем злоумышленник легализовал похищенные им биткоины, конверти-

ровав их в фиатную валюту на сумму более 16 млн руб. и приобрел на вырученные деньги объекты недвижимости в Московской области. В ходе расследования на имущество обвиняемого – криптовалюту «биткоин» в количестве 22,83913281 единиц, эквивалентном 641 328 долл. США, – наложен арест.

Если ключи доступа к криптокошельку находятся в руках их владельцев, «заморозка» средств нецелесообразна, так как распоряжаться активами могут и лица, имеющие копию ключа. Иначе говоря, подельники фигуранта, имея ключ доступа, могут оперативно перевести криптовалюту на кошелек, который ранее использован не был. В этом случае единственный способ сохранить все имеющиеся активы – перевести криптовалюту на контролируемый правоохранительными органами кошелек. Соответственно, в этих целях заблаговременно создается кошелек при проведении следственного действия, о чем составляется протокол.

Факты легализации преступных доходов с использованием криптовалюты подтверждались проведенными в ходе предварительного расследования допросами обвиняемых, специалистов, осмотрами предметов (смартфонов, в которых установлены специальные программы кошельков для выполнения операций с криптовалютой в сети Интернет), документов (выписок по банковским счетам и др.), осмотром переписки обвиняемых в мессенджере «Телеграм» и личной почты фигурантов, полученными от операторов криптовалютных платформ сведениями.

Приведем в пример расследованное уголовное дело по факту организации сбыта наркотических средств жителями Мурманской области. В ходе осмотра персонального компьютера участницы преступной группы техническое средство было переведено в режим, защищающий доступ к сети сотового оператора мобильной связи и к иным беспроводным интерфейсам, служащим для приема и передачи информации в локальную и глобальную сеть. После этого удалось установить не только непосредственно переписку участницы с организатором преступной деятельности в приложении «Телеграм», но и криптокошелек, с использованием которого осуществлялись финансовые операции с денежными средствами с помощью пиринговой платежной системы *Bitcoin*.

Заключение

Повторим, что стремительная эволюция цифрового пространства постоянно приводит к появлению новых инструментов проведения финансовых операций. Использование криптовалют в преступной деятельности в силу присущей им псевдоанонимности представляет собой серьезную проблему для правоохранительных органов, что требует периодически всесторонне оценивать риски использования виртуальных активов, а также совершенствовать методику раскрытия и расследования преступлений рассматриваемой группы. Нужно вырабатывать новые методы выявления и мониторинга транзакций, изобличения анонимизированных аккаунтов, используемых фигурантами. Этому, в частности, можно способствовать, если расширить практику взаимодействия подразделений финансовой разведки и правоохранительных органов.

Список литературы

Dupuis D., Gleason K. Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic // Journal of Financial Crime. 2020. Vol. 28. №. 1. P. 60–74.

Wang H. M., Hsieh M. L. Cryptocurrency Is New Vogue: A Reflection on Money Laundering Prevention // Security Journal. 2024. № 37. P. 25–46.

Зайцев А. А., Сулаева Д. С. Криптовалюта как элемент криминалистической характеристики преступлений // Проблемы правовой и технической защиты информации. 2021. № 9. С. 28–32.

Каширгов А. Х., Семенов Е. А. Некоторые вопросы противодействия преступлениям, совершенным с использованием IT-технологий // Евразийский юридический журнал. 2021. № 9. С. 309–310.

Клевцов К. К. Особенности взаимодействия правоохранительных органов с зарубежными поставщиками услуг виртуальных валют (на примере localbitcoins) // Вестник Московского университета МВД России. 2023. № 1. С. 139–145.

Клевцов К. К., Квык А. В. Изъятие и осмотр информации, находящейся в электронной памяти абонентских устройств // Законность. 2020. № 12. С. 56–60.

Колычева А. Н. Перспективы внедрения искусственного интеллекта в раскрытие и расследование преступлений // Научный вестник Орловского юридического института МВД России имени В. В. Лукьянова. 2022. № 3. С. 172–179.

Морозова Н. В. Некоторые особенности расследования компьютерных преступлений // Современное уголовно-процессуальное право – уроки истории и проблемы дальнейшего реформирования: сб. материалов Междунар. науч-практ. конф., посвященной 100-летию принятия УПК РСФСР 1922 г., 20-летию действия УПК РФ: в 2 ч. Орел: ОрЮИ МВД России им. В. В. Лукьянова, 2022. Ч. 1. С. 240–245.

Пинкевич Т. В. Предупреждение преступлений, совершаемых в сфере оборота цифровой валюты (криптовалюты) // Правовое государство: теория и практика. 2021. № 4. С. 82–96.

Пушкарев В. В., Токолов А. В. Основы организации противодействия преступлениям, совершаемым с использованием криптовалют // Вестник экономической безопасности. 2023. № 4. С. 88–92.

Самойло В. А. Характерные особенности преступлений, связанных с использованием криптовалют // Преступность в СНГ: проблемы предупреждения и раскрытия преступлений: сб. материалов конф.: в 3 ч. Воронеж, 2023. Ч. 1. С. 337–338.

Сильченко Е. В., Васильев А. М. Криптовалюта как средство обезличивания при совершенном или совершающемся преступлении // International Law Journal. 2023. Т. 6. № 3. С. 168–172.

Виталий Федорович Васюков – доктор юридических наук, профессор, профессор кафедры уголовного права, уголовного процесса и криминалистики Московского государственного университета международных отношений МИД России (МГИМО). 119454, Российская Федерация, Москва, проспект Вернадского, д. 76. E-mail: vvf0109@yandex.ru.

ORCID: 0000-0003-0743-5616

Анна Николаевна Старжинская – кандидат юридических наук, доцент кафедры уголовного процесса и криминалистики Всероссийского государственного университета юстиции (РПА Минюста России). 117638, Российская Федерация, Москва, ул. Азовская, д. 2. E-mail: starzhinskaya1983@mail.ru.

ORCID: 0009-0008-0435-1023

On the Operational and Investigative Measures to Counter Money Legalization Using Cryptocurrencies

The paper raises the questions about the role of cryptocurrencies in money laundering, and provides data on a sharp increase in illegal turnover. The authors present a list of information that can be obtained by authorized employees during operational activities, as well as when interacting with foreign law enforcement agencies. Emphasis is laid on information that may be particularly important for solving crimes related to the legalization of criminal proceeds. Attention is also paid to conducting various measures to establish control over ATMs, through which persons involved in criminal activity cash out illegal proceeds. Examples of solving the crimes in question in several jurisdictions are also given.

The authors analyze the means and methods that contribute to the disclosure of a crime related to the legalization of criminal proceeds. The importance of analyzing the blockchain using various hardware and software systems, as well as Internet resources is determined. The possibility of using the OSINT methods for accumulating and studying information in open sources is considered. It is emphasized that thanks to theese methods, an operative officer can obtain information about unregistered crypto exchanges. The authors reveal the specifics of investigating the crimes in question in the Russian Federation. Conclusions are made that the use of cryptocurrencies in the legalization of criminal proceeds requires law enforcement agencies to periodically conduct

a comprehensive risk assessment, as well as to improve the methodology for solving and investigating crimes related to cryptocurrencies.

Keywords: *crime detection, operational investigative activities, cryptocurrency, cryptocrime, legalization of criminal proceeds, blockchain*

Recommended citation

Vasyukov V. F., Starzhinskaya A. N. Ob operativno-rozysknykh i sledstvennykh merakh protivodeistviya legalizatsii prestupnykh dokhodov s ispol'zovaniem kriptovalyut [On the Operational and Investigative Measures to Counter Money Legalization Using Cryptocurrencies], *Rossiiskoe pravo: obrazovanie, praktika, nauka*, 2024, no. 4, pp. 68–78, DOI: 10.34076/2410-2709-2024-142-4-68-78.

References

Dupuis D., Gleason K. Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic, *Journal of Financial Crime*, 2020, vol. 28, no. 1, pp. 60–74.

Kashirgov A. Kh., Semenov E. A. Nekotorye voprosy protivodeistviya prestupleniyam, sovershennym s ispol'zovaniem IT-tekhnologii [Some Issues of Countering Crimes Committed Using IT Technologies], *Evraziiskii yuridicheskii zhurnal*, 2021, no. 9, pp. 309–310.

Klevtsov K. K., Kvyk A. V. Iz"yatie i osmotr informatsii, nakhodyashcheisya v elektronnoi pamyati abonentskikh ustroistv [Seizure and Inspection of Information Stored in the Electronic Memory of Subscriber Devices], *Zakonnost'*, 2020, no. 12, pp. 56–60.

Klevtsov K. K. Osobennosti vzaimodeistviya pravookhranitel'nykh organov s zarubezhnymi postavshchikami uslug virtual'nykh valyut (na primere localbitcoins) [Features of Interaction of Law Enforcement Agencies with Foreign Providers of Virtual Currency Services (Using Localbitcoins as an Example)], *Vestnik Moskovskogo universiteta MVD Rossii*, 2023, no. 1, pp. 139–145.

Kolycheva A. N. Perspektivy vnedreniya iskusstvennogo intellekta v raskrytie i rassledovanie prestuplenii [Prospects for the Introduction of Artificial Intelligence in the Detection and Investigation of Crimes], *Nauchnyi vestnik Orlovskogo yuridicheskogo instituta MVD Rossii imeni V. V. Luk'yanova*, 2022, no. 3, pp. 172–179.

Morozova N. V. *Nekotorye osobennosti rassledovaniya komp'yuternykh prestuplenii* [Some Features of the Investigation of Computer Crimes], *Sovremennoe ugolovno-protsessual'noe pravo – uroki istorii i problemy dal'neishego reformirovaniya* [Modern Criminal Procedure Law – Lessons of History and Problems of Further Reform]: conference papers, in 2 parts, Orel, ORYuI MVD Rossii im. V. V. Luk'yanova, 2022, pt. 1, pp. 240–245.

Pinkevich T. V. Preduprezhdenie prestuplenii, sovershaemykh v sfere oborota tsifrovoi valyuty (kriptovalyuty) [Prevention of Crimes Committed in the Sphere of Turnover of Digital Currency (Cryptocurrencies)], *Pravovoe gosudarstvo: teoriya i praktika*, 2021, no. 4, pp. 82–96.

Pushkarev V. V., Tokolov A. V. Osnovy organizatsii protivodeistviya prestupleniyam, sovershaemym s ispol'zovaniem kriptovalyut [Fundamentals of the Organization of Countering Crimes Committed Using Cryptocurrencies], *Vestnik ekonomicheskoi bezopasnosti*, 2023, no. 4, pp. 88–92.

Samoilo V. A. *Kharakternye osobennosti prestuplenii, svyazannykh s ispol'zovaniem kriptovalyut* [Characteristic Features of Crimes Related to the Use of Cryptocurrencies], *Prestupnost' v SNG: problemy preduprezhdeniya i raskrytiya prestuplenii* [Crime in the CIS: Problems of Crime Prevention and Disclosure]: conference papers, in 3 parts, Voronezh, 2023, pt. 1, pp. 337–338.

Sil'chenko E. V., Vasil'ev A. M. Kriptovalyuta kak sredstvo obezlichivaniya pri sovershennom ili sovershayushchemsya prestuplenii [Cryptocurrency as a Means of Depersonalization in a Committed or Ongoing Crime], *International Law Journal*, 2023, vol. 6, no. 3, pp. 168–172.

Wang H. M., Hsieh M. L. Cryptocurrency Is New Vogue: A Reflection on Money Laundering Prevention, *Security Journal*, 2024, no. 37, pp. 25–46.

Zaitsev A. A., Sulaeva D. S. Kriptovalyuta kak element kriminalisticheskoi kharakteristiki prestuplenii [Cryptocurrency as an Element of Criminalistic Characteristics of Crimes], *Problemy pravovoi i tekhnicheskoi zashchity informatsii*, 2021, no. 9, pp. 28–32.

Vitaly Vasyukov – doctor of juridical sciences, professor of the Department of criminal law, criminal procedure and criminalistics, Moscow State University of International Relations of the Ministry of Foreign Affairs of Russia (MGIMO). 119454, Russian Federation, Moscow, Vernadsky ave., 76. E-mail: vvf0109@yandex.ru.

ORCID: 0000-0003-0743-5616

Anna Starzhinskaya – candidate of juridical sciences, associate professor of the Department of criminal procedure and criminology, All-Russian State University of Justice (RLA of the Ministry of Justice of Russia). 117638, Russian Federation, Moscow, Azovskaya str., 2. E-mail: starzhinskaya1983@mail.ru.

ORCID: 0009-0008-0435-1023

Дата поступления в редакцию / Received: 01.10.2024

Дата принятия решения об опубликовании / Accepted: 21.10.2024