№ 27895 // Полное собрание законов Российской империи. Собрание 1 : в 45 т. — СПб., 1830. — Т. 36 : 1819. — С. 306–314.

5. К новому закону о дисциплинарной ответственности содержащихся в тюрьмах и исправительных арестантских отделениях и о предупреждении побега арестантов // Тюрем. вестн. — 1901. — № 5. — С. 220–233.

6. О занятии арестантов работами и о распределении получаемых от сего доходов : мнение Гос. совета, 6 янв. 1886 г., № 5447 // Полное собрание законов Российской империи. Собрание 3 : в 33 т. — СПб., 1888. — Т. 6, отд. 1. — С. 8–11.

7. Свод законов Российской империи, повелением Государя Императора Николая Первого составленный, изд. 1903 г. : в 15 т. — СПб. : Гос. тип., 1903. — Т. 14 : Уставы благочиния. — 1356 с.

8. Об изменении постановлений о дисциплинарной ответственности содержащихся под стражей в тюрьмах и исправительных арестантских отделениях и о предупреждении побега арестантов : мнение Гос. совета, 23 мая 1901 г., № 20121 // Полное собрание законов Российской империи. Собрание 3 : в 33 т. — СПб., 1903. — Т. 21, отд. 1. — С. 380–381.

9. Общая тюремная инструкция. — Петроград : Тип. Петроград. тюрьмы, 1916. — 110 с.

УДК 343.98

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

ПРОБЛЕМНЫЕ ВОПРОСЫ ОПРЕДЕЛЕНИЯ РАЗМЕРА ВРЕДА, ПРИЧИНЕННОГО ХИЩЕНИЕМ КРИПТОВАЛЮТ: КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ

PROBLEMATIC ISSUES IN DETERMINING THE EXTENT OF HARM CAUSED BY THE THEFT OF CRYPTOCURRENCIES: THE CRIMINALISTIC ASPECT

Аннотация. *Статья посвящена анализу проблем общего и частного характера, возникающих при определении суммы материального вреда, причиненного потерпевшему в результате хищения криптовалют. Автором выделяется проблема установления курса криптовалют в пересчете на белорусские рубли*

в условиях отсутствия общеустановленного алгоритма конвертации и проблема установления размера вреда при отсутствии необходимой криминалистически значимой информации о неправомерной транзакции, предлагаются пути их решения.

Ключевые слова: *криптовалюта, конвертация, размер вреда, курс, криптокошелек, хищение.*

Annotation. *The article analyzes the problems of general and specific nature that arise when determining the amount of material damage caused to the victim as a result of theft of cryptocurrencies. The author singles out the problem of determining the exchange rate of cryptocurrencies converted into Belarusian rubles in the absence of a generally accepted conversion algorithm and the problem of determining the amount of damage in the absence of criminalistically significant information about the unlawful transaction and suggests ways to solve them.*

Keywords: *cryptocurrency, conversion, amount of harm, exchange rate, cryptocurrency wallet, theft.*

Одним из элементов частной криминалистической методики расследования отдельного вида или группы преступлений выступает совокупность обстоятельств, подлежащих установлению и доказыванию по делу. Такая совокупность формируется из обстоятельств как общего характера, предусмотренных уголовно-процессуальным законом для всех категорий преступлений, так и частного, выделяющихся криминалистической наукой за счет специфики конкретной группы преступлений. Применительно к хищениям в сфере оборота криптовалют следует отметить, что данную группу составляют такие преступления как хищения путем модификации компьютерной информации, мошенничество, вымогательство и в единичных случаях грабеж. Несмотря на то, что методики расследования указанных преступлений криминалистикой сформированы и успешно апробируются, правоохранительная практика и современное состояние преступности вносят свои коррективы, выявляя ранее неизвестные проблемы, требующие научного подхода к разрешению. Одной из таких проблем, возникающих при расследовании хищений в сфере оборота криптовалют, является определение размера причиненного преступлением вреда как обстоятельства, подлежащего доказыванию. Установление размера вреда, выраженного в противоправной утрате потерпевшим денежных средств, затраченных под предлогом приобретения криптовалют (выступают как средство хищения), трудностей не вызывает. Алгоритм в данном случае предполагает определение валюты и суммы похищенных средств, если валюта иностранная — ее конвертацию в белорусские рубли по курсу Национального банка Республики

Беларусь (далее — НБ) на день совершения хищения. Размер похищенных средств, заявленный потерпевшим, подтверждается в ходе осмотра выписки о движении денежных средств по счету, предоставленной либо банком, обслуживающим счет потерпевшего, по санкционированному прокурором запросу, либо самим потерпевшим, получившим такую выписку в банке самостоятельно. Также осмотру может быть подвергнут архив платежей и переводов, зафиксированный в личном кабинете мобильного или интернет-банкинга потерпевшего.

Иначе ситуация складывается при необходимости определения размера вреда в пересчете на национальную валюту, если хищению подверглись криптовалюты. Можно выделить проблему общего характера, присущую всем уголовным делам, возбужденным по фактам хищения криптовалют, а также частного, вытекающую из особенностей складывающейся следственной ситуации при хищении криптовалюты путем модификации компьютерной информации.

Основной и актуальной проблемой общего характера в правоприменительной практике выступает отсутствие надлежащего общеустановленного алгоритма конвертации суммы похищенной криптовалюты на белорусские рубли. Анализ изучения уголовных дел, возбужденных по фактам хищения криптовалют и находящихся в производстве подразделений Следственного комитета Республики Беларусь, показал, что среди следователей выработались две методики определения курса криптовалют в пересчете на белорусские рубли:

1) установление курса криптовалюты по отношению к доллару США через любую общедоступную криптобиржу, обменник или аналитические сайты, отслеживающие курсы криптовалют на различных биржах и определяющие средневзвешенное значение (например, обменник Bitok, аналитический сайт CoinMarketCap) — 40 %;

2) установление курса криптовалюты по отношению к доллару США через показатели конвертации, предусмотренные встроенным в криптокошелек потерпевшего обменником — 60 %.

Далее полученная долларовая сумма конвертируется на белорусские рубли по курсу НБ. Разобщенность подходов приводит к дифференциации счетного показателя, влияющего на общий размер причиненного материального вреда: стоимость единицы некоторого вида криптовалюты на определенную дату по одному уголовному делу будет отличаться от стоимости такой же единицы при аналогичных условиях по другому уголовному делу, если применялись разные подходы установления ее курса. Данная проблема носит не только криминалистический, но и тесно

связанный с ним уголовно-правовой характер, поскольку даже небольшая разница в итоговой сумме размера похищенного может повлиять на квалификацию преступного деяния по признаку размера ущерба.

В целях разрешения возникшей проблемы представляется целесообразным, по принципу алгоритма установления курса иностранной валюты к белорусскому рублю через НБ как общее связующее звено получения информации, заключить многостороннее соглашение между Следственным комитетом, Министерством внутренних дел, Комитетом государственной безопасности с одной стороны, и оператором криптоплатформы — резидентом Парка высоких технологий (далее — ПВТ) с другой стороны, о сотрудничестве в области оперативного получения справочной информации о курсах различных криптовалют к доллару США с пересчетом на белорусские рубли по курсу НБ. В качестве резидента ПВТ — оператора криптоплатформы может выступать биржа либо обменник. Например, по результатам изучения уголовных дел отмечается неоднократное взаимодействие органов предварительного расследования с белорусской криптовалютной биржей Currency.com (ЗАО «Дзеньги Ком»), которая может выступать в качестве перспективной стороны по данному соглашению [1]. Также следует отметить, что по результатам анкетирования, проведенного среди следователей подразделений Следственного комитета Республики Беларусь, специализирующихся на расследовании киберпреступлений, 73,6 % респондентов посчитали целесообразным предложение устанавливать курс криптовалют через операторов криптоплатформ — резидентов ПВТ (из них 31,8 % — через любого резидента, 41,8 % — через резидента, с которым заключено соглашение о сотрудничестве), что подтверждает практическую ориентированность и значимость предложенного решения.

Проблема частного характера возникает в случае, если установление суммы похищенных криптовалют затруднительно в связи отсутствием у потерпевшего доступа к криптокошельку и сведений о неправомерной транзакции. Следственная ситуация может складываться следующим образом: потерпевший, имея намерение заработать на криптовалюте при отсутствии должных знаний и опыта, воспользовался в этих целях услугами куратора-преступника, который зарегистрировал для него криптовалютный кошелек и оказывал сопровождение всех операций по пополнению счета. При этом доступ к кошельку имел как сам потерпевший, так и его куратор (оба обладали ID кошелька и паролем). Спустя определенное время потерпевший получил уведомление об успешно проведенной транзакции без детализации по его кошельку на электронную почту (такая функция характерна для большинства криптоплатформ).

Намереваясь проверить достоверность данной информации, последний осуществил попытку доступа к своему кошельку, однако авторизация была неуспешной ввиду несоответствия пароля, который был изменен преступником.

Для того чтобы, исходя из изложенных обстоятельств, определить хеш неправомерной транзакции и, соответственно, сумму криптовалютного перевода, потерпевшему необходимо обладать сведениями либо о хотя бы одном из привязанных к кошельку публичных адресов, либо о любом хеше транзакции, ранее проводимой по данному кошельку (и адрес, и хеш можно проверить через обозреватель для установления всех транзакций по данному кошельку, например, через Wallet Explorer), либо seed-фразой для восстановления доступа. Однако, как показывает практика, потерпевшие могут такими данными не обладать по ряду причин: публичные адреса генерируются кошельком и не один раз, трудны для визуального запоминания и фиксации не требуют, так как хранятся в кошельке; хеш не запоминается по тем же причинам; seed-фраза может быть вообще неизвестна потерпевшему, поскольку она вводится при регистрации кошелька, которая производилась преступником. Таким образом, единственно доступной является информация об ID кошелька, проанализировать которую через общедоступные сервисы не представляется возможным (это лишь имя кошелька, предназначенное для идентификации пользователя на платформе), а также сведения о движении денежных средств по банковскому счету потерпевшего, свидетельствующие о переводах.

В этом случае альтернативным способом определения размера похищенных криптовалют в переводе на национальную валюту можно было бы считать общую сумму денежных переводов, реализованных потерпевшим на криптокошелек. Однако данный метод встречается с двумя проблемами: первая — следователь не может достоверно знать, вся ли сумма реализована с кошелька потерпевшего на кошелек преступника (что может оказать влияние на квалификацию), вторая — высокая волатильность криптовалют, предопределяющая их стоимость в конкретный период времени (т. е. для покупки криптовалюты потерпевший потратил одну сумму, а на момент хищения ее общая стоимость изменилась в большую или меньшую сторону). Следовательно, такой способ не пригоден для целей предварительного расследования.

В связи с этим применимыми для установления реального размера вреда видятся два способа: запросно-справочный и эмпирико-криминалистический. При использовании запросно-справочного метода следователю необходимо проанализировать движение денежных средств

по банковскому счету потерпевшего и установить реквизиты стороны, которой осуществлялись переводы для покупки криптовалюты. Следственная ситуация в этом случае может иметь несколько вариантов: могут быть установлены либо реквизиты банковской карты преступника, который самостоятельно переводил деньги на криптокошелек для покупки криптовалюты, либо реквизиты платежной системы, в чей адрес направлялся перевод, в том числе идентификационный номер кошелька. По полученным реквизитам направить запрос (в подавляющем большинстве случаев — международный) банку-эмитенту преступника или платежной системе (бирже, обменнику, платформе криптокошелька) об установлении владельца счета, либо владельца кошелька и перечне проведенных по нему транзакций с соответствующей детализацией. Вместе с тем, имея сведения о платформе кошелька и его ID, направить запрос в адрес данной платформы для установления владельца кошелька и проведенных по нему транзакций за определенный период (на случай, если кошелек, использованный потерпевшим, отличен от кошелька, на который переводились деньги для приобретения криптовалюты, т. е. может иметь место цепочка переводов для сокрытия преступником цифровых следов). Данный способ времязатратный и не во всех случаях эффективный, поскольку практика международного взаимодействия свидетельствует о частой отрицательности дачи ответов на указанные запросы.

Практико-ориентированным видится эмпирико-криминалистический способ, заключающийся в установлении курса покупки криптовалюты на каждый отдельный перевод в установленные движением средств по счету даты через общедоступные сервисы. При данном способе следует учитывать, через какую криптоплатформу приобреталась криптовалюта, поскольку имеет место курсовая разница, а также размер комиссии за перевод. Определить курс можно как путем анализа доступной информации на криптоплатформе, так и посредством регистрации экспериментального аккаунта на криптоплатформе, если в общем доступе искомые сведения отсутствуют (как правило, все криптокошельки с встроенными обменниками содержат графики с курсом криптовалют за длительный период времени). Установив курс на дату каждого перевода, необходимо подсчитать общее количество приобретенной криптовалюты за средства потерпевшего с вычетом комиссии за перевод (размер указывается правилами платформы), далее — конвертировать полученную сумму в доллары по курсу, установленному на день хищения, итоговую сумму — в белорусские рубли. Описанный способ позволит установить размер причиненного вреда с условием, что преступником выведены все

криптосредства с кошелька (в последующем, если иными путями представится возможным определить точные данные неправомерной транзакции, размер вреда подлежит корректировке в меньшую сторону, при необходимости, с переквалификацией деяния).

Таким образом, резюмируя изложенное, можно прийти к следующим выводам:

1. В целях установления общего алгоритма определения размера вреда, причиненного хищением криптовалют, пригодного для использования правоохранительными органами при расследовании данной группы преступлений, целесообразно заключить соглашение между представителями правоохранительных структур и оператором криптоплатформы — резидентом ПВТ о предоставлении справочной информации по курсам криптовалют на запрашиваемые даты. Видится, что предложенная мера позволит избежать разрозненности по однотипным уголовным делам в итоговых размерах ущерба, причиненного хищением криптовалют, а также исключить ошибки в квалификации преступного деяния. Кроме того, налаженное взаимодействие в условиях оперативности позволит сэкономить процессуально необходимое время, затрачиваемое на самостоятельный поиск достоверной информации.

2. При невозможности установления деталей противоправной транзакции, ввиду отсутствия сведений о ее хеше, адресе криптокошелька потерпевшего или доступа к нему, для установления размера причиненного хищением криптовалют вреда следует прибегнуть к предложенным и описанным выше запросно-справочному и/или эмпирико-криминалистическому способам определения суммы криптовалют, на которые посягал или имел возможность посягать преступник. Установленная информация позволит дать соответствующую криминалистическую и уголовно-правовую оценку совершенному хищению в целях определения путей дальнейшего расследования (в частности, стоимостный размер вреда может повлиять на возможность международного взаимодействия, поскольку отдельные государства предоставляют информацию при наличии минимально установленной суммы ущерба).

Список основных источников

1. Дзеньги Ком [Электронный ресурс] // Парк высоких технологий. — Режим доступа: https://www.park.by/residents/dzengi-com/. — Дата доступа: 27.05.2023.