ветствующую аппаратуру, а в случае неполадок в ходе дистанционного допроса устраняет их. В СССР существовали диктомашбюро, сотрудники которых фиксировали в протоколах информацию, надиктовываемую им следователем или содержащуюся на диктофоне. В то время данная технология позволила повысить грамотность составления процессуальных документов, а в наши дни могла бы способствовать снижению нагрузки на следователя и повышению эффективности расследования, т.к. лицо, производящее расследование, было бы сосредоточено непосредственно на допросе и допрашиваемом, а стенографист (сотрудник «диктомашбюро») занимался бы фиксацией информации.

Таким образом, тактика производства дистанционных следственных действий нуждается в разработке методических рекомендаций, т.к. существует множество аспектов, о которых необходимо знать следователю (дознавателю). Однако криминалистическое значение технологии ВКС имеет неоценимое влияние на дальнейшее расследование уголовного дела и его рассмотрение в суде.

Литература

1. Уголовно-процессуальный кодекс Республики Беларусь от 16.07.1999 № 295-З (с изм. и доп. по сост. на 26.05.2021). URL: https://online.zakon.kz/Document/?doc_id=30414958&doc_id2=30414958#activate_doc=2&pos=79;-81.19999694824219&pos2=2385;-81.19999694824219.

О.А. Попова, *канд. юрид. наук, доцент*
Волгоградская академия МВД России

Поиск и изъятие криптовалют, используемых в криминальных расчетах, в ходе раскрытия и расследования преступлений

Цифровизация всех сфер общественных отношений изменяет и способы совершения преступлений. Число преступных деяний, совершенных с использованием информационно-телекоммуникационных технологий, с каждым годом неизменно растет, увеличившись за последние пять лет более чем в одиннадцать раз [4].

Согласно данным аналитики Clain Technologies, по итогам 2020 г. Россия является лидером на рынке высокорискованных биржевых площадок, совершающих операции в криптовалютах Ehtereum и Bitcoin, в которых ее доля составляет 41,1%. Зарубежные аналитики небезосновательно полагают, что это может быть связано с популярностью в России запрещенных сервисов, таких как Hidra [5] – нелегальный сегмент интернет-пространства, в котором осуществляется торговля наркотиками, поддельными деньгами, вредоносным софтом и многим другим.

Учитывая сложившуюся ситуацию, следует наращивать усилия государства в противодействии IT-преступлениям и использованию криптовалют в криминальных расчетах. Деятельность правоохранительных органов осложняется отсутствием должного правового регулирования криптовалют, а также неразработанностью механизмов блокирования транзакций и наложения ареста на криптовалюты. Не вдаваясь в обсуждение проблем легализации криптовалют, остановимся на криминалистических аспектах производства отдельных следственных действий, направленных на отыскание и изъятие следов преступлений, связанных с их использованием.

Основным доказательством осуществления криминальных сделок, совершаемых с использованием криптовалюты, является установление цепочки транзакций, при этом «отследить передвижения криптовалюты с одной криптобиржи на другую практически невозможно, поскольку владельцы таких интернет-площадок и криптобирж являются иностранными гражданами, а их серверы находятся за пределами Российской Федерации. При этом исполнение запросов правоохранительных органов Российской Федерации для владельцев таких площадок не является обязательным» [2]. Кроме того, участники преступной деятельности дополнительно используют различные механизмы анонимизации операций с криптовалютами, такие как:

- миксеры криптовалют – специальные сервисы, позволяющие разорвать связь между отправителем и получателем криптовалют,
- анонимные платежные системы (система Z-pay), позволяющие осуществлять платежи и обменивать криптовалюту без верификации,
- перевод более «прозрачных» криптовалют в менее «прозрачные», такие как Dash, Zcash,

Monero, имеющие более высокую степень анонимности за счет встроенных инструментов.

В мире существуют сервисы по анализу операций с криптовалютами Titanium, Elliptic, Ciphertrace, Chainalysis, Crystal, AnChain, Coinfirm. Несмотря на попытки создания действенного российского инструмента по анализу криптовалютных операций («прозрачный блокчейн»), широкого применения в расследовании преступлений он в полной мере еще не получил, поэтому, как это ни печально констатировать, доступ к криптокошельку определенного лица возможен лишь при его содействии или в случае обнаружения у него соответствующих ключей к нему.

Поэтому в ходе следственных следствий, направленных на отыскание и изъятие материальных объектов и цифровых следов (осмотр, обыск, выемка), следует обращать особое внимание на электронные и непосредственные записи, содержащие такие криминалистически значимые сведения, как bitcoin-адреса, записанные на бумажный или электронный носитель ключи. Такой поиск может вестись также и на пользовательских устройствах с целью обнаружения стандартных форматов кошельков, анализа оперативной памяти или выгрузки необходимых сведений с работающего устройства (например, если в момент внезапного начала обыска осуществлялась и не была прервана работа с криптокошельком).

Сведения о криптокошельках могут сохраниться в служебных журналах системных и прикладных программ, программах-кошельках, применяемых для осуществления транзакций, а также файлах wallet.dat.

Важную для расследования информацию можно получить от бирж и обменников, которые взаимодействуют с Пенсионным фондом России либо имеют представительства в Российской Федерации. Они обладают информацией о псевдониме пользователя и его реальных персональных данных (фамилии, имени, отчестве, дате рождения, номере мобильного телефона, E-mail), о переписке с данным пользователем, датах создания аккаунта и последнего входа в него, о принадлежащих данному пользователю криптовалютных адресах, входящих/исходящих операциях, в т.ч. о конвертации криптовалюты в государственно обеспеченные валюты (фиатные средства).

Не менее насущным является вопрос об изъятии криптовалюты в случае ее обнаружения. Среди правоприменителей не существует единого мнения на этот счет. Так, М.М. Догилева полагает, что «единственным способом для правоохранительных органов произвести конфискацию криптовалюты является физическое удержание секретных ключей» [1]. В.А. Перов предлагает два варианта действий: перевод денежных средств на контролируемый следователем криптокошелек либо замена кода доступа, необходимого для авторизации и использования кошелька того лица, на чьи средства накладывается арест [3]. Каждый из вариантов имеет свои недостатки: все они возможны лишь в том случае, когда доступ к кошелькам уже получен и ни один из них не гарантирует сохранность криптовалюты, т.к. в первом случае сведения о ключах, которые представляют собой всего лишь последовательность символов, могли быть известны третьим лицам. Предложение В.А. Перова не выдерживает критики, поскольку возлагает на следователя обязанность хранения объектов нематериального мира, для обращения с которыми ему в соответствии с действующим уголовно-процессуальным законом требуется специалист.

К концу текущего года планируется разработка механизмов наложения ареста на криптовалютные активы, возможно, путем создания государственных криптокошельков. Требуется дальнейшая разработка обеспечения технической возможности и тактики следственных действий, направленных на обнаружение и изъятие криптовалют с учетом международного опыта.

Литература

1. Догилева М.М. Конфискация криптовалюты // Законность. 2018. № 11. С. 45-49.

2. Догилева М.М. Легализация криптовалюты: судебная практика // Законность. 2021. № 3. С. 50-54.

3. Перов В.А. Проблемные вопросы, возникающие при расследовании уголовных дел о преступлениях с использованием криптовалюты // Российский следователь. 2020. № 7. С. 20-22.

4. Состояние преступности в России за январь-декабрь 2020 года и за январь-июль 2021 года // Портал правовой статистики Генеральной прокуратуры РФ. URL: https://crimestat.ru/analytics (дата обращения: 17.09.2021).

5. Near $20B Passed Through High-Risk Exchanges in 2020 // Clain Technologies SA. URL: https://clain.io/blog/post/near-20b-passed-through-high-risk-exchanges-in-2020 (дата обращения: 17.09.2021).