внимание имеющиеся факты коррупционных проявлений в судебной системе, думается, что это правильное решение;

В-третьих, необходимо создать условия для технического обеспечения судопроизводство. При этом под техническим обеспечением суда следует понимать оснащение залов судебного заседания видеокамерами для трансляции судебного процесса в режиме on-line. Любой гражданин, изучив график судебных разбирательств, выбирает тот или иной процесс и наблюдает его в интернете. Это обеспечит гласность и прозрачность судебного процесса, предупредит нарушение закона со стороны участников процесса и упредит усмотрение суда.

Кроме того, техническая оснащенность суда облегчит возможность обращения граждан в суд (заявления, жалобы) вне зависимости их места жительства по электронной почте. Это ускорит рассмотрение заявлений граждан, принятия решения судом, сократит денежные затраты на транспортные переезды и проживание и т.д. Положительным примером в данном вопросе, на наш взгляд, является создание «электронного правительства».

Таким образом, вышеизложенное позволяет нам сделать следующие выводы.

Необходимо изменить понятие коррупции, расширив круг субъектов данного преступления (включить все физические лица и юридические лица). Для формирования эффективной судебной системы необходимо коренным образом реформировать всю судебную систему.

Библиографический список

1. Борчашвили, И. Ш. Коррупционные преступления: закон, теория и практика: монография / И. Ш. Борчашвили. – Алматы: Жеті Жарғы, 2008. – 396 с.

2. Скаков, А. Б. Противодействие системной коррупции в государственных органах: теоретико-правовые аспекты, научный отчет / А. Б. Скаков, А. М. Жалмагамбетов // Научные труды НИИ КНБ. – Астана. – 2008.

3. Максимов, С. В. Эффективность общего предупреждения преступлений: учеб. пособие / С. В. Максимов. – М., Академия МВД России. 2002.

КРИПТОВАЛЮТА В СЛЕДСТВЕННОЙ ДЕЯТЕЛЬНОСТИ: ОСОБЕННОСТИ ОБНАРУЖЕНИЯ, УСТАНОВЛЕНИЯ ХАРАКТЕРА И ОБСТОЯТЕЛЬСТВ ЕЕ ИСПОЛЬЗОВАНИЯ

Слащинин О. А.

Следственный комитет Республики Беларусь
ул. Фрунзе, 9, 220034, г. Минск, Беларусь, mailtempus@mail.ru

В статье рассматриваются общие положения о функционировании и особенностях технологии блокчейн, ее использовании профессиональной преступностью для осуществления своей деятельности, получения преступного дохода, его сокрытия или легализации. На основе обозначенной проблемы приватности криптовалютных транзакций, имеющих противоправный характер, определены типичные следственные ситуации, возникающие при расследовании уголовных дел, связанных с оборотом криптовалюты. В

зависимости от возникшей следственной ситуации описаны порядок и особенности проведения следственных и других процессуальных действий, направленных на обнаружение органом уголовного преследования криптовалюты, установление характера и обстоятельств ее использования. Детализированы современные методы и приемы установления участников информационной системы обмена виртуальными активами.

Ключевые слова: альткоин; биткоин; блокчейн; криптовалюта; криптокошелек; следственная деятельность; токен

Введение. Популяризация криптографической валюты (далее – криптовалюты) как средства платежа и накопления сформировала новые условия существования профессиональной преступности и происходящие из их деятельности методы получения преступного дохода, его сокрытия или легализации. Криптовалюта – это определенные цифровые знаки (токены), являющиеся единицей учета операции в информационной системе обмена виртуальными активами. В настоящее время наиболее популярной и наибольшей по капитализации криптовалютой является биткоин (от англ. Bitcoin, от bit – бит и coin – монета) [BTC]. Существуют и другие информационные системы со своей криптовалютой: Ethereum [ETH], Ripple [XRP], Bitcoin Cash [BCH], Stellar [XLM], Tether [USDT], Toncoin [TON], Monero [XMR] и иные альткоины. Для функционирования и защиты указанной системы применяется технология блокчейн (англ. blockchain – цепочка из блоков), отдельные особенности которой усложняют процесс установления (деанонимизации) ее пользователей со стороны органов предварительного следствия, а именно:

– распределенный реестр блоков транзакций, препятствующий единоличному внесению в него изменений, в том числе для блокирования отдельных криптовалютных кошельков (далее – криптокошельков), конфискации или ареста конкретных цифровых знаков (токенов);

– децентрализованная (одноранговая) сеть, основанная на равноправии ее участников (узлов), предполагающем относительную невозможность влияния отдельных субъектов на работу всей системы, а также ее принудительного отключения или блокирования сетевого доступа к ней;

– использование криптографических методов защиты информации при генерации открытых и приватных ключей криптокошельков, а также при проверке полномочий участника на совершение действий в системе [1].

Вышеуказанные особенности являются причиной ограниченности перечня идентификаторов, которые могут быть использованы следователем для установления участников «криптовалютных» сетей. Условный перечень может зависеть от используемого блокчейна или клиент-приложения, однако в силу задействования криптографии все возможные идентификаторы будут максимально обезличены их хешированным видом. Если устанавливаемое лицо при взаимодействии с криптовалютой не пользовалось услугами или сторонними клиент-приложениями посредников в виде операторов обмена криптовалют (далее – криптообменников) или криптобирж, то упомянутый перечень сократится до следующих идентификаторов:

– адрес(-а) криптокошелька, представленный в виде комбинации букв и цифр, автоматически вычисляемой хеш-функцией его открытого ключа (например, 34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo);

– хеш транзакции (TxID/TxHash), генерируемый при осуществлении перевода для определения ее текущего статуса в блокчейне (например, d486aeb0e59181fd1addb4aa69ce04d638188fc1125c424899267e8ed6a8af24);

– другие сопутствующие идентификаторы осуществленной транзакции: сумма, дата и время перевода, комиссия (газ) за перевод, количество подтверждений и получателей перевода, высота блока в системе и иные;

– IP-адрес устройства (узла), на котором запускается клиент-приложение для осуществления транзакции. Стоит отметить, что определение указанного идентификатора теоретически возможно при получении контроля над другими узлами сети, к которым устанавливаемое лицо будет подключаться при совершении транзакции [2].

В отдельных следственных ситуациях орган уголовного преследования может не располагать даже ранее упомянутым перечнем идентификаторов. Это связано с тем, что профессиональный преступник для осуществления своей деятельности может использовать «анонимные» блокчейны, применяющие следующие криптографические технологии:

1) сокрытие адреса криптокошелька;

2) кольцевая подпись транзакций;

3) автоматический миксер транзакций;

4) доказательство транзакции с нулевым разглашением.

Несмотря на малое количество доступных для анализа идентификаторов и их хешированный вид, профессиональные преступники, не ограничиваясь уже имеющейся приватностью совершения транзакций, сочетают использование криптовалют с дополнительными элементами конспирации. Так, последними могут применяться (раздельно или в комплексе) следующие методы и инструменты конспирации:

1) шифрование своего сетевого соединения;

2) работа с удаленного рабочего стола или устройства, к которому осуществлен несанкционированный доступ;

3) использование миксеров криптовалют;

4) увеличение цепочек транзакций;

5) перевод криптоактивов на биржевые криптокошельки с их последующим выводом в виде криптовалюты другого вида.

Однако если устанавливаемое лицо взаимодействует с блокчейном посредством ранее указанных криптообменников или криптобирж, то перечень искомых идентификаторов расширяется за счет реквизитов учетных записей, присваиваемых сетевым ресурсом (логин, пароль, сетевое имя, абонентский номер, адрес электронного почтового ящика, IP-адрес и MAC-адрес устройства, User-Agent браузера и веб-приложения, данные KYC и иные).

Порядок и особенности проведения следственных и других процессуальных действий, направленных на обнаружение криптовалюты, установление характера и обстоятельств ее использования (проведения тех или иных транзакций), зави-

сят от складывающихся обстоятельств. Можно выделить следующие типичные следственные ситуации:

1. Установлен факт совершения преступления с использованием криптовалюты либо ее применением для сокрытия или легализации доходов, полученных преступным путем. В том числе обнаружены отдельные идентификаторы проведенной криптовалютной транзакции, относимой к исследуемым обстоятельствам, однако лицо, подозреваемое в совершении описываемых действий, не установлено.

2. Установлено лицо, подозреваемое в совершении или в соучастии в совершении расследуемого преступления(-ий), изъяты его компьютерная техника и другие накопители цифровой информации. В свою очередь, органом уголовного преследования проверяется следственная версия об использовании подозреваемым криптоактивов или предоставлении другим лицам имеющихся у него технических (вычислительных) ресурсов для поддержания работоспособности и функционирования информационной системы.

Следственная ситуация № 1. Для сбора первичной информации об используемой сети, адресах криптокошельков или совершенных транзакциях следователь использует расположенные на сетевых ресурсах обозреватели блоков конкретной сети (например, etherscan.io, litecoinblockexplorer.net) или универсальные обозреватели (например, blockchair.com, blockchain.com) нескольких блокчейнов. Ручной анализ информации, содержащейся в упомянутых обозревателях, позволяет установить:

1) количество всех и детали отдельных транзакций, совершенных с участием конкретного адреса криптокошелька;

2) период времени его использования и оборот всей криптовалюты по исследуемому адресу;

3) ранее взаимодействовавшие с ним адреса других кошельков-контрагентов. Во время всего периода производства предварительного следствия также может осуществляться визуальный или программный мониторинг движения криптовалюты по исследуемым криптокошелькам.

Для проведения автоматического анализа открытых данных блокчейнов следователем могут использоваться свободные и коммерческие программные инструменты (веб-приложения). Среди полезного для расследования функционала можно выделить следующее:

1) визуализация проведенных транзакций (например, Maltego, GraphSense);

2) оценка рисков (скоринг) адреса криптокошелька;

3) кластеризация блокчейна и группировка адресов криптокошельков на основе проведенных транзакций;

4) взаимодействие криптокошельков и отслеживание потока криптовалюты во всем блокчейне (например, Reactor, Crystal Expert).

В свою очередь, предполагается, что следователь в рамках направленного требования может поручить анализ открытых данных блокчейна или получить уже проанализированные данные у органов финансовой разведки (например, ДФМ КГК Республики Беларусь), а также у имеющих регистрацию криптооб-

менников и криптобирж (например, соответствующие резиденты Парка высоких технологий).

Перспективным направлением сбора информации об адресах криптокошельков и проведенных по ним транзакциям может признаваться разведка по открытым источникам (OSINT – от англ. Open Source INTelligence), в том числе ее разведывательные субдисциплины: Интернет-разведка и разведка по утечкам данных. В первом случае, разведывательный поиск предполагает обнаружение упоминаний адреса криптокошелька, хешей транзакций и других сопутствующих идентификаторов блокчейна на различных сетевых ресурсах (веб-сайты и их отдельные веб-страницы, открытые FTP-сервера и иные общедоступные сетевые хранилища (репозитории). Основные инструменты Интернет-разведки, которые могут результативно применяться следователем при установлении указанных упоминаний – это различные поисковые системы (например, Google, Baidu Search, Яндекс) с грамотным использованием операторов расширенного поиска (например, intext:, «», -, AND). Во втором случае, под упомянутыми утечками данных подразумевается ранее скрытое владельцами сетевых ресурсов криптообменников и криптобирж содержимое данных их серверной части, но опубликованное третьими лицами в открытый доступ после совершения последними несанкционированного доступа к указанной серверной части и копирования ее содержимого [3]. Так, упомянутое содержимое может представлять собой идентификаторы зарегистрированных на сетевом ресурсе учетных записей, установленные сеансы авторизации, список проведенных транзакций, реквизиты и балансы криптокошельков, личные сообщения и обращения в службу поддержки, а также иные сведения. Для разведки по утечкам данных следователю необходимо обладать их ранее саккумулированными массивами либо идентифицировать по мере необходимости конкретные утечки на тематических сетевых ресурсах. Осуществление указанных мероприятий возможно в рамках проведения осмотра компьютерной информации, предусмотренного ст. 204-1 Уголовно-процессуального кодекса Республики Беларусь (далее – УПК) [4]. В случае установления движения отслеживаемой криптовалюты по адресам криптокошельков, используемых криптообменниками или криптобиржами, следователь направляет в указанные организации требования о предоставлении информации о совершенной транзакции. При наличии технических возможностей, следует проверить на причастность к исследуемой криптовалютной транзакции абонентов различных Интернет-провайдеров. Для этого необходимо установить устройства абонентов, которые в период времени совершения исследуемой транзакции осуществляли доступ (обращение к доменному имени) к сетевым ресурсам конкретных криптоообменников или криптобирж (например, к доменному имени bynex.io или по сетевому адресу 185.183.121.15:443). Исходя из полученных сведений, следователь проводит другие следственные и процессуальные действия, направленные на установление лиц, причастных к совершению противоправных действий с криптовалютой.

Следственная ситуация № 2. В данном случае не будут рассматриваться обстоятельства обнаружения аппаратного или бумажного криптокошелька, а также записей с мнемонической (seed)-фразой для его восстановления, т.е. очевидного

факта использования подозреваемым криптовалюты. Так, в рассматриваемой ситуации первостепенной задачей будет являться детальное исследование изъятой компьютерной техники и других накопителей цифровой информации, в том числе восстановление удаленных данных. Вышеуказанное исследование подразумевает собой назначение и проведение компьютерной-технической экспертизы (экспертизы радиотехнических устройств) либо самостоятельное проведение осмотра согласно положениям статей 203, 204 и 204-1 УПК Республики Беларусь [4]. Обнаруженная в рамках проведения процессуальных действий компьютерная информация позволит установить факт, характер и обстоятельства использования подозреваемым той или иной криптовалюты.

Первый этап исследования – определение факта установки и использования подозреваемым программных криптокошельков, специальных расширений Интернет-браузеров, программ для майнинга, приложений криптообменников или криптобирж. Для проведения их автоматического или ручного поиска могут составляться:

– словарь (список ключевых слов), состоящий из полных или кратких наименований ярлыков, конфигурационных и исполняемых электронных файлов (далее – файлов) (например, «bitcoin-qt», «electrum», «btcminer», «metamask», «binance»);

– словарь из хеш-сумм вышеуказанных файлов (например, ранее вычисленных и записанных при расследовании схожих уголовных дел) для их идентификации на основании совпадения результатов выполнения хеш-функции по тому или иному алгоритму вычисления (например, MD5, SHA-1).

Обнаружение установленных компонентов ранее определенного программного обеспечения или его остаточных файлов позволит определить факт использования подозреваемым криптовалюты, вид цифровых знаков (токенов) и отдельные обстоятельства их применения.

Второй этап исследования – обнаружение файлов криптокошельков или установленных сеансов авторизации в учетные записи с доступом к указанным кошелькам (субсчетам криптобменников и криптобирж). Настоящий этап необходим для принятия мер по переводу всех криптоактивов подозреваемого на криптокошельки, подконтрольные органу уголовного преследования, или по аресту криптовалюты в порядке ст. 132 УПК Республики Беларусь [4]. Существующие меры направлены на последующее обеспечение возмещения вреда, причиненного преступлением, взыскания дохода, полученного преступным путем, гражданского иска, других имущественных взысканий, а также специальной конфискации. Описанный этап реализуется посредством следующих мероприятий:

– поиск файлов формата «*.dat» с наименованием «wallet*» или иными схожими масками ввода;

– восстановление и поиск раннее удаленных данных с форматированием, присущим файлам криптокошельков;

– поиск зашифрованных файлов криптокошельков или файлов формата «*.dat» посредством измерения информационной энтропии (по К. Шеннону) компьютерной информации, содержащейся на исследуемом накопителе. Как правило, зашифрованные файлы будут иметь максимальные значения уровня

энтропии: в диапазоне от 7 до 8, а другие файлы формата «*.dat» можно идентифицировать по заранее определенным границам типичного диапазона их уровня энтропии [5, с. 32-33];

– поиск мнемонических (seed)-фраз для восстановления доступа к криптокошелькам (от 12 до 24, как правило, английских слов) посредством настройки маски ввода по словарю, состоящему из 2048 возможных английских слов [6]);

– установление сеанса авторизации к программным криптокошелькам, посредством которых возможно осуществить экспорт его приватных ключей и получить прямой доступ к содержащимся в них криптоактивам;

– установление сеанса авторизации к учетным записям сетевых ресурсов или веб-приложений криптообменников и криптобирж;

– установление сеанса авторизации к учетным записям других сетевых ресурсов, с помощью которых возможно восстановить доступ или осуществить аутентификацию к криптокошелькам, а также субсчетам учетных записей сетевых ресурсов криптообменников или криптобирж.

Третий этап исследования – обнаружение иных идентификаторов или реквизитов доступа, необходимых для успешной реализации приемов из второго этапа исследования (при наличии проблем с аутентификацией к учетным записям или криптокошелькам), а также установление другой информации о характере и обстоятельствах использования криптовалюты. Рассматриваемый этап включает в себя следующие мероприятия:

– поиск адресов и приватных ключей криптокошельков в наименовании, содержании и метаданных файлов, сохраненных на накопителе информации, посредством настройки маски ввода по форматам имеющихся адресов (например, Legacy (1*), Script (3*), SegWit (bc1q*), Taproot (bc1p*), EIP55 (0x*) и приватных ключей (например, WIF (5*), сжатый WIF (K*/L*), Hex, Base64). В свою очередь, в указанные объекты поиска входят QR-коды, которые могут отображать адреса и приватные ключи криптокошельков;

– поиск и анализ сообщений переписок, сохраненных на накопителе информации или содержащихся в учетных записях различных сетевых ресурсов (мессенджеров, социальных сетей, почтовых сервисов, форумов и иных). Обнаруженные сообщения анализируются на предмет упоминаний адресов криптокошельков, осуществленных транзакций, реквизитов доступа к учетным записям, субсчетам и криптокошелькам, а также обсуждения преступной деятельности, в том числе характера и обстоятельств использования подозреваемым и (или) его соучастниками криптовалюты;

– поиск и анализ файлов Интернет-браузеров на предмет обнаружения сохраненных паролей и форм автозаполнения в виде реквизитов доступа к учетным записям, а также упоминаний идентификаторов криптокошельков и субсчетов в виде истории посещений и cookies-файлов сетевых ресурсов криптообменников и криптобирж;

– поиск программного обеспечения (приложений) для осуществления двухфакторной аутентификации к учетным записям сетевых ресурсов или веб-приложений криптообменников или криптобирж.

После исследования компьютерной техники и других накопителей цифровой информации следователь может проводить мероприятия, ранее указанные в следственной ситуации № 1, а именно: разведка по открытым источникам (OSINT), в том числе ручной и автоматический анализ открытых данных блокчейнов, разведка по утечкам данных, направление зарегистрированным криптообменникам и криптобиржам требований о предоставлении информации.

Вместе с вышеописанными мероприятиями следователь проводит другие следственные и процессуальные действия, направленные на обнаружение, установление характера и обстоятельств использования подозреваемым и (или) его соучастниками криптовалюты. Так, на основе ранее полученных сведений следователь проводит допросы подозреваемого(-ых) и свидетелей, направляет требования о предоставлении информации, предметов и документов, имеющих значение для уголовного дела, направляет требования о производстве проверок, а также дает поручения органам, осуществляющим дознание, на проведение оперативно-розыскных мероприятий.

Выводы. Приведенные в статье порядок и особенности проведения следственных и других процессуальных действий, направленных на обнаружение криптовалюты, установление характера и обстоятельств ее использования, не являются исчерпывающими и требуют дополнительного исследования. В связи со стремительным развитием информационных технологий, в том числе блокчейна, соответственно, происходит совершенствование методов получения преступного дохода, его сокрытия или легализации. Рассмотренные методы, приемы и инструменты, направленные на установление участников указанных информационных систем и собирание доказательств, нуждаются в дальнейшей разработке и совершенствовании практики их применения. В свою очередь, необходимо формировать новые подходы к решению проблемы приватности криптовалютных транзакций, совершаемых профессиональной преступностью, в том числе:

– глубокий анализ сетевых пакетов (DPI – англ. Deep Packet Inspection) по их содержимому в целях обнаружения и фильтрации Интернет-трафика абонентов локальных и региональных провайдеров, связанного с проведением криптовалютных транзакций или функционированием майнинг-ферм;

– работа органа уголовного преследования с большими данными (англ. Big Data), предполагающая их мониторинг и собирание из различных источников информации, обработку, анализ и последующее использование в следственной деятельности. В указанном случае, применительно к тематике статьи, подразумеваются данные, связанные с блокчейном и проведением криптовалютных транзакций.

Библиографический список

1. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System (2008) / Bitcoin [Электронный ресурс]. – Режим доступа: bitcoin.org/bitcoin.pdf. – Дата доступа: 16.03.2023.

2. Biryukov, A. Deanonymisation of clients in Bitcoin P2P network (Nov-2014) / A. Biryukov, D. Khovratovich, I. Pustogarov // Open Repository and Bibliography of the Uni-

versity of Luxembourg Library [Электронный ресурс]. – Режим доступа: orbilu.uni.lu/handle/10993/18679. – Дата доступа: 18.03.2023.

3. Обменник KeepChange сообщил о взломе, но похищены только данные / Новости журнала «ХАКЕР» [Электронный ресурс]. – Режим доступа: xakep.ru/2021/02/12/keepchange. – Дата доступа: 21.03.2023.

4. Уголовно-процессуальный кодекс Республики Беларусь : по состоянию на 21 сент. 2022 г. – Минск : Нац. центр правовой информ. Респ. Беларусь, 2022. – 536 с.

5. Матвеева, В. С. Энтропия и ее использование для решения задач информационной безопасности / В. С. Матвеева // Безопасность информационных технологий. – Том 21. – № 3. – 2014 [Электронный ресурс]. – Режим доступа: bit.mephi.ru/index.php/bit/article/view/163. – Дата доступа: 22.03.2023.

6. Bitcoin: Bitcoin improvement proposals / GitHub [Электронный ресурс]. – Режим доступа: github.com/bitcoin/bips/blob/master/bip-0039/english.txt. – Дата доступа: 22.03.2023.

НАЗНАЧЕНИЕ И ПРОВЕДЕНИЕ ЭКСПЕРТИЗ ПРИ РАССЛЕДОВАНИИ ХИЩЕНИЙ ПРЕДМЕТОВ ВООРУЖЕНИЯ

Талалаев В. А.

УО «Военная академия Республики Беларусь»,
ул. Уручская, 1а, 220056,Минск, Беларусь, varb@mod.mil.by

Определены основные особенности назначения и проведения экспертиз в ходе раскрытия и расследования хищений предметов вооружения с учетом практики правоохранительных органов Республики Беларусь. Специфика их подготовки и проведения установлена с учетом этапа оборота предметов вооружения и связанными с ним особенностями места, времени, обстановки хищения, ограниченного круга лиц, причастных к обороту вооружения на конкретном этапе. Указан круг отдельных задач расследования рассматриваемых преступлений, которые могут быть успешно решены при помощи современных криминалистических экспертиз. При этом обозначено, что специальные знания, применяемые как в процессуальной, так и непроцессуальной формах, ориентированы на преодоление элементов противодействия расследованию.

Ключевые слова: судебная экспертиза; специальные знания; хищение; огнестрельное оружие; боеприпасы; взрывчатые вещества; предметы вооружения

Изучение оружия – это один из аспектов, рассматриваемых исследователями в контексте исторического развития человеческого общества с точки зрения военных, военно-технических, историко-этнографических, судебно-медицинских, спортивно-технических и иных аспектов. С учетом современных реалий, такая специфическая категория, как предметы вооружения, заслуживает дальнейшего более детального изучения именно с криминалистической точки зрения.

При расследовании преступлений, связанных с хищением оружия, боеприпасов и взрывчатых веществ, криминалистически значимая информация играет особую, а иногда и решающую роль, особенно когда свидетельская база является недостаточной или сознательно искажена. Поэтому можно отметить, что уголов-