УДК 343.98

Д. И. Шнейдерова
старший преподаватель кафедры уголовного права,
уголовного процесса и криминалистики
Могилевского института МВД Республики Беларусь

АЛГОРИТМ ДЕЙСТВИЙ НА ЭТАПЕ ПРОВЕРКИ ЗАЯВЛЕНИЙ (СООБЩЕНИЙ) ПО ФАКТАМ ХИЩЕНИЙ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

В условиях становления и развития информационного общества качественное состояние преступности за последнее десятилетие претерпело коренные преобразования, что обусловлено востребованностью среди лиц преступной активности инструментов информационно-коммуникационной сферы, повсеместно используемых в механизме совершения различных видов преступлений. Реализуемая в Республике Беларусь с 2018 г. концепция перехода к цифровой экономике содействовала внедрению и распространению среди белорусских граждан новых финансовых инструментов, среди которых отдельное место занимают криптовалюты как легализованное универсальное средство обмена в рамках трансграничного оборота [1, с. 196]. Как справедливо отмечает С. Л. Гамко, популярность криптовалют активизировала как легальную, так и преступную деятельность. Автор приходит к выводу, что, несмотря на законодательное урегулирование оборота криптовалют на территории Республики Беларусь, направленное на защиту общественных отношений в данной сфере, «криптовалюта стала привлекательным объектом преступной деятельности, поскольку находятся и те, кто создает и использует вредоносное программное обеспечение, незаконно завладевает конфиденциальной информацией, используя которую, похищает криптовалюту» [2, с. 87].

Среди видового разнообразия преступлений, совершаемых с использованием криптовалют, отдельную группу составляют хищения, в механизме совершения которых криптовалюты, обладающие имущественной ценностью, выступают и как предмет преступного посягательства, и как средство при посягательстве на денежные средства под предлогом совершения разнообразных сделок с криптовалютой. Поскольку криптовалютная индустрия — достаточно молодая сфера, инструменты которой задействованы сегодня в преступной деятельности, то развитие теоретических взглядов с позиции криминалистической науки на методику расследования хищений в сфере оборота криптовалют находится на этапе своего формирования, и до настоящего момента комплексное исследование обозначенной проблематики в научной литературе отражения не нашло. В этой связи видится актуальной и целесообразной, с точки зрения криминалистического обеспечения процесса расследования хищений в сфере

оборота криптовалют, разработка элементов частной методики расследования указанной группы хищений, одним из которых выступают типичные ситуации отдельных этапов расследования и алгоритмы действий по каждой из них. На основе изложенного целью настоящей статьи является определение алгоритма действий в условиях складывающейся типичной ситуации на этапе проверки заявления (сообщения) по фактам хищений в сфере оборота криптовалют.

Анализ возбужденных на территории Республики Беларусь за период 2018–2023 гг. уголовных дел по фактам хищений в сфере оборота криптовалют (грабежи, вымогательство, мошенничества и хищения путем модификации компьютерной информации) позволил выделить следующие типичные ситуации этапа проверки и алгоритм проверочных мероприятий по каждой из них:

1. Сведения о хищении поступили от лица, которому хищением причинен вред (заявитель), предметом преступного посягательства выступают криптовалюты либо денежные средства в наличной или безналичной форме, способ хищения установлен со слов заявителя, личность преступника не известна, но имеются цифровые следы-идентификаторы, на нее указывающие:

− Получение объяснений заявителя.

− Осмотр устройства заявителя с содержащейся в его памяти цифровой информацией, в т. ч. веб-ресурсов удаленного доступа (в зависимости от способа хищения осмотру подлежат чаты и группы в социальных сетях, мессенджерах, история посещений и закладки браузера, программные или онлайн-криптокошельки, журналы вызовов, журналы программ удаленного доступа, электронная почта, веб-страницы торговых площадок, форумов, фишинговых сайтов, архивы платежей в мобильном или интернет-банкинге, кабинеты криптобирж и обменников, заблокированные программой-вымогателем файлы и т. д.). Если получить доступ к цифровой информации на устройстве заявителя не представляется возможным, то его следует либо изъять в ходе осмотра места происшествия и назначить по нему судебную компьютерно-техническую экспертизу или экспертизу радиоэлектронных устройств для обнаружения, восстановления и копирования проверяемых (искомых) данных для их последующего осмотра, либо провести осмотр устройства и компьютерной информации на месте с участием специалиста и применением аппаратно-программных комплексов, позволяющих в полевых условиях обнаружить и скопировать файлы из памяти устройства либо создать образ.

− Осмотр документов — скриншотов, предоставленных заявителем в ходе объяснений (если есть).

− Направление запроса банку о движении денежных средств по счету заявителя, если предмет преступного посягательства — денежные средства.

− Осмотр кабинета криптокошелька заявителя, если предмет преступного посягательства — криптовалюты (при наличии возможности доступа).

− Получение справочной информации из общедоступных поисковых систем, веб-ресурсов, чат-ботов по выявленным цифровым следам-идентификаторам.

− Направление запросов о предоставлении или оказании содействия в сохранении данных белорусским и зарубежным организациям по выявленным следам-идентификаторам, в т. ч. по линии Национального контактного пункта МВД (далее — НКП) и Интерпола (мобильным операторам, владельцам веб-ресурсов, провайдерам, хостинговым организациям, банкам).

− Проведение оперативно-розыскных мероприятий, направленных на установление личности преступника.

2. Сведения о хищении поступили от лица, которому хищением причинен вред (заявитель), предметом преступного посягательства выступают криптовалюты или денежные средства, способ хищения не установлен, личность преступника не известна, цифровые следы-идентификаторы не установлены (характерна для бесконтактных способов хищения при взломе электронной почты, подборе данных авторизации, удаленном доступе к устройству потерпевшего):

− Получение объяснений заявителя.

− Осмотр устройства заявителя с содержащейся в его памяти цифровой информацией, в т. ч. веб-ресурсов удаленного доступа (осмотру подлежат аккаунт криптокошелька заявителя; привязанная к нему электронная почта, в частности входящие письма и письма, перемещенные в корзину, или спам от криптоплатформы кошелька, сведения об устройствах, с которых осуществлялся доступ к аккаунту почты, если почтовый сервис их предоставляет пользователю в личном кабинете; история посещения веб-сайтов в используемом заявителем браузере на предмет наличия адресов фишинговых сайтов криптоплатформ, банкинга и иных ресурсов, где могли быть введены данные авторизации; архив загрузок браузера на предмет скачивания и установки на устройство заявителя вирусных программ-шпионов; менеджер программ и компонентов устройства заявителя; кабинет мобильного или интернет-банкинга).

− Получение справочной информации из общедоступных поисковых систем, веб-ресурсов, чат-ботов по выявленным цифровым следам-идентификаторам.

− Направление запросов о предоставлении или оказании содействия в сохранении данных белорусским и зарубежным организациям, в т. ч. по линии НКП и Интерпола, а именно почтовым сервисам (восстановление удаленных писем, получение сведений об устройствах, с которых осуществлялся доступ к аккаунту почты за интересуемый период), криптоплатформам (сведения об устройствах, осуществлявших доступ к кабинету криптокошелька заявителя, а также сведения о владельце криптокошелька заявителя), банкам (о движении денежных средств по счету заявителя), хостинговым провайдерам (получение

сведений о лицах, разместивших на их серверах фишинговые веб-сайты), провайдерам сети Интернет и мобильным операторам (получение сведений о движении сетевого трафика с устройства заявителя).

− Проведение оперативно-розыскных мероприятий, направленных на установление личности преступника.

3. Сведения о хищении поступили от лица, которому хищением причинен вред (заявитель), предметом преступного посягательства выступают денежные средства (реже криптовалюты), способ хищения установлен, личность преступника установлена со слов заявителя или очевидцев (характерна для грабежа, контактного мошенничества или хищения путем модификации, если имела место личная встреча с преступником):

− Получение объяснений заявителя.

− Осмотр места происшествия (места совершения грабежа, передачи наличных денежных средств при мошенничестве, получения непосредственного личного доступа к устройству заявителя при хищении путем модификации) с целью обнаружения, фиксации и изъятия материальных следов в обстановке места преступления, записей с камер видеонаблюдения или автомобильных регистраторов, установления очевидцев, а также лиц, имевших доступ к месту нахождения устройства заявителя.

− Получение объяснений очевидцев (при наличии).

− Осмотр устройства заявителя с содержащейся в его памяти цифровой информацией, в т. ч. веб-ресурсов удаленного доступа с целью выявления способа контакта между заявителем и преступником (чаты и группы в социальных сетях, мессенджерах, форумах, торговых площадках, журналы вызовов), либо установления неправомерной транзакции и подтверждения принадлежности криптокошелька заявителю (осмотр кабинета криптокошелька, архива транзакций).

− Осмотр документов — скриншотов, предоставленных заявителем в ходе объяснений (если есть).

− Направление запроса мобильному оператору, если установлен абонентский номер, использованный преступником.

− Получение справочной информации по криминалистическим и оперативным учетам о личности преступника.

− Задержание в порядке ст. 108 Уголовно-процессуального кодекса Республики Беларусь и личный обыск предполагаемого преступника.

4. Сведения о хищении поступили от должностного лица организации, хищение направлено на причинение вреда юридическому лицу — гражданскому истцу, предметом преступного посягательства выступают криптовалюты, причинен имущественный вред (либо вред не причинен по независящим от преступника причинам), способ установлен со слов заявителя, личность

преступника не известна (характерна для вымогательства в отношении юридического лица):

− Получение объяснений должностного лица организации о событии преступления.

− Осмотр устройства организации с содержащейся в его памяти цифровой информацией, в т. ч. веб-ресурсов удаленного доступа (в зависимости от способа вымогательства осмотру подлежат файлы и программы, установленные на устройстве, история загрузок браузера, веб-сайт, с которого осуществлено скачивание вирусной программы, и/или аккаунт электронной почты, на который поступило письмо с требованием о выкупе); при невозможности осмотра устройства и цифровой информации по месту его нахождения (например, при повреждении файлов программой-вымогателем), целесообразно провести осмотр места происшествия с изъятием устройства для назначения судебной компьютерно-технической экспертизы.

− Если сообщение о выкупе поступило по электронной почте и/или программа-вымогатель скачана из вложения в электронное письмо — направить запрос по линии НКП почтовому сервису с целью оказания содействия в предоставлении или сохранении сведений об IP-адресе устройства преступника, с которого отправлено сообщение, либо хостинг-провайдеру с целью получения сведений о владельце сайта, на котором размещен установочный файл вирусной программы.

− Если требование вымогателя реализовано — направить запрос банку о движении денежных средств по счету организации или физического лица (должностного лица), выполнившего требование.

− Получение справочной информации из общедоступных поисковых систем, веб-ресурсов, чат-ботов по выявленным цифровым следам-идентификаторам.

− Проведение оперативно-розыскных мероприятий, направленных на установление личности преступника.

5. Сведения о хищении поступили от должностного лица организации, хищение направлено на причинение вреда физическому лицу (гражданину), предметом преступного посягательства выступают криптовалюты и/или денежные средства, личность физического лица, которому хищением причинен вред, установлена по информации заявителя, способ хищения не известен, личность преступника не установлена (характерна для хищений путем несанкционированного доступа к криптокошелькам биржи посредством подбора данных авторизации):

− Получение объяснений должностного лица организации о событии преступления, личных данных физических лиц, которым хищением причинен вред.

− Осмотр устройства организации с содержащейся в его памяти цифровой информацией (как правило, серверы организации) с целью установления криптокошельков, к которым осуществлен несанкционированный доступ для списания средств, а также их владельцев, сведений об устройствах, с которых преступником реализован несанкционированный доступ.

− Проведение оперативно-розыскных мероприятий, направленных на установление личности и местонахождения физических лиц, которым хищением причинен вред.

− Получение объяснений физических лиц, которым хищением причинен вред.

− Осмотр устройства физического лица, которому хищением причинен вред, с содержащейся в его памяти цифровой информацией, в т. ч. веб-ресурсов удаленного доступа с целью определения вероятного способа получения данных авторизации криптокошелька (осмотру подлежат кабинет электронной почты, история посещений веб-ресурсов браузера, программы, установленные на устройстве физического лица).

− Направление запросов о предоставлении или оказании содействия в сохранении данных белорусским и зарубежным организациям, в т. ч. по линии НКП и Интерпола, а именно провайдерам сети, за которыми зарегистрированы проверяемые IP-адреса предполагаемых преступников; почтовым сервисам для установления сведений об устройствах, получивших несанкционированный доступ к электронной почте физического лица, которому хищением причинен вред; хостинг-провайдерам, на серверах которых размещены фишинговые сайты.

− Проведение оперативно-розыскных мероприятий, направленных на установление личности преступника.

− Получение справочной информации из общедоступных поисковых систем, веб-ресурсов, чат-ботов по выявленным цифровым следам-идентификаторам.

Таким образом, комплекс проверочных мероприятий, предложенных в рамках настоящей статьи, на основе поступившей от заявителя исходной информации о событии преступления, проводимых в условиях обозначенных типичных ситуаций этапа проверки по фактам хищений в сфере оборота криптовалют, способствует установлению обстоятельств, указывающих на признаки состава хищения, способа его совершения, предмета преступного посягательства, сведений о лице, которому хищением причинен вред, вида и размера вреда, источников иной информации, способной подтвердить показания заявителя, что в целом способствует принятию решения о возбуждении уголовного дела.

1. Дедковский А. А., Бушкевич Н. С. Уголовно-процессуальное регулирование криптовалюты: законодательное решение актуальных прикладных проблем // Актуальные проблемы гражданского права. 2019. № 1 (13). С. 195–204. Вернуться к статье

2. Гамко С. Л. Разоблачение преступной схемы хищения криптовалюты // Предварительное расследование. 2019. № 2 (6). С. 87–90. Вернуться к статье