ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ ПО МАТЕРИАЛАМ ПРОВЕРКИ И УГОЛОВНЫМ ДЕЛАМ О ХИЩЕНИЯХ В СФЕРЕ ОБОРОТА КРИПТОВАЛЮТ

Шнейдерова Д. И.

УО «Могилевский институт МВД Республики Беларусь»
ул. Крупской, 67, 212011, г. Могилев, Беларусь, shneidmimvd@mail.ru

Статья посвящена определению типичных следственных ситуаций, складывающихся на различных этапах досудебного производства по делам о хищениях в сфере оборота криптовалют, представленных вымогательством, мошенничеством и хищением путем модификации компьютерной информации. Обозначается актуальность применения ситуационного подхода при формировании частной методики расследования указанной группы хищений, который позволяет учесть специфику предмета преступного посягательства и алгоритмизировать процесс расследования за счет выборки необходимых проверочных, следственных и процессуальных действий, направленных на получение доказательственной информации. По результатам проведенного исследования автор приходит к выводу, что доследственный этап в белорусской правоохранительной практике характеризуется наличием одной следственной ситуации, которая заключается в поступлении заявления о хищении от потерпевшего, сведений из которого недостаточно для принятия решения о возбуждении уголовного дела, и необходим комплекс проверочных мероприятий, состав которого зависит от вида и предмета хищения. Следственные ситуации первоначального этапа складываются исходя из объема информации, полученной в рамках проверки, и характеризуются наличием признаков одного из состава хищений, установлением данных, указывающих на преступника, или их отсутствием. Последующий этап направлен на подтверждение причастности подозреваемого к хищению, предъявление ему обвинения и закрепление полученных сведений отдельными следственными действиями. Характеризуется наличием одной из следственных ситуаций, которые выделяются в зависимости от признания обвиняемым своей вины.

Ключевые слова: ситуационный подход; хищение; оборот криптовалют; следственная ситуация; следственные действия

Для криминалистической науки криптовалюта как самостоятельный объект – явление новое и, с точки зрения теории, малоизученное, поскольку стало вызывать научный интерес лишь с момента регистрации в 2018 г. первых преступлений, в механизме которых выступала либо как предмет, либо как средство преступного посягательства. Указанное обстоятельство, а также специфика криптовалют и нетривиальность способов их хищения, свидетельствуют об актуальности и практической целесообразности формирования частной криминалистической методики расследования хищений в сфере оборота криптовалют, структурным компонентом которой выступают типичные следственные ситуации.

Следственные ситуации являются категорией, вытекающей из сформированного и апробированного в криминалистике ситуационного подхода, исследование которого нашло отражение в работах Т.С. Волчецкой, Л.Я. Драпкина, Р.С. Белкина, Г.А. Зорина, В.К. Гавло, Е.Р. Россинской, И.М. Лузгина, В.Б. Шабанова, А.М. Хлуса, В.Л. Григоровича, Г.А. Шумака, С.А. Куемжиевой, Н.Н. Бе-

ломытцева, Н.И. Малыхиной, С.В. Кузьминой и иных авторов, каждый из которых представляет свою точку зрения относительно содержания понятия следственной ситуации, что породило плюрализм мнений и отсутствие общепринятой формулировки. Обобщая их взгляды, можно отметить, что следственная ситуация складывается из совокупности условий, в которых проводится расследование на определенный момент времени, формируемых под воздействием ряда факторов информационного, материально-технического, субъективного и иного характера, т.е. с одной стороны следственная ситуация характеризуется массивом имеющейся в распоряжении следствия доказательственной информации, а с другой – условиями самого процесса расследования, которые зависят от лица, его производящего, обеспечения его деятельности и иных участников процесса.

В то же время, указанные авторы сходятся во мнении относительно значимости выделения следственных ситуаций, в том числе применительно к частным методикам, для которых характерно формирование типичных следственных ситуаций и алгоритмов расследования исходя из содержания последних. Определение следственной ситуации оказывает непосредственное влияние на формирование версий совершенного преступления, подлежащих последующей проверке, а также на планирование и организацию процесса расследования. Следует согласиться с точкой зрения Н.Н. Беломытцева, который утверждает, что применение ситуационного подхода в криминалистике «дает возможность алгоритмизировать процесс расследования уголовных дел; разрабатывать и вводить в следственную практику современные методы и средства, позволяющие уменьшить количество процессуальных и тактических ошибок; производить исследования обстоятельств дела в полном объеме, всесторонне и объективно; оптимизировать образовательный процесс» [1, с. 42].

Необходимо отметить, что отдельным частным криминалистическим методикам свойственно разделение типичных следственных ситуаций в зависимости от этапа расследования на ситуации, возникающие при проверке заявления (сообщения) о совершенном преступлении, ситуации первоначального и последующего этапов расследования. Такое же деление применимо и по отношению к хищениям в сфере оборота криптовалют. На этапе проверки следственные ситуации выделяются благодаря такому критерию, как источник получения первичных сведений о факте совершенного хищения, который одновременно является поводом для возбуждения в последующем уголовного дела. Российские исследователи Н.И. Малыхина и С.В. Кузьмина, рассматривая типовые ситуаций расследования мошенничеств, совершенных с использованием сети Интернет (входят в группу хищений в сфере оборота криптовалют), приходят к выводу, что на этапе проверки по данной категории дел может возникать две следственные ситуации: первая – сведения о совершенном мошенничестве поступили от потерпевшего, и их совокупности недостаточно для принятия решения о возбуждении уголовного дела; вторая – факт мошенничества выявлен органами дознания или следствия при проведении оперативно-розыскных действий или расследовании иных уголовных дел, и таких сведений достаточно для возбуждения дела без дополнительных проверочных мероприятий, личность подозреваемого установлена [2, с. 239-240]. Анализ уголовных дел, возбужденных по фактам хищений в сфе-

ре оборота криптовалют, показал, что на сегодняшний день в Республике Беларусь поводом для возбуждения дел данной категории выступают только заявления потерпевших. Указанное обстоятельство свидетельствует о том, что для белорусской практики характерна лишь первая следственная ситуация, которую и целесообразно рассмотреть в данной статье, при этом появление второй также не исключается в перспективе.

Поскольку заявление само по себе уже является поводом для принятия решения о возбуждении уголовного дела, то все проверочные мероприятия направлены на выявление достаточных для этого оснований. Для хищений в сфере оборота криптовалют характерен устоявшийся комплекс первичных мероприятий, который включает получение объяснений от заявителя (потерпевшего), проведение осмотров, направление запросов. Объяснения – отправная точка проверки и в то же время ключевой источник информации о совершенном преступлении. Из содержания объяснений устанавливается предмет преступного посягательства, общие сведения о способе хищения и задействованных при этом технических и программных средствах, характер и объем наступивших последствий. Кроме того, данные, полученные от заявителя, позволяют наметить объекты последующих осмотров, а также сведения, которые требуют проверки и подтверждения посредством направления различным организациям запросов.

Так как хищения в сфере оборота криптовалют образуются из различных составов, которые по характеру своей объективной стороны могут быть материальными и формальными, то и объем устанавливаемых данных будет также разниться. Для подтверждения вымогательства криптовалют достаточно установить факт предъявления потерпевшему требований о выкупе, подкрепляемых определенной угрозой, исполнение которой должно иметь явный характер для потерпевшего. В этих целях после получения объяснений следователю (лицу, производящему дознание) необходимо провести осмотр источника, из которого потерпевшему стало известно о заявленных преступником требованиях. Таким источником, как правило, является либо письмо, полученное по электронной почте, либо текстовый файл, автоматически запускаемый при намерении пользователя открыть файлы на своем устройстве (последствия вирусной программы). В первой ситуации лицо, осуществляющее проверку, может провести либо осмотр компьютерной информации – электронного письма – со своего компьютера, при наличии технической возможности и доступа в сеть Интернет, либо осмотр предмета и компьютерной информации, если он будет проводиться с устройства потерпевшего. В случае с текстовыми файлами имеется неразрывная связь с устройством потерпевшего, поэтому необходимо прибегнуть к осмотру устройства и компьютерной информации. При этом такой осмотр нацелен на подтверждение факта наличия требования о выкупе в криптовалютах и не ставит перед собой задач выяснения вида вирусной программы и способа ее проникновения на устройство потерпевшего (данные обстоятельства должны устанавливаться в рамках компьютерно-технической экспертизы, которая может быть назначена уже на первоначальном этапе расследования). Исходя из изложенного, для принятия решения по заявлению о вымогательстве криптовалют видится достаточным получение объяснений и их подтверждения проведенным осмотром.

В случаях, когда из заявления потерпевшего усматриваются признаки мошенничества или хищения путем модификации, то установление из объяснений и результатов осмотра устройств и компьютерной информации обстоятельств преступного механизма недостаточно для принятия решения о возбуждении дела. Необходимо подтверждение факта выбытия средств из распоряжения потерпевшего. Если предметом хищения являлись безналичные денежные средства, то лицу, проводящему проверку, необходимо направить санкционированный запрос банку, в котором у потерпевшего открыт счет, с целью получения сведений о движении средств по счету за интересующий период, которые в последующем подлежат осмотру. Также перевод на карту, электронный или криптокошелек может быть дополнительно подтвержден осмотром архива платежей и переводов в личном кабинете Интернет– или мобильного банкинга, если таковые используются потерпевшим. Если предметом хищения выступали наличные денежные средства, то необходимо провести осмотр места происшествия, которым является непосредственное место их передачи преступнику или его посреднику, с целью установления камер видеонаблюдения и осмотра записей с них, возможно изъятие материальных следов (следы транспортного средства преступника, пальцев рук и т.д.). В ходе осмотра места происшествия или со слов потерпевшего могут быть также установлены и опрошены очевидцы, способные подтвердить передачу средств. Важным является комплекс оперативно-розыскных мероприятий, направленных на установление личности преступника и его задержание, отправные сведения для поиска которого могут быть получены как по результатам выше указанных проверочных действий, так и осмотра чатов социальных сетей и мессенджеров с перепиской между преступником и потерпевшим, голосовых сообщений (к примеру, могут быть получены данные об имени и фамилии, номере мобильного телефона, реквизитах банковской карты). В белорусской правоохранительной практике имеют место немногочисленные случаи, когда потерпевший и преступник знакомы между собой, в этой связи контактные данные о последнем могут быть получены непосредственно от заявителя и задержание проводится в кратчайшие сроки.

Иным образом обстоит ситуация, когда предметом хищения явились электронные деньги или криптовалюты. Подтверждение осуществления транзакции может быть получено посредством осмотра электронного или криптовалютного кошелька, а вот установление принадлежности осматриваемого кошелька и, соответственно, похищенных средств, потерпевшему вызывает трудности. Для электронных кошельков необходимо направить запрос владельцу электронной платежной системы о предоставлении необходимых сведений. При этом если такие платежные системы зарегистрированы на территории Республики Беларусь, то по запросу, санкционированному прокурором, сведения будут предоставлены. Однако если платежные системы зарегистрированы на территории иностранных государств, то в предоставлении сведений в рамках материала проверки будет отказано, поскольку такая возможность возникает только в рамках возбужденного уголовного дела и только по международному поручению (просьбе) об оказании содействия. Следовательно, официально подтвердить принадлежность электронного кошелька потерпевшему на этапе проверки в боль-

шинстве случаев не представится возможным, и этот факт будет удостоверяться только результатами осмотра самого кошелька.

Получение сведений от владельцев сервисов криптовалютных кошельков еще более проблематично, поскольку такие запросы выполняются не только исключительно по возбужденным делам, но и в большинстве случаев безрезультативны. Объясняется данное обстоятельство двумя причинами. Первая – используемые потерпевшими и преступниками криптокошельки принадлежат организациям, зарегистрированным на территории иностранных государств (анализ уголовных дел показал, что в каждом случае использовалась иностранная, а не белорусская платформа), которые отказывают в предоставлении сведений, ссылаясь либо на политику конфиденциальности, либо запрос вообще не исполняется правоохранительными органами другого государства ввиду отсутствия международной договоренности, недостаточности суммы ущерба, непротивоправности деяния по местному законодательству. Вторая – даже если организация предоставляет данные по запросу, то по содержанию они являются ложными или вымышленными, поскольку никем не проверяются. Исходя из изложенного, можно прийти к выводу, что подтвердить принадлежность криптокошелька на сегодняшний день не представляется возможным, если только организация не будет являться резидентом Республики Беларусь. В этом случае должен в обязательном порядке проводиться осмотр криптовалютного кошелька, в рамках которого лицу, его производящему, надлежит установить сведения-идентификаторы, связывающие личность потерпевшего с личным кабинетом кошелька: личные данные, номер телефона, реквизиты банковской карты, адрес электронной почты (что на практике не выполняется, осмотр кошелька проводится в единичных случаях, а данные о транзакции получаются из объяснений и приобщаемых заявителями скриншотов).

Для хищений в сфере оборота криптовалют важна скорость проведения проверочных и следственных действий для получения и закрепления доказательственной информации. И поскольку большая часть получается через международные поручения (просьбы) о предоставлении информации от иностранных организаций – владельцев Интернет-ресурсов, хостинг-провайдеров, банков, мобильных операторов, то на этапе проверке необходимо обеспечить сохранность информации, которая в последующем будет получена по уголовному делу. В этих целях лицу, производящему проверку, следует направить через национальный контактный пункт МВД (далее – НКП) запрос об оказании содействия в сохранении информации.

Таким образом, на этапе проверки по заявлениям о хищениях в сфере оборота криптовалют посредством мошенничества или модификации компьютерной информации, алгоритм проверочных действий включает: получение объяснений, проведение осмотра устройства и компьютерной информации (в обязательном порядке – криптовалютного или электронного кошелька, при наличии – кабинета Интернет-банкинга, в зависимости от ситуации – чатов в мессенджерах и социальных сетях, на торговых площадках, форумах, электронных писем, журналов программ удаленного доступа), проведение оперативно-розыскных мероприятий

по установлению личности преступника, направление запросов банку-эмитенту счета потерпевшего и запросов по линии НКП о сохранении информации.

Совокупность полученных данных по результатам проверочных мероприятий образует не только основание для возбуждения дела, но и типичные следственные ситуации первоначального этапа расследования:

1) совершено вымогательство, установлена информация, подтверждающая способ хищения, имеются данные, указывающие на личность преступника, преступник не установлен и не задержан (характерна для случаев, когда требование предъявляется через электронное письмо);

2) совершено вымогательство, установлена информация, подтверждающая способ хищения, отсутствуют данные, указывающие на личность преступника, преступник не установлен и не задержан (характерна для случаев, когда вымогательство реализовано через вирусную программу, внедренную на устройство потерпевшего);

3) совершено мошенничество (либо хищение путем модификации), установлена информация, подтверждающая способ хищения, имеются данные, указывающие на личность преступника, преступник не установлен и не задержан (ситуация, когда в распоряжении следователя оказываются сведения, проверка которых может привести к преступнику: личные данные, номер телефона, id аккаунта, e-mail, ip-адрес его устройства, реквизиты банковской карты, фотография, доменное имя фишингового сайта и т.д.);

4) совершено мошенничество (либо хищение путем модификации), установлена информация, подтверждающая способ хищения, имеются данные, указывающие на личность преступника, преступник установлен, но не задержан (характерна для тех случаев, когда потерпевший либо знаком с преступником, либо имел с ним личный контакт);

5) та же, что и в п. 4, но преступник задержан;

6) совершено хищение путем модификации (в редких случаях – мошенничество), установлена информация, подтверждающая способ хищения, отсутствуют данные, указывающие на личность преступника, преступник не установлен и не задержан (при модификации имеет место, если доступ к кошельку получен путем хакерской атаки на криптосервис, либо данные с ip-адресами устройств, осуществлявших вход в кошелек, не регистрируются его общедоступным журналом; при мошенничестве – если потерпевший ввиду неосторожности уничтожил цифровые следы).

Для всех указанных ситуаций общими следственными действиями будут являться подробный допрос потерпевшего и свидетелей, при их наличии. Если похищены криптовалюты, обязателен осмотр криптовалютной транзакции через блокчейн анализатор, который позволит установить данные кошелька преступника, с какими биржами и обменниками он взаимодействовал для вывода средств, на каком кошельке находятся криптовалюты на момент расследования, платформу кошелька (полученные сведения ложатся в основу дальнейших запросов и международных поручений). Первоначальный этап ситуаций пунктов 1-3, 6 нацелен на установление личности подозреваемого и его задержание. При ситуациях 1 и 3 следователю необходимо в первую очередь направить

международные поручения об оказании содействия в предоставлении информации по идентификаторам, выявленным в рамках проверки. При положительном результате такая информация подлежит осмотру. В ситуациях 2 и 6 – выемкой изъять устройства потерпевшего и назначить по ним компьютерно-техническую экспертизу, полученные результаты осмотреть, при выявлении данных, указывающих на преступника, – направить запросы соответствующим организациям, в том числе международные поручения. При ситуации 4 – произвести задержание преступника, в дальнейшем, в том числе в ситуации 5, допросить подозреваемого, установить его сообщников, провести обыск по месту жительства, работы, транспортного средства для выявления и изъятия следов, подтверждающих причастность к хищению, использованных технических устройств, по которым назначить экспертизу, полученные результаты осмотреть.

Последующий этап ситуаций 1-3, 6 направлен на работу с подозреваемым, которая заключается в его допросе, проведении обысков, назначении экспертиз, проведении осмотров, предъявлении ему обвинения, закреплении полученной информации посредством проверки показаний, очной ставки с потерпевшим, проведении следственного эксперимента. В ситуациях 4 и 5 последующий этап начинается сразу с предъявления обвинения, поскольку значительная часть доказательств, подтверждающих вину подозреваемого, уже получена на первоначальном этапе. При любых обстоятельствах на последующем этапе может складываться две ситуации: подозреваемый (обвиняемый) либо свою вину признает и оказывает содействие следователю в расследовании, либо вину отрицает и плохо идет на контакт со следствием. Первая ситуация благоприятная, способствует быстрому окончанию предварительного следствия, вторая – противодействия, в рамках которой следователю необходимо прибегнуть к выработанным криминалистикой тактическим приемам для расположения подозреваемого к совместной эффективной работе.

Таким образом, резюмируя изложенное, можно прийти к выводу, что каждому этапу досудебного производства по делам о хищениях в сфере оборота криптовалют свойственны свои типичные следственные ситуации.

Исходя из анализа уголовных дел, доследственному этапу присуща ситуация, при которой заявление о хищении поступило от потерпевшего, представленная информация требует подтверждения путем проведения проверочных мероприятий. Алгоритм и разновидность таких мероприятий зависит от вида хищения, признаки которого усматриваются из заявления потерпевшего.

На первоначальном этапе расследования могут иметь место четыре варианта следственных ситуаций, для каждой из которых общим является установленный факт совершенного хищения определенного вида, подтвержденный имеющимися в деле доказательствами: имеются данные, указывающие на личность преступника, но он не установлен и не задержан; данные, указывающие на личность преступника, отсутствуют, он не установлен и не задержан; в деле имеются сведения, указывающие на личность преступника, он установлен, но не задержан; имеются сведения, указывающие на личность преступника, он установлен и задержан. Для последующего этапа характерна либо благоприятная ситуация сотрудничества, когда интересы следствия совпадают с интересами заявителя и

подозреваемого (обвиняемого), последний в свою очередь признает вину и оказывает содействие процессу доказывания, либо ситуация противодействия расследованию со стороны обвиняемого, обусловливающая выбор следователем тактики ее преодоления.

Библиографический список

1. Беломытцев, Н. Н. Типичные следственные ситуации первоначального этапа расследования хищений с использованием компьютерной техники / Н. Н. Беломытцев // Вестник Академии МВД Республики Беларусь. – 2020. – № 1. – С. 42–46.

2. Малыхина, Н. И. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершенных с использованием сети Интернет / Н. И. Малыхина, С. В. Кузьмина // Вестник Томского государственного университета. – 2021. – № 426. – С. 238–247.

СЕКСУАЛЬНАЯ ЭКСПЛУАТАЦИЯ КАК ФОРМА СЕКСУАЛЬНОГО НАСИЛИЯ И ОБЪЕКТ КРИМИНАЛИСТИЧЕСКОГО ИССЛЕДОВАНИЯ

Шруб М. П.

УО «Институт повышения квалификации и переподготовки Следственного комитета Республики Беларусь», ул. Первомайская, 9, 220034, г. Минск, Беларусь, m.shrub@sledcom.by

С позиций криминалистической науки исследуется понятие «сексуальная эксплуатация». Обосновывается системообразующая роль сексуальной эксплуатации как формы сексуального насилия применительно к определенному виду преступлений, имеющих в основе своего механизма единое сущностное наполнение. На основе анализа действующего уголовного законодательства обозначается круг и проводится классификация данных преступлений. Определяются перспективные направления исследования обозначенной проблемы.

Ключевые слова: сексуальная эксплуатация; сексуальное насилие; преступления в сфере сексуальной эксплуатации; способ совершения преступления; криминалистическая методика

Одной из ключевых задач криминалистической методики как консолидирующего раздела криминалистики является совершенствование имеющихся и разработка новых частных методик расследования [1]. Решение данной важной специальной задачи основывается на изучении характерных особенностей преступной деятельности и деятельности по их расследованию применительно к преступлениям отдельных видов и групп. В этой связи, с позиций криминалистики, для целей совершенствования правоприменительной практики посредством вооружения ее актуальными рекомендациями важно четко понимать объединяющие начала, общие черты, характеризующие преступную деятельность в определенной сфере. Эти общие черты подлежат исследованию с целью выявления конкретных закономерностей, которые ложатся в основу разработки информаци-