Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»
ЮРИДИЧЕСКИЙ ИНСТИТУТ
Кафедра «Уголовное и уголовно-исполнительное право, криминология»

ОСОБЕННОСТИ ПЕРВОНАЧАЛЬНОГО ЭТАПА РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

ФГАОУ ВО «ЮУрГУ (НИУ)» – 40.03.01. 2017. 460. ВКР

Руководитель работы,
канд. юрид. наук, доцент,
заведующая кафедрой
_____Русман Галина Сергеевна
_____2021 г.

Автор работы,
студент группы Ю-460
_____Вязовцева Виктория Евгеньевна
_____2021 г.

Нормоконтролер,
старший преподаватель
_____Бирюкова Дарья Вячеславовна
_____2021 г.

Челябинск
2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В современной действительности бесспорным является тот факт, что цифровые и телекоммуникационные технологии, равно как и соответствующие технические средства – мобильные телефоны (смартфоны), компьютеры и прочие подобные – стали неотъемлемой частью повседневной жизни практически каждого человека. Возможности, которые сегодня предоставлены уровнем технического развития, делают жизнь человека значительно удобнее и позволяют затрачивать существенно меньшее количество времени на выполнение тех или иных действий, начиная от простого общения со знакомым, находящимся на значительном удалении и заканчивая управлением своими финансами посредством дистанционного взаимодействия с банками и иными финансовыми сервисами. Таким образом, цифровые и телекоммуникационные технологии выступают в роли удобного, практичного и многофункционального инструмента, применяемого во множестве сфер человеческой деятельности, жизненных ситуаций и вариантов.

При этом, любой инструмент, теоретически, может быть использован как в положительных, полезных целях, так и в целях причинения кому-либо вреда и получения, таким образом, какой-либо корыстной выгоды. Как кухонный нож одним лицом применяется в целях приготовления пищи, а другим – в целях убийства, точно так же и цифровые и телекоммуникационные технологии могут быть использованы, и зачастую используются, различными злоумышленниками в целях совершения преступных деяний. В частности, одним из распространенных преступлений, связанных с использованием цифровых и телекоммуникационных технологий, является мошенничество.

Актуальность темы данной выпускной квалификационной работы обусловлена значительной общественной опасностью мошенничества, совершаемого при использовании ресурсов и средств, предоставляемых

человеку цифровыми и телекоммуникационными технологиями. Любой пользователь мобильного телефона, даже сравнительно нечасто берущий его в руки, является потенциальной жертвой такого преступления, не говоря уже о лицах, чья повседневная деятельность напрямую связана с цифровыми и телекоммуникационными технологиями. В свою очередь, дистанционный характер совершения таких преступлений многократно усложняет работу правоохранительных органов по расследованию и раскрытию преступных деяний, относящихся к указанной категории. Так, злоумышленник, контактируя с жертвой преступления посредством телекоммуникационной сети, может находиться на любом удалении от собеседника и использовать различные способы сокрытия своей личности. Кроме того, учитывая характер мошенничества – хищения, совершаемого путем обмана или злоупотребления доверием, далеко не каждое лицо, подвергшееся такому дистанционному обману, своевременно поймет, что стало жертвой преступления, что также способствует возникновению дополнительных затруднений при расследовании.

Помимо указанных фактов, актуальность выбранной темы подтверждается данными официальной статистики МВД, согласно которой за 2020 год количество зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий, составило 510,4 тысяч, что на 73,4 процента больше, чем за 2019 год. При этом, количество преступлений, совершаемых с использованием сети Интернет возросло на 91,3 процента, по сравнению с 2019 годом, а совершаемых при помощи средств сотовой связи – на 88,3 процента. При этом, 80,4 процента от указанного числа преступлений приходятся на хищения, совершаемые в форме мошенничества или кражи. Если же принять то, что не каждая жертва мошенничества осознает, что в отношении нее совершено преступление, и тем более, далеко не все из них обращаются с заявлениями в правоохранительные органы, можно предположить, что число

реально совершаемых преступлений в обозначенной сфере существенно выше данных, учтенных в статистике.

Мошенничества, совершаемые с помощью цифровых и телекоммуникационных технологий, в большинстве случаев, имеют цель завладение денежными средствами, находящимися на банковских счетах потерпевших, либо цифровыми финансовыми активами, и в случае удачного посягательства, таким образом, потерпевшему причиняется существенный имущественный вред, что также подтверждает высокую степень общественной опасности исследуемой категории преступлений.

Рост количества преступлений в рассматриваемой сфере и характерные для таких преступлений особенности расследования и возможные типологические затруднения, закономерно вызывают повышение интереса к указанной проблеме с точки зрения разработки и систематизации различных положений криминалистической науки, которые, будучи правильно примененными впоследствии в ходе производства расследования по делам о мошенничестве, совершенном с использованием цифровых и телекоммуникационных технологий, помогут более эффективно и менее затратно достигать криминалистически значимых целей.

Целью данной выпускной квалификационной работы является исследование криминалистически значимых аспектов расследования мошенничеств, совершаемых с использованием цифровых и телекоммуникационных технологий, рассмотрение их типологической криминалистической модели.

В целях полноценного достижения поставленной цели при выполнении данной выпускной квалификационной работы были выбраны следующие задачи:

1) рассмотрение понятия криминалистической модели мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий в целом, а также составляющих ее элементов в частности;

2) всестороннее изучение способа совершения мошенничества с использованием цифровых и телекоммуникационных технологий, являющегося основным и главным определяющим элементом криминалистической модели таких преступлений;

3) анализ цифровых финансовых активов, выступающих в качестве предмета посягательства при совершении мошенничества с использованием цифровых и телекоммуникационных технологий;

4) исследование существующей системы обстоятельств, подлежащих обязательному установлению в ходе проведения проверки полученной информации о совершении мошенничества с использованием цифровых и телекоммуникационных технологий;

5) изучение особенностей производства следственных действий по делам о мошенничестве с использованием цифровых и телекоммуникационных технологий, характеризующих первоначальный этап расследования рассматриваемых преступлений.

Объектом исследования данной выпускной квалификационной работы являются общественные отношения, связанные с криминалистически значимыми особенностями мошеннических действий, совершаемых с использованием цифровых и телекоммуникационных технологий, а также деятельностью компетентных органов по расследованию и раскрытию указанных преступных деяний.

Предметом исследования данной выпускной квалификационной работы являются нормы российского законодательства, научные положения криминалистической техники и тактики, а также материалы правоприменительной практики, касающейся исследуемых вопросов.

Теоретической основой исследования при подготовке данной выпускной квалификационной работы выступили труды таких ученых, анализировавших изучаемую проблему, как А.А. Шаевич, В.А. Родивилина, А.Н. Колесниченко, С.И Винокуров, С.Л. Денисов, В.А. Машлякевич, В.П.

Бахин, Н.В. Карепанов, А.В. Шебалин, Н.Д. Литвинов, Ю.М. Бойцов, О.С. Бутенко, Р.С. Белкин, и других авторов.

При выполнении данной выпускной квалификационной работы были применены следующие общенаучные методы познания: анализ (при рассмотрении отдельных элементов системы криминалистической модели изучаемых преступлений), синтез (при изучении признаков самой модели, состоящей из различных элементов), дедукция (при экстраполяции положений, выработанных при расследовании конкретных преступлений, на модель расследования всех преступлений схожей категории), моделирование (при изучении создаваемых при расследовании преступления криминалистических моделей), а также методы абстрагирования, аналогии, и другие.

Кроме того, применению подлежал ряд специально-научных методов: исторический (при изучении динамики изменения следовой картины, как элемента криминалистической модели), формально-юридический (при изучении норм действующего законодательства с позиции их криминалистической значимости), а также сравнительно-правовой, метод системного анализа и другие.

Применялись также и специальные методы криминалистики, такие как структурно-криминалистический (при изучении выстраиваемых систем планирования расследования преступления), и другие.

Структурно данная выпускная квалификационная работа включает в себя введение, основную часть, содержащую две главы, разделенные на параграфы, заключение и список использованных при подготовке нормативных, правоприменительных и научно-доктринальных источников.

1 КРИМИНАЛИСТИЧЕСКАЯ МОДЕЛЬ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

1.1 Понятие и элементы криминалистической модели мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий

Общество – динамично развивающаяся система, каждая из сфер которой проходит через определенные эволюционные преобразования. При этом, учитывая тесную взаимосвязь и взаимозависимость каждой из этих сфер от других, очевидно, что та или иная перемена в одной из них, требует оперативного внесения изменений в другие, в целях обеспечения их общей стабильности и сопоставимого уровня развития. В условиях технологического прогресса экономической и социальной сфер, появляются все новые, более сложные технические средства, использование которых может как преследовать общественно полезные цели, так и быть направлено на причинение вреда отдельным лицам, и обществу в целом.

Одним из примеров, иллюстрирующих данное положение, безусловно, являются цифровые и телекоммуникационные технологии, которые, будучи призванными сделать процесс общения и обмена данными между лицами более быстрым, простым и удобным, не могли не стать одним из возможных орудий совершения различных противоправных деяний, среди которых можно выделить, такие экономические преступления как мошенничество.

Все большую распространенность сегодня получают киберпреступления, информационные блокады, виды мошенничества с применением современных IT-технологий и технологий сотовой связи[1].

[1] В МВД созданы подразделения по борьбе с IT-преступлениями. IZ.RU Сайт газеты Известия. URL: https://iz.ru/973398/2020-02-07/v-mvd-sozdany-podrazd (дата обращения: 15.10.2020).

Существование возможности совершения мошеннических преступлений с использованием цифровых и телекоммуникационных технологий закономерно ведет к необходимости формирования определенного набора приемов и методов, использование которых позволит более эффективно вести работу по расследованию и раскрытию данных преступлений. В данном вопросе, следует обратить внимание на роль такой науки, как криминалистика, которая, будучи юридической дисциплиной прикладного характера, изучает, в том числе, закономерности, связанные с совершением и раскрытием преступлений, а также возникновением криминалистически значимой следовой картины, отображающей элементы механизма преступления. Именно данная наука способствует разработке приемов, методов и средств, применяемых впоследствии при практической деятельности компетентных органов по расследованию и раскрытию преступлений.

Для того, чтобы обеспечить максимально полное, всестороннее и объективное изучение объекта исследования данной выпускной квалификационной работы и достичь поставленных цели и задач, необходимо, в первую очередь, определить основные понятия.

Так, одним из наиболее значимых элементов в работе криминалиста, пожалуй, является моделирование исследуемого объекта или ситуации. Это обусловлено ретроспективным характером расследования, производимого по уголовному делу. Расследуемое противоправное деяние имело место в прошлом, относительно момента проведения тех или иных процессуальных действий, связанных с ним. Это значит, что реальный исследуемый объект или же существовавшая на момент совершения преступления обстановка, вероятнее всего, не представлена в распоряжении лица, производящего расследование. В свою очередь, по данной причине, становится необходимым создание некоего аналога, способного заменить оригинальный объект в целях его изучения, то есть использование криминалистического моделирования.

По мнению А.И. Бастрыкина, криминалистическое моделирование является методом, используемым в криминалистике, сущность которого заключается в создании мысленной или материальной модели, позволяющей, при ее дальнейшем изучении, получить необходимую для расследования преступления информацию[1].

При этом, в ходе использования данного метода на практике, получаемая в итоге модель может иметь различную степень сходства с оригинальным объектом. Такая схожесть зависит от того, насколько подробно были учтены все признаки исходного объекта, а степень подробности, в свою очередь, обуславливается целями создания модели.

В каких же целях применяется метод моделирования? Ответить на этот вопрос позволит раскрытие его основных характеристик:

1) моделирование выступает в качестве способа приобретения новой информации об изучаемом объекте;

2) в ходе моделирования следователем или иным субъектом производится определенный ряд действий и операций, как мыслительного характера, так и производственного, то есть связанного с реальным созданием физического объекта;

3) алгоритм действий субъекта моделирования, то есть криминалиста, имеют своей целью создание и дальнейшее изучения полученной модели, а также проверку свойств оригинального объекта, отражаемых ей.

Безусловно, эффективное применение моделирования возможно не в любой ситуации, поскольку не всегда имеет смысл использовать неоригинальный объект в целях его исследования. Однако, можно обозначить ряд случаев, когда создание модели является целесообразным:

1) познаваемый объект существовал в действительности в прошлом (например, в момент совершения преступного деяния), однако физически не существует в момент проведения расследования;

---

[1] Аверьянова Т.В. Криминалистика: учебник. Том I / Т.В. Аверьянова, И.В. Александров, А.И. Бастрыкин и др. / под общ. ред. А.И. Бастрыкина. М.: Изд-во Экзамен, 2014. С. 230.

2) познаваемый объект с некоторой вероятностью будет существовать в будущем, относительно момента моделирования (например, моделирование следователем возможной следственной ситуации, которая возникнет в ходе предстоящего допроса обвиняемого);

3) познаваемый объект, хотя и существует в действительности на момент расследования, но не представляется доступным для непосредственного познания, в связи, с его чрезмерной сложностью (например, выстроенная в организованной преступной группе иерархическая система);

4) в ситуациях, когда необходимо познать процесс, который, в силу своей природы, происходит или слишком быстро, или, напротив, слишком медленно для непосредственного изучения (например, технико-криминалистическое исследование документов).

При этом, создаваемые модели имеют различную природу, что позволяет разделить их определенные группы.

Итак, классификацию криминалистических моделей можно изложить следующим образом:

1) материальные модели;

2) мысленные (идеальные) модели.

Первая группа имеет характерную особенность в виде воспроизведения исследуемых объектов в материально-фиксированном виде. К ней можно отнести различные предметы или более сложные конструкции, создаваемые в целях непосредственного их познания, а также образцы предметов, производимых серийно, в случае, когда необходимо получить модель одного конкретного объекта из этой серии (например, стеклянная бутылка определенной марки, которая выступила орудием или средством совершения преступления, может быть заменена моделью в виде другой бутылки этой же марки, не отличающейся по своих физическим характеристикам).

Кроме того, в рамках данной группы можно выделить два вида моделей: пространственно-подобные и физически-подобные. Первые

воссоздают в натуре пространственные свойства объектов, а также геометрическую форму оригинала. Такими могут выступать слепки, муляжи, макеты и др. Но наиболее сложной моделью, относящейся к данному виду, можно назвать криминалистическую реконструкцию, отличающуюся комплексным характером воспроизведения какой-либо системы во всей полноте внутренних взаимосвязей входящих в нее объектов (например, место происшествия).

Второй вид материальных моделей предполагает, в качестве важнейшей характеристики, сходство физической природы с природой оригинала, что выражается в идентичной динамике различных процессов или явлений, подлежащих изучению. Среди таких моделей можно выделить, например, макеты механизмов в действующем виде, позволяющие изучить механизм их действия в действительности, а также различные фонограммы голосов, видеозаписи производства следственных действий и другие.

Мысленные модели в практике расследования преступлений используются чаще материальных, поскольку любое предположительное представление следователя о различных событиях, связанных с совершением расследуемого преступления, по сути своей, является мысленной моделью, поскольку воспроизводит, на основании фактических или предполагаемых данных, умозрительную картину прошлого, которая впоследствии используется для такого же мысленного изучения. То же можно сказать и о планировании следователем своих дальнейших действий в ходе производства расследования.

Мысленные (идеальные) модели, в свою очередь, подразделяются на три вида:

1) модели, создаваемые в целях воспроизведения объекта (какого-либо предмета либо события), имевшего место в прошлом, относительно момента познания. Например, события, которые происходили ранее, и допрашиваемое лицо было их свидетелем, то есть непосредственно воспринимало;

2) модели, создаваемые в целях воспроизведения объекта, существующего в настоящем, одновременно с моментом познания. Например, моделирование взаимосвязей между преступлениями со схожим «почерком» преступника – серийных убийств, - или же выстраивание модели иерархической структуры преступного сообщества, существующей на момент расследования, но достоверного знания о которой у следователя нет;

3) модели, создаваемые в отношении объектов, которые будут иметь место в будущем относительно момента познания. Целью такого моделирования может являться как планирование действий следователя на следующий день, так и предотвращение возможного преступного деяния в будущем, посредством предположения о том, в какое время, в каком месте и так далее, оно должно произойти.

При этом, характер знаний, используемых при построении любой из вышеперечисленных мысленных моделей, может быть различным, например:

1) исключительно положительное, то есть достоверное знание используется в ситуации, когда субъект познания обладает точными данными относительно всех признаков исследуемого объекта. Например, эти данные основываются на каких-либо подлинных документах, таких как банковская выписка;

2) исключительно предположительное знание, имеющее место в ситуации, когда однозначных и достоверных сведений об объекте исследования в распоряжении следователя нет. Примером такого знания могут служить показания свидетеля с плохим зрением о событии, имевшем место в сумерках, когда у самого свидетеля отсутствует уверенность в своих показаниях, или же о событиях, произошедших настолько быстро, что с уверенностью говорить о его деталях не представляется возможным (так, затруднительно указать точную модель и номер автомобиля, проехавшего мимо свидетеля на большой скорости);

3) «смешанное», сочетающее в себе положительное знание о части признаков объекта исследования, и предположительное знание о другой их

части. Например, такое знание имеет место в ситуации, когда часть показаний свидетеля подтверждена объективными фактами, а другая часть – нет, и ее достоверность остается в области предположений субъекта познания (в данном случае - следователя)[1].

Основываясь на вышеперечисленном, можно сделать вывод, что криминалистическое моделирование, как метод, используемый при расследовании преступлений, равно как и создаваемые в ходе этого расследования модели, могут приобретать различные формы и применяться в разнообразных целях. С помощью моделирования субъект познания может погрузиться в обстановку совершения того или иного преступления и наиболее подробно изучить различные присущие ему детали и типовые черты. Со временем эффективность моделирования в отношении преступлений определенной категории только повышается, поскольку накапливаемый опыт расследования предыдущих преступлений способствует созданию более точной модели будущих схожих преступных деяний и приводит к повышению эффективности их расследования.

Важную роль моделирование играет и в расследовании такого преступления, как мошенничество. Приоритет при расследовании мошенничества, в том числе совершаемого с использованием средств сотовой связи, отдается мысленным моделям, которые, по мнению некоторых авторов, можно также именовать криминалистической характеристикой[2].

Само понятие криминалистической характеристики было сформировано и получило дальнейшее развитие более пятидесяти лет назад в трудах такого отечественного ученого, как А.Н. Колесниченко[3], который

---

[1]Лоер В. Криминалистика: учебник / В. Лоер. М., 2000. С. 34.

[2] Шаевич А.А., Родивилина В.А. Об особенностях некоторых элементов криминалистической характеристики мошенничеств, совершаемых с использованием средств мобильной связи // В сборнике: Актуальные проблемы науки и практики. сборник научных трудов. Хабаровск, 2018. С. 449-450.

[3] Колесниченко А.Н. Общие положения методики расследования отдельных видов преступлений / А.Н. Колесниченко. Харьков, 1965. С. 23.

считается одним из основоположников криминалистической методики как раздела криминалистики. Криминалистическую характеристику он понимал, как систему сведений о криминалистически значимых признаках преступлений данного вида, отражающая закономерные связи между ними и служащая построению и проверке следственных версий для решения задач расследования, являющуюся основой методики расследования преступлений.

Однако по поводу определения криминалистической характеристики нет единства среди представителей научного сообщества[1]. Так, например, С.И. Винокуров[2] вкладывал в данный термин следующее значение: научно разработанная система типичных признаков конкретного вида преступления, позволяющая выяснить механизм следообразования, уяснить первоочередные следственные задачи.

В.П. Бахин полагал, что в содержание криминалистической характеристики того или иного преступления должны входить исключительно такие его элементы, которые можно назвать имеющими розыскную направленность. К этим элементам относятся, в частности, следующие[3]:

1) предмет преступного посягательства;

2) характеристика личности преступника;

3) следовая картина происшествия;

4) способ совершения преступления.

Говоря же непосредственно о криминалистической характеристике мошенничеств, совершаемых с использованием средств сотовой связи, исчерпывающим представляется мнение, высказанное В.А. Машлякевичем, который определял ее, как взаимосвязанную информационно наполненную

---

[1] Денисов С.Л. Понятие «Криминалистическая характеристика преступления» // Гуманитарные, социально-экономические и общественные науки. 2015. №5. С. 67-68.

[2] Винокуров С.И. Криминалистическая характеристика преступления, ее содержание и роль в построении методики расследования // Методика расследования преступлений. Общие положения:Материалы научно-практической конференции. М., 1976. С. 101.

[3] Бахин В.П. Криминалистическая характеристика преступлений как элемент расследования // Вестник криминалистики. 2000. № 1. С. 21.

систему, целью которой является обеспечение надлежащего расследования преступного деяния, содержащую сведения о предмете преступного посягательства; об обстановке совершения преступления, диктующей выбор преступником способа его совершения; о зависящем от выбранного способа и обстановки преступления механизме следообразования; о типичной личности преступника и потерпевшего, а также о связующем их звене - доверенных лицах преступника[1].

Анализируя криминалистическую характеристику указанной категории преступлений, будет правильно начать с рассмотрения личности субъекта, совершающего такие деяния.

Еще недавно, большая часть мошенничеств с применением средств сотовой связи, являющихся частным случаем использования телекоммуникационных технологий, совершалась лицами, содержащимися в местах лишения свободы, несмотря на то, что данная категория лиц должна быть ограничена в применении таких средств. Так, согласно мнению, высказанному первым заместителем начальника Главного управления уголовного розыска МВД России Александром Фроловым, заключенные совершают около трети преступлений данной категории[2]. Ю.М. Бойцов полагает, что ситуация еще хуже – по его мнению, доля мошенничеств, совершаемых осужденными, составляет 60 процентов от общего числа таких преступлений[3].

Такая статистика позволяет сделать вывод о том, что на момент ее собирания работу уголовно-исполнительной системы нельзя было назвать

---

[1]Машлякевич В.А. К вопросу о структуре и содержании криминалистической характеристики мошенничеств, совершаемых с использованием средств телефонной связи // Алтайский юридический вестник. 2016. № 14. С. 104.

[2] Три года тюрьмы за телефонное мошенничество. URL: https://ribalych.ru/2016/03/24/tri-goda-tyurmy-za-telefonnoe-moshennichestvo/ (дата обращения 28.09.2020).

[3] Бойцов Ю.М. Проблемы проверки, выявления и раскрытия мошенничества с использованием мобильных средств связи // Вестник Санкт-Петербургского Университета МВД. 2016. № 2. С. 108.

достаточно эффективной и обеспечивающей установленный порядок отбывания наказания осужденными лицами.

Большая распространенность мошенничеств с использованием средств сотовой связи, совершаемых заключенными, отбывающими наказание в местах лишения свободы связана, в первую очередь, с благоприятной средой для обмена криминальным опытом. Таким образом, становится возможным образование обновленных мошеннических схем и даже формирование устойчивых связей и преступных групп, для чего достаточно появления среди осужденных одного «специалиста» в сфере мобильного мошенничества.

Так, согласно приговору Волжского районного суда Самарской области от 14 января 2020 года[1], лицо признано виновным в совершении преступления, предусмотренного частью второй статьи 159 Уголовного кодекса Российской Федерации, то есть мошенничества, совершенного группой лиц по предварительному сговору при следующих обстоятельствах. Данное лицо, будучи осужденным к лишению свободы за совершение другого преступления, отбывая назначенное наказание на территории ФКУ ИК-28 ГУФСИН России по Самарской области, решило завладеть чужим имуществом, посредством обмана, для чего вступило в сговор с иными неустановленными лицами. Преступной деятельностью данные лица занимались в период с 2013 года по декабрь 2014, и в целях ее осуществления лицо приобрело сотовый телефон и сим-карты. Впоследствии, лицо обратилось к другим осужденным, находящимся в том же исправительном учреждении и занимавшимся ранее преступной деятельностью, с просьбой о привлечении их знакомых к рассылке смс-сообщений с текстом «Ваша банковская карта заблокирована, перезвонить по телефону …». При этом, номер телефона в указанных сообщениях

[1] Приговор Волжского районного суда Самарской области от 14 января 2020 г. по делу № 1-242/2019. URL: https://sudact.ru/regular/doc/cPdsiyJgw5JR/ (дата обращения 19.12.2020).

указывался тот, которым пользовалось само это лицо. Рассылка осуществлялась по абонентским номерам, коды которых выбирались в случайном порядке путем бессистемной замены последних цифр.

Со слов осужденной, умысел на совершение данных преступлений у нее возник после того, как она заметила, как аналогичной деятельностью занимаются другие отбывающие наказание в колонии. Способ совершения мошенничества с использованием сотового телефона также узнала от них. Так, используя имевшееся средство сотовой связи, осужденная отправила заведомо ложное по своему содержанию текстовое сообщение о блокировании банковской карты на абонентский номер потерпевших. Получив данное сообщение, потерпевшие осуществляли звонки по номеру, указанному в сообщении, и в ходе разговора лицо, представившись работником службы безопасности банка, сообщало потерпевшим ложную информацию о блокировании их банковских карт в связи с совершением с них определенных платежей на счета лиц, находящихся в других регионах. Далее осужденная заявляла, что для разблокирования карты необходима проверка анкетных данных потерпевших и установление денежных сумм, находящихся на банковских картах. При этом, в случае, если суммы оказывались небольшими, осужденная объясняла, что смс-сообщение было ошибочным, и с картой все в порядке, а если же сумма была крупной, она подтверждала блокирование и говорила о необходимости перевести денежные средства в целях их сохранности, по указываемым лицом платежным реквизитам.

Таким образом, потерпевшая, следуя инструкции, переводила через банкомат указанную сумму на абонентские номера, которые находились в пользовании осуждённого лица. После поступления денежных средств, осуждённая переводила их в банк или на абонентские номера лиц, которым она должна была денежные средства. Похищенные денежные средства она тратила на продукты питания и товары первой необходимости.

Приговором суда данное лицо осуждено за совершение мошеннических действий группой лиц по предварительному сговору.

Основываясь на данном приговоре, можно подтвердить предположение о том, что совершение мошеннических действий с использованием средств сотовой связи лицами, отбывающими наказание в виде лишения свободы, связано, во многом, с влиянием окружающей их «атмосферы», под воздействием которой формируется не только умысел на совершение указанных действий, но и необходимые для этого навыки.

Субъектом мошенничества в общем виде является вменяемое физическое лицо, достигшее шестнадцатилетнего возраста. При этом, наиболее часто такие преступления совершаются лицами зрелого возраста, обладающие определенными личностными качествами, в частности, хитростью, изворотливостью и умением привлечь к себе внимание собеседника. Именно такие лица, обладающие также некоторым набором знаний о человеческой психологии, способны войти в доверие и спровоцировать нужные эмоции, для достижения преступного результата в виде завладения чужой собственностью.

При этом, мошенничество, совершаемое дистанционно с использованием цифровых и телекоммуникационных технологий, имеет, в этом смысле, определенные особенности. Так, лицо, совершающее данное преступление, находится на значительном удалении от потерпевшего и, чаще всего, не знакомо с ним лично, из-за чего у него фактически отсутствует возможность использования персонального влияния на потерпевшего или применения психологических методов воздействия, связанных именно с физическим контактом. Кроме того, отсутствие знакомства лишает злоумышленника возможности использовать личный авторитет, как это возможно при классической модели мошенничества[1].

[1] Литвинов Н.Д., Федоров А.Н. Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения // JSRP. 2015. №12. С. 75-76.

Предмет мошенничества в классическом смысле представляет собой чужое имущество либо право в отношении данного имущества, которое путем обмана похищает лицо, совершающее данное преступление. Предмет же мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий, существенно более узкий – принадлежащие потерпевшему денежные средства, а также цифровые финансовые активы, которые мошенник получает в свое владение дистанционным способом, не прибегая к какой-либо форме прямого контакта. Также, стоит отметить, что дистанционный характер такого мошенничества предопределяет форму денежных средств, выступающих его предметом – эти средства могут быть только в безналичном, электронном виде (цифровые финансовые активы). Специфика же цифровых финансовых активов, выступающих предметом преступного посягательства, заключается, помимо отсутствия их физического выражения, также в том, что отношения в данной сфере, на сегодняшний день, российским законодательством в полной мере не урегулированы, что затрудняет работу сотрудников правоохранительных органов по расследованию и раскрытию соответствующих преступлений.

Кроме того, особенности способа совершения мошенничества с использованием цифровых и телекоммуникационных технологий и предмета посягательства, обуславливает то, что такое мошенничество никогда не перерастет, в ходе его совершения, в другой состав преступления, например, грабеж или разбой.

Рассмотрев предмет мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий, полагаем необходимым также проанализировать особенности следовой картины таких преступлений.

Исследуемая категория преступлений, оставляет лишь незначительное количество материальных следов, в то время как большая их часть сохраняется в виде следов виртуальных.

Такие виртуальные следы требуют внимания не только правоприменителей, расследующих соответствующие преступления, но ученых и законодателей, потому что, как и любая новая и развивающаяся категория, они имеют свои определенные особенности, например, в выявлении и изъятии.

В ходе расследования преступлений, необходимо всестороннее изучение следовой картины, оставленной конкретным деянием, при этом след необходимо сначала выявить, а затем правильно изъять.

Итак, чтобы остался электронный след и в дальнейшем его можно было выявить, нужна определенная информация. Она посредством материальных носителей передается от одной системы к другой в виде сигнала, являющегося отображением сообщения и средством переноса информации в пространстве и времени[1]. Следовательно, для установления обстоятельств преступления нужно само устройство, содержащее электронные следы.

С учетом этого, такие ученые, как А.В. Шебалин и О.С. Бутенко, предложили классифицировать электронные следы, разделив их на две группы[2]:

1) следы, которые отобразились непосредственно в памяти сотового телефона или иного технического устройства – соответственно, материальным носителем следов будет данное техническое устройство, и в целях их изъятия необходимо произвести определенные действия в отношении него;

2) следы, которые отобразились в информационной системе компании-оператора (в случае, если таковая имеется), предоставляющей телекоммуникационные услуги – местом нахождения таких следов будет эта система.

---

[1]Карепанов Н.В. Некоторые вопросы выявления и исследования следов преступлений // Российское право: Образование. Практика. Наука. 2019. №3. С. 49-50.

[2] Шебалин А.В. Расследование хищений средств сотовой связи: дис. … канд. юрид. наук. Томск, 2010. С. 9.

В свою очередь, первая из указанных групп следов, по мнению данных авторов, содержит в себе несколько определенных видов следов[1]:

1) следы переговоров – электронный «отпечаток» процесса ведения такого разговора;

2) следы передачи и приема сообщений;

3) следы доступа в информационно-телекоммуникационную сеть Интернет с помощью электронного устройства, а также следы использования услуг и функций посредством использования данной сети;

4) следы, непосредственно содержащиеся в аудио- и видеозаписях, а также фотографиях, сохраненных в памяти устройства;

5) следы финансовых операций, например, произведенных с помощью приложений или сервисов, предоставленных банком;

6) следы, отраженные в иных сервисах и приложениях, содержащих данные, принадлежащие лицу. Чаще всего, такими приложениями являются социальные сети – Вконтакте, Facebook, WhatsApp и другие.

Таким образом, помимо привычных и традиционных следов – материальных (например, отпечатков пальцев рук) и идеальных (например, образа преступника, запечатленного в памяти потерпевшего), преступления, совершаемые с использованием цифровых и телекоммуникационных технологий, оставляют также специфические «электронные» следы, которые, в свою очередь, требуют специфических способов их обнаружения и изъятия. Особенности данных следов и методов криминалистической работы с ними, будут рассмотрены в следующих параграфах.

Произведенный анализ криминалистической модели мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий как в целом, так и в части отдельных ее элементов, позволяет подчеркнуть значимость моделирования в целях совершенствования

---

[1] Бутенко О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия // LexRussica. 2017. № 4. С. 49.

возможных способов расследования преступления, поскольку систематизация знаний об определенных закономерностях преступлений, совершенных ранее, способствует эффективному их использованию в отношении раскрытия схожих преступлений, которые будут совершены в будущем.

1.2 Способ совершения мошенничества посредством цифровых и телекоммуникационных технологий, как основной элемент криминалистической модели

Наряду с предметом и обстановкой совершения любого преступления, одним из наиболее значимых элементов модели преступного деяния, является способ его совершения. Его важность обусловлена тем, что каждая отдельная категория преступлений предусматривает определенный, отличающийся от других категорий, набор возможных способов как непосредственно достижения преступной цели, так и приготовления к преступлению и сокрытия его следов[1].

Несмотря на самостоятельную значимость каждого элемента криминалистической модели преступления, все они находятся в непосредственной системной взаимосвязи, и каждый из них оказывает определенное влияние на другие. Так, способ совершения преступления, применяемый в конкретной ситуации преступником, определяется сочетанием таких элементов, как предмет посягательства, обстановка, в которой совершается преступное деяние, и характеристика личности самого лица, совершающего его.

---

[1]Гавло В.К. Судебно-следственные ситуации: психолого-криминалистические аспекты: монография / В.К. Гавло, В.Е. Клочко, Д.В. Ким. Барнаул: Издательство Алтайского университета, 2006. С. 116.

Термин «способ преступления» не имеет легального закрепления, в связи с чем, в научной литературе среди авторов отсутствует единство в определении данной категории.

Так, по мнению Г.Г. Зуйкова, способ преступления является взаимосвязанной системой, включающей в себя действия, направленные на подготовку и совершение преступления, а также сокрытие его следов, которые обуславливаются сложившимися в момент совершения преступления условиями внешней среды, набором психофизиологических характеристик личности, а также используемых орудий[1].

Подход, выработанный Г.Г. Зуйковым, был дополнен Р.С. Белкиным, который указал на то, что все входящие в способ совершения преступления действия, а также иные элементы криминалистической характеристики, объединяются единым «преступным замыслом»[2].

Позже, ссылаясь на приведенные выше позиции ученых, В.Ф. Ермолович[3] сформулировал определение способа совершения преступления, как «систему умышленных действий по подготовке, совершению и сокрытию преступления, охватываемую единым преступным замыслом, детерминированную психофизическими качествами личности преступника (его соучастников) и избирательным использованием им (ими) соответствующих условий, места, времени, а также с учётом возможных действий (бездействия) со стороны потерпевшего, иных лиц[4].

Проанализировав приведенные подходы к пониманию способа совершения преступления, полагаем, что данные авторы формулируют достаточно полные определения рассматриваемой категории, позволяющие

---

[1] Зуйков Г.Г. Криминалистическое учение о способе совершения преступления: автореф. дис. … докт. юрид. наук. М., 1970. С. 10.

[2] Белкин Р.С. Курс криминалистики. В 3–х т. Т. 3 / Р.С. Белкин. М.: Юристъ, 1997. С. 359.

[3] Ермолович В.Ф. Криминалистическая характеристика преступлений / В.Ф. Ермолович. Минск: Амалфея, 2001. С. 54–55.

[4] Бессонов А.А. Способ преступления как элемент его криминалистической характеристики // Пробелы в российском законодательстве. 2014. №4. С. 172. URL: https://cyberleninka.ru/article/n/sposob-prestupleniya-kak-element-ego-kriminalisticheskoy-harakteristiki (датаобращения: 08.11.2020).

судить как о взаимосвязанности всех элементов криминалистической характеристики, так и о принципиальной значимости каждого из них и, в частности, способа, применяемого преступником.

В.Н. Кудрявцев, в свою очередь, считает, что способ совершения преступления представляет собой объективную характеристику совершенного лицом действия, не зависящую от присутствующей в нем формы вины[1]. Однако, при рассмотрении данного подхода к определению, представляется, что автор, стремясь подчеркнуть характеристику способа совершения деяния, как элемента объективной стороны состава преступления, приводит более узкую трактовку данного понятия, поскольку не указывает на его взаимосвязанность с другими элементами, характеризующими преступление.

На основании анализа рассмотренных точек зрения о способе совершения преступления, целесообразным представляется выделение следующих составляющих его элементов:

1) действия, совершаемые как самим преступником, так и его соучастниками (при их наличии), направленные на подготовку к преступлению, достижение преступного результата, а также сокрытие оставляемых следов;

2) системная связанность данных действий с другими элементами криминалистической характеристики преступления: предметом, на который непосредственно направлено посягательство, сопровождающей преступное деяние обстановкой, а также психофизиологическими свойствами личности, присущими лицу, совершающему преступление;

3) совокупность используемых в целях совершения преступления орудий, средств и приемов;

4) следовая картина, отражающая особенности произведенных в целях совершения преступления действий и примененных орудий с средств;

---

[1] Кудрявцев В.Н. Объективная сторона преступления: монография / В.Н. Кудрявцев. М., 1960. С. 72.

5) единый преступный замысел, объединяющий все предшествующие элементы.

Стоит отметить, что наибольшая связь у способа совершения преступления прослеживается с таким элементом криминалистической характеристики, как личность преступника. Качества, присущие лицу, совершающему преступление, сформировавшиеся в течение его жизни, накладывают определенный отпечаток на модель его поведения в каждой конкретной ситуации. Следовательно, способы, применяемые для достижения преступного результата лицами, обладающими резко отличающимися психофизиологическими характеристиками, будут также отличаться друг от друга.

Кроме того, играет роль и профессия лица, а также соответствующие ей специальные навыки и привычки. При этом, если в одном случае такие привычки являются лишь особенностью, необязательной для достижения цели, то в другом случае, именно профессиональные навыки являются необходимыми для достижения преступного результата, и лицо, не обладающее ими, объективно будет неспособно совершить определенное преступление.

Также, существенная связь присутствует между способом совершения преступления, и обстановкой данного преступления, поскольку в зависимости от окружающих условий действия лица, направленные на достижение преступной цели, также могут изменяться. При этом, реакция того или иного лица, например, на стрессовую и неблагоприятную обстановку зависит и от его личностной характеристики, что снова указывает на непосредственное взаимное влияние различных элементов криминалистической характеристики преступления друг на друга.

Важно отметить, что принципиальное значение имеет сбор и систематизация данных о возможных способах совершения преступлений, относящихся к определенной категории, поскольку такая систематизация позволяет выработать типичную модель действий преступника в

определенных условиях. В свою очередь, такая модель способствует более эффективной работе уполномоченных органов, направленной на расследование и раскрытие схожих преступлений в будущем.

Такая категория преступлений, как мошенничество, совершаемое с использованием цифровых и телекоммуникационных технологий, безусловно, имеет свою выраженную специфику, касающуюся, в том числе, и способа совершения преступления. Это обусловлено как предметом посягательства, так и орудиями, и средствами достижения преступного результата, которыми выступает телекоммуникационная сеть и технические средства, использующие ее.

Преступления, относящиеся к исследуемому виду, могут совершаться различными способами, объединенными одной общей родовой чертой – дистанционным характером воздействия преступника на потерпевшего, лишенным непосредственного прямого контакта. Именно данная черта и предопределяет возможные конкретные способы мошеннических действий.

Также, выполняя действия, направленные на подготовку к совершению преступления, злоумышленники могут предпринять попытки добычи определенной информации, касающейся потенциальных жертв преступлений. Доступ к данной информации они могут получить посредством, например, незаконного завладения какими-либо базами данных. Наибольшей популярностью, в этом смысле, пользуются базы операторов сотовой связи, которые в результате противоправных действий работников самого оператора оказываются в руках третьих лиц. Безусловно, располагая базой номеров и имен владельцев этих номеров, мошенник получает дополнительную возможность оказать воздействие и добиться определенного доверия жертвы преступления, поскольку, позвонив такому лицу, сразу же обращается к нему по имени, что у абонента может вызвать ошибочное мнение о том, что звонящий является представителем той же компании-оператора сотовой связи или даже банка, клиентом которого этот абонент является.

Однако, базы операторов сотовой связи являются одними из наименее опасных в случае их попадания в распоряжение преступника. Так, например, если мошенник получает доступ к базе пациентов медицинского учреждения, он сразу же располагает еще более существенным рычагом воздействия на жертву преступления, поскольку знает не только ее имя, но и историю болезней, и может, отталкиваясь от этих сведений, предложить приобрести дорогостоящий лекарственный препарат, способный помочь именно при том заболевании, которое наблюдается у потерпевшего. И, разумеется, наиболее эффективно и просто мошенник может, таким образом, завладеть денежными средствами человека, больного смертельной болезнью и находящегося, из-за этого, в состоянии отчаяния, и готового расстаться с крупной суммой денег ради надежды на излечение.

Еще одной потенциальной опасностью являются «утечки» баз данных клиентов банковских организаций. В результате попадания таких сведений в распоряжение злоумышленников, они получают возможность более точечного планирования и выбора жертвы, исходя их уровня ее доходов. Соответственно, для мошенников более привлекательным объектом хищения являются денежные средства в крупных размерах, а, следовательно, и лицо, на банковском счету которого находится крупная сумма денег, с большей долей вероятности будет выбрано мошенником в качестве «цели». Одним из последних и вызвавших наибольший общественный резонанс примеров такого рода «утечек» является ситуация, имевшая место осенью 2019 года. Тогда, в результате противозаконных действий сотрудника банка, в так называемый «даркнет» были выложены данные большого количества клиентов Сбербанка. Эти данные включали в себя номера телефонов, полные имена, номера банковских счетов, лимит по кредиту, предоставленный банком данному клиенту, и даже сумму остатка на счете. Данная утечка, став самой крупной из известных подобных случаев в России, безусловно могла повлечь неблагоприятные последствия, в том числе, и в виде использования этих данных мошенниками, в целях завладения денежными средствами

клиентов банка, например, посредством звонков по опубликованным номерам телефонов. По данному делу было проведено расследование, в результате которого 8 сентября 2020 года Красногорским городским судом Московской области был вынесен обвинительный приговор одному из бывших сотрудников банка, по обвинению в незаконном получении и разглашении сведений, составляющих банковскую тайну[1].

Таким образом, говоря о стадии подготовки к совершению такого преступления, как мошенничество с использованием цифровых и телекоммуникационных технологий, можно выделить определенные группы способов достижения поставленной преступником предварительной цели[2]:

1) первоначальное подготовка технических устройств (сотовых телефонов, SIM-карт, иных средств) для их последующего использования в целях совершения преступных действий;

2) использование данных устройств для собирания информации о потенциальных жертвах преступлений, для чего могут быть использованы базы данных, незаконно полученные от операторов сотовой связи, медицинских учреждений, а также банков, и данные, содержащиеся в социальных сетях или иных приложениях, аккумулирующих информацию о лице;

3) подготовка программной базы для облегчения совершения будущих преступлений. Такая база может состоять, например, из приложений, изменяющих голос говорящего во время телефонного разговора;

---

[1] Приговор Красногорского городского суда Московской области от 08 сентября 2020 г. по делу № 1-222/2020. URL: https://krasnogorsk--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&case_id=142605937&case_uid=03ac451d-aafe-448b-b9e6-fa620e52afda&delo_id=1540006 (датаобращения 23.12.2020).

[2] Журкина О.В., Бондаренко И.В. К вопросу о способах совершения мошенничества с использованием сотовой (подвижной) связи // Вопросы российского и международного права. 2015. № 3–4. С. 22.

4) приготовление способов получения денежных средств или цифровых финансовых активов от потерпевших путем, например, создания электронных кошельков в различных платежных системах;

5) определение злоумышленником способа дальнейшего выбора лица, в отношении которого будут производиться действия, направленные на хищение денежных средств. Такими способами, в свою очередь, могут выступать: набор абонентского номера либо начало переписки с лицом, определяемым случайным образом; использование попавших в распоряжение злоумышленника баз данных; совершение действий в отношении заранее конкретно определенного лица, с которым, в том числе, злоумышленник может быть непосредственно знаком[1].

Выполнив действия по подготовке к преступлению, злоумышленник приступает к реализации преступного замысла. Достижение цели в виде хищения денежных средств путем обмана, при этом, может обеспечиваться различными способами. В числе наиболее типичных способов, применяемых именно при использовании средств сотовой связи, можно выделить:

1) рассылки SMS-сообщений с различным содержанием. Данные сообщения могут содержать, например, просьбу о пополнении счета друга или родственника, который, будто столкнулся с какой-либо финансовой проблемой (данные сообщения сопровождаются, как правило, такими обращениями, как «мама», «сынок», «друг» и так далее, для того, чтобы создать впечатление о том, что отправителем сообщения действительно является близкий абоненту человек); уведомление о блокировании банковской карты с указанием номера, по которому необходимо позвонить, чтобы карту разблокировать; уведомление от имени оператора сотовой связи о подключении платной услуги, для отключения которой необходимо пройти

[1] Лабутин А.А. «Мобильные» мошенничества: основные способы совершения // Вестник Казанского юридического института МВД России. 2013. № 12. С. 51-52.

по указанной ссылке и т.д.[1]. Так, например, факт мошеннических действий в целях хищения денежных средств путем рассылки сообщений о блокировке банковской карты абонента был установлен Приговором Промышленного районного суда города Самары от 13 февраля 2019 года по делу № 1-10/2019[2];

2) звонок абоненту от злоумышленника, который заявляет о выигрыше - дорогостоящем призе (автомобиль, крупная сумма денег и т.д.). После этого, мошенник предлагает жертве преступления оплатить определенную сумму налога или стоимость почтовой пересылки[3]. Использование такого приема в целях завладения денежными средствами потерпевшего было установлено, например, приговором Кудымкарского городского суда Пермского края от 17 января 2014 года по делу № 1-10/2014, которым лицо было признано виновным в совершении нескольких эпизодов мошеннических действий с использованием средств сотовой связи[4];

3) звонок от злоумышленника, в ходе которого он, представившись должностным лицом государственного органа или банка, узнает у абонента сведения, касающиеся его банковских счетов, данных паспорта и иных документов, и в последующем используют данную информацию в целях хищения принадлежащих потерпевшему денежных средств[5]. Так, приговором Когалымского городского суда Ханты-Мансийского

---

[1] Жукова Н.А. Расследование и раскрытие преступлений, совершенных посредством sms-сообщений: метод. указания / Н.А. Жукова, Ю.А. Ковтун и др. М.: ДГСК МВД России, 2014. С. 23-25.

[2] Приговор Промышленного районного суда города Самары от 13 февраля 2019 года по делу № 1-10/2019. URL: https://sudact.ru/regular/doc/qnhprHQxwRLQ/(дата обращения 06.10.2020).

[3] Литвинов Н.Д., Федоров А.Н. Особенности, причины и тенденции развития дистанционного мошенничества лицами, отбывающими наказание в местах лишения свободы // Научно-исследовательские публикации. 2015. №13. С. 66.

[4] Приговор Кудымкарского городского суда Пермского края от 17 января 2014 года по делу № 1-10/2014. URL: https://sudact.ru/regular/doc/L5zD7vIBXl5O/ (дата обращения 06.10.2020).

[5]Астишина Т. В., Маркелова Е. В. Проблемы расследования преступлений, связанных с мошенническими действиями, совершенных с использованием средств сотовой телефонной связи // Вестник Казанского юридического института МВД России. 2014. №2. С. 96-96.

автономного округа от 7 мая 2020 года по делу №1-19/2020 установлен факт виновности лица в неоднократном совершении мошеннических действий в целях хищения денежных средств с банковских счетов абонентов, посредством выдачи себя за сотрудника банка, которым, в действительности, данное лицо не являлось[1];

4) использование телефонного номера, звонок по которому сразу списывается крупная сумма со счета звонившего. Также могут использоваться и специальные ссылки, переход по которым также приводит к списанию со счета[2].

При использовании таких способов, главным является подбор приема, который наиболее эффективно побудит жертву преступления позвонить по номеру или перейти по ссылке. Например, это может быть сообщение с текстом о том, что необходимо в срочном порядке найти донора с редкой группой крови для спасения жизни ребенка или же просто с призывом перечислить небольшую сумму в «благотворительный фонд». Такие приемы вызывают эмоциональную реакцию, благодаря которой некоторые пользователи сразу же переходят по указанной ссылке, не подумав о возможных последствиях, которые выражаются в том, что после открытия ссылки, на мобильное устройство лица скачивается вредоносное (вирусное) программное обеспечение, начинающее в автоматическом порядке отправлять сообщения, посредством которых осуществляется перевод денежных средств на счета мошенников. Также, схожего результата достигают сообщения, в которых указывается, что абоненту поступило голосовое сообщение или MMS-открытка, для просмотра которой необходимо перейти по указанной ссылке. При этом, часто такие сообщения содержат в себе какое-либо имя лица, которое, будто отправило данную

[1] Приговор Когалымского городского суда Ханты-Мансийского автономного округа от 7 мая 2020 года по делу №1-19/2020. URL: https://sudact.ru/regular/doc/UvHCmAkAvGLH/ (дата обращения 06.10.2020).

[2] Лозовский Д.Н., Ульянова И.Р. Особенности расследования преступлений, совершенных путем смс-сообщений // Гуманитарные, социально-экономические и общественные науки. 2016. №12. С. 146.

открытку, чтобы у абонента сложилось впечатление, что речь идет о каком-то знакомом ему человеке с таким именем.

Характерно, что все указанные способы объединяет определенная психологическая черта, лежащая в основе каждого из них. Так, процесс достижения мошенником преступного результата путем использования цифровых и телекоммуникационных технологий всегда начинается с того, что жертва преступления вводится преступником в положение, связанное с чувством вины или «жертвенности», либо же в состояние психологического ступора. Это необходимо для того, чтобы субъект, в отношении которого совершается преступление, оказался на более слабой позиции в диалоге, чем мошенник, вербально «нападающий на него».

Неожиданность, с которой жертва получает информацию, как и содержание этой информации, существенно ослабляет ее способность «защищаться», используя какие-либо свои доводы, и приводит к тому, что позиция мошенника буквально навязывается его собеседнику, практически вынуждая его действовать, в соответствии с указаниями, получаемыми от злоумышленника.

Безусловно, наиболее ярко такое влияние проявляется именно при телефонном разговоре, в котором, помимо указанных выше приемов, используются также определенные интонации и темп речи, также способствующий невозможности должным образом защититься для жертвы. Именно данная причина способствует большей эффективности мошеннических действий при наличии голосового контакта, по сравнению с обменом текстовыми сообщениями.

Однако, несмотря на это, нельзя недооценивать опасность мошенничества, совершаемого также в сети Интернет, поскольку, даже в отсутствие «голосового контакта» между преступником и жертвой, многообразие способов такого мошенничества часто позволяет достичь преступной цели в виде хищения денежных средств или иных объектов, принадлежащих потерпевшему. В числе наиболее часто применяемых в

информационно-телекоммуникационной сети Интернет способов совершения мошеннических действий следует выделить[1]:

1) фишинг, целью которого является получение преступником доступа к данным потерпевшего, имеющим конфиденциальный характер (например, паролям, кодам доступа к ресурсам интернет-банкинга, данных банковской карты, достаточных для совершения операций в Интернете, и так далее). При этом, фишинг объективно выражается не во взломе учетной записи, с целью хищения содержащихся в ней данных, а в получении их путем обмана потерпевшего, который, в результате воздействия на него фишера, самостоятельно сообщает указанные данные. Само же воздействие на потерпевшего оказывается посредством технических приемов, таких как массовая рассылка электронных писем, содержащих ссылку на поддельный сайт, внешне идентичный странице, принадлежащей популярном бренду, и отправляющий введенные на нем данные пользователя мошеннику;

2) скам, заключающийся в получении данных или денежных средств, принадлежащих потерпевшему, путем установления с ним личных отношений (например, посредством переписки в социальной сети), вхождения в доверие, и использование этого доверия для достижения преступного результата. Отличие данного способа от фишинга заключается в том, что скам предусматривает именно установление личной связи преступника с потерпевшим, а не использование технических приемов, вроде рассылок, что позволяет мошеннику применять психологические приемы при общении с жертвой преступления.

Помимо данных способов, в сети Интернет мошенники могут пользоваться и иными, однако именно два представленных варианта являются наиболее распространенными и эффективными с точки зрения преступника.

---

[1]Майтесян А.М. Мошенничество в сети интернет и способы защиты от него // Международный журнал гуманитарных и естественных наук. 2020. №5-4. С. 70.

Также, важной чертой рассматриваемой категории преступлений является ее высокая степень латентности, обусловленная тем, что многие потерпевшие, ставшие жертвами такого мошенничества, просто не обращаются за защитой в правоохранительные органы. Такое поведение может быть обусловлено как уверенностью в том, что преступление все равно не будет раскрыто, так и опасение лишних материальных и временных затрат, связанных с расследованием уголовного дела. При этом, сами мошенники, осознавая данный факт, часто намеренно действуют таким образом, чтобы жертва преступления не обращалась с заявлением о преступлении, например, путем хищения сумм, не являющихся крупными, поскольку, действительно, далеко не каждый человек обратится в полицию в случае хищения у него, например, трёх тысяч рублей.

Также, говоря о факторах, объединяющих все указанные и рассмотренные способы совершения мошеннических действий с использованием цифровых и телекоммуникационных технологий, стоит отметить, что все они, будучи непосредственно связанными с обманом потерпевшего, так или иначе, сопряжены с использованием, так называемых, «криминальных фикций».

Р.С. Белкин дал следующее определение криминальным фикциям – нечто, объективно не существующее, ложное, но выдаваемое за действительное[1]. Под этим подразумевается осуществление заведомо, в целях введения лица в заблуждение, используемое впоследствии для достижения преступного результата в виде, например, завладения денежными средствами потерпевшего.

Рассматривая криминальные фикции с точки зрения процесса осуществления преступной деятельности, такие авторы, как В.А. Образцов, Л.В. Бертовский и Н.Л. Бертовская полагают, что они представляют собой систему, включающую в себя определенные действия, направленные на

[1] Белкин Р.С. Криминалистическая энциклопедия / Р.С. Белкин. М.: Мегатрон XXI, 2000, С. 278.

реализацию мысленной модели, призванной дезинформировать лицо, в отношении которого она применяется. При этом, для такой реализации субъектом преступления создается некий искусственный объект (или изменяются свойства объекта естественного), посредством которого осуществляется противоправное психологическое воздействие на потерпевшего в целях введения его в заблуждение и навязывания ему ошибочных решений, в которых непосредственно заинтересован субъект преступления[1].

По мнению тех же авторов, криминальные фикции, в целом, применяемые при совершении преступления, можно подразделить на определенные подгруппы в зависимости от цели, на которую их использование непосредственно направлено[2]:

1) фикции, применяемые в процессе приготовления к совершению преступления. К данной подгруппе можно отнести, например, продумывание «легенды», которая будет использована для введения потерпевших в заблуждение, составление шаблонных текстов сообщений, содержащих подложные данные;

2) фикции, применяемые в качестве средства совершения преступного деяния. Данная подгруппа включает в себя, например, использование при разговоре с потерпевшим заранее изготовленных записей голоса, применение программного обеспечения, изменяющего голос говорящего, умышленное создание помех, в целях объяснения неразборчивых фрагментов речи или препятствования узнаванию голоса звонящего. Так, например, согласно Приговору Чулымского районного суда Новосибирской области от 20 марта 2015 г. по делу № 1-200/2014, осужденный искусственно искажал голос и

---

[1] Образцов В.А. Фикции в криминальной, оперативно-розыскной и следственной практике / В.А. Образцов, Л.В. Бертовский, Н.Л. Бертовская. М.: Юрлитинформ, 2011. С.75.
[2] Там же. С. 78-79.

создавал видимость помех в целях имитации вступления в разговор другого человека[1];

3) фикции, применяемые в целях сокрытия факта совершения преступления. К таким фикциям можно отнести, например, сообщение потерпевшему ложной информации о том, что его банковская карта, которая будто была заблокирована, после получения денежных средств автоматически разблокируется, что создает у потерпевшего впечатление о том, что его денежные средства были не похищены, а с необходимостью и обоснованно потрачены им для разблокирования карты;

4) фикции, применяемые для сокрытия данных о личности злоумышленника. К данной подгруппе можно отнести получение мошенником незарегистрированного абонентского номера или номера, зарегистрированного на другое лицо, использование устройств сотовой связи с измененным международным идентификатором мобильного оборудования (IMEI), а также использование компьютерного оборудования с динамическим IP-адресом, VPN-программ, прокси-серверов и т.д., что способствует усложнению идентификации злоумышленника;

5) фикции, направленные на достижение иных преступных целей.

Также, некоторыми учеными, в качестве отдельного предмета изучения выделяются способы, которыми осуществляется передача денежных средств или цифровых финансовых активов лицу, совершающему преступление, относящееся к рассматриваемой категории. Например, Р.Р. Гилязов выделяет следующие способы[2]:

1) оставление определенной суммы наличных денежных средств в месте, указанном злоумышленником;

---

[1] Приговор Чулымского районного суда Новосибирской области от 20 марта 2015 г. по делу № 1-200/2014. URL: https://sudact.ru/regular/doc/KrAcjzfvYNbJ/ (дата обращения 07.10.2020).

[2]Гилязов Р.Р. Способы совершения мошенничеств с использованием средств сотовой телефонной связи как элемент криминалистической характеристики // Евразийский юридический журнал. 2014. № 12. С. 167-169.

2) приобретение специализированных карт экспресс-оплаты услуг операторов сотовой связи и сообщение мошеннику уникального кода, указанного на них;

3) перевод денежных средств на абонентский счет используемого мошенником телефона;

4) перевод денежных средств на указанный мошенником номер банковского счета или карты, а также перевод, осуществляемый и использованием электронных кошельков, как в традиционном понимании, так и используемых для аккумулирования цифровых финансовых активов – криптовалют (например, биткоин-кошелек);

5) осуществление телефонного звонка на специальный номер, за звонок по которому автоматически осуществляется списание крупной суммы денежных средств с абонентского счета потерпевшего, или же переход по интернет-ссылке, указанной в полученном от мошенника сообщении, приводящий к аналогичному результату.

Таким образом, изучив способы, применяемые злоумышленниками, и так или иначе связанные с подготовкой, осуществлением и сокрытием мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий, можно заключить, что способ, как один из основных элементов криминалистической характеристики преступления, представляет собой сложную многоуровневую систему возможных моделей поведения лица, совершающего противоправное деяние. В свою очередь, фактически выбираемая в каждом индивидуальном случае комбинация конкретных способов, во многом, определяется иными элементами криминалистической характеристики – обстановкой совершения преступления и психофизиологическими особенностями личности, совершающей его.

Обращаясь к статистике МВД РФ[1], следует обратить внимание на процент выявления преступлений, совершаемых в электронной среде. Он составляет 98,6%, что значительно выше, чем процент выявления за 2018 и 2019 годы. Следовательно, криминалистика развивается в верном направлении, что позволяет без проблем выявлять «невидимые» следы преступлений 21 века. Так, при работе с электронными носителями информации криминалисты стали использовать технологии, позволяющие получить доступ к данным без модификации. Благодаря этому появляется возможность ознакомиться с содержащейся на носителях информацией без внесения изменений в ее целостность[2]. Для этого применяются специализированные комплексы, такие как UFED, XRY, позволяющие извлекать информацию из мобильных телефонов, карт памяти или иных устройств.

Информационно-аналитический комплекс «Мобильный криминалист» делает возможным не только выявление, но и анализ таких данных. Основными функциями данного комплекса программ, применительно к техническим устройствам является: создание логических образов устройств, работающих на базе операционных систем iOS, Android, WindowsPhone и других; извлечение и последующая расшифровка данных, содержащихся на устройстве, а также тех, что были удалены; работа с облачными хранилищами данных, такими как Viber, iCloud, Yandex и другие, с целью извлечения размещенных на них данных. Кроме того, «Мобильный криминалист» располагает необходимым набором инструментов, для высокоскоростного поиска данных как внутри всего уголовного дела, так и по тексту любого отдельно взятого документа, а также анализа получаемых с устройств данных, в том числе, с нескольких одновременно.

---

[1]Краткая статистика состояния преступности в Российской федерации за январь 2020 года. Официальный сайт МВД РФ. URL: https://мвд.рф/reports/item/19655871/ (дата обращения: 16.10.2020).

[2] Салихов Т.Ю. Поиск и изъятие электронных носителей информации // Совершенствование следственной деятельности в условиях информатизации: сборник материалов Международной научно-практической конференции, 2018. С. 289-290.

Особенности данного программного комплекса позволяют достижение следующих криминалистически значимых целей:

1) установить существование определенной связи между владельцем мобильного или иного технического устройства и контактами, зафиксированными в его памяти;

2) выстроить хронологическую последовательность событий, имеющих отношение к делу и произведенных с использованием устройства;

3) группировать собранные по делу доказательства в виде электронных следов и обеспечить их аккумулирование в одном месте;

4) осуществить поиск учетных данных, хранящихся в памяти устройства, и их извлечение;

5) использовать контекстный поиск - по ключевым словам, регулярно используемым сочетаниям слов, номерам телефонов и иным данным.

Однако, чтобы усложнить или сделать невозможным извлечение электронных следов, преступники разрабатывают средства защиты информации. Это могут быть всевозможные пароли, препятствующие деятельности государственных органов в выявлении следов преступления, поскольку доступ к информации на некоторых носителях без ввода пароля невозможен, даже при использовании передового оборудования. При этом, получение информации, защищенной таким образом, часто является необходимым для расследования преступления. Следовательно, криминалисты всегда должны быть на шаг впереди, и иметь представление о том, как возможно преодолеть различные средства защиты информации, содержащей в себе следы расследуемого деяния.

Так, например, пользовательская информация, находящаяся на мобильных устройствах на базе операционной системы iOS, часто защищается алгоритмом шифрования, под названием AES (AdvancedEncryptionStandard). Следовательно, знания о принципах работы данной системы могут помочь в дешифровании данных, защищенных таким образом.

Из упомянутого выше следует, что, в современных условиях технологического прогресса, расширяются требования не только к материально-техническому обеспечению криминалиста, в части аппаратного и программного обеспечения, но и к его собственной компетенции, ведь в список необходимых навыков, используемых в криминалистической деятельности, сегодня, входят и навыки программирования. Причем, требуемый уровень развития этих навыков непрерывно растет, поскольку усложняются, в частности и способы шифрования информации, представляющей решающее значение для расследования. Соответственно, существующие на сегодняшний день требования по техническому оснащению и уровню компетенции, хоть и актуальны сейчас, уже в ближайшее время устареют, что обуславливает необходимость устойчивого прогрессирующего движения в развитии соответствующих криминалистических положений и технических средств[1].

1.3 Цифровые финансовые активы, как предмет мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий

«Каждый день непрерывно происходит развитие экономической сферы, а именно ее модернизация. Появляются новые электронные способы обработки информации, платежа, банкинга и т.д.»[2] - такой точки зрения придерживаются Х.А. Ахматов и И.А. Панченко. По их мнению, такое

[1] Белкин Р.С. Криминалистическая энциклопедия. С. 264.
[2] Ахматов Х.А., Панченко И.А. Криптовалюта в Российской Федерации: позиция банка России // Сб. науч. тр. вузов России «Проблемы экономики, финансов и управления производством», 2017. № 41. С. 8-11.

развитие обусловлено движением к повышению удобства и снижению временных затрат.

Безусловно, трудно спорить с данным утверждением, поскольку действительно, появление новых оптимизированных способов управления финансовыми активами способствует тому, что на сегодняшний день, это управление может осуществляться лицом без существенных затрат времени и иных ресурсов, и вне зависимости от его местоположения.

Постепенный переход к использованию цифровой среды и телекоммуникационных сетей в управлении финансами, выражается различными способами. Так, уже привычными стали, так называемые, электронные деньги, широко используемые в самых разных целях. Электронные деньги могут аккумулироваться с помощью специальных средств, называемых электронными кошельками, среди которых наиболее популярными в России являются Qiwi, Яндекс.Деньги и Webmoney.

При этом, разумеется, удобство использования подобных средств имеет и определенную отрицательную сторону, которая выражается в том, что деньги, хранящиеся в электронном виде, потенциально могут стать предметом хищения, в том числе, путем мошенничества, значительно проще, чем деньги в традиционном понимании.

Так, например, создавая электронный кошелек в какой-либо платежной системе («Qiwi», «Яндекс.Деньги», «Webmoney» и т.д.), лицо не осознает, что уже в этот момент становится потенциальной «легкой добычей» для преступника, поскольку именно данные способы получения денежных средств злоумышленники используют наиболее часто. Удобство электронных кошельков, как способа получения денег мошенником объясняется тем, что, в отличие от, например, банковских карт, в электронных платежных системах отсутствует жесткая система идентификации лица, производящего операции по счету. Примером может послужить система «Qiwi», которая, хоть и требует указания паспортных данных для полноценного доступа к услугам по переводам и платежам, все

же, не защищена должным образом, поскольку в сети Интернет существует множество сайтов, предлагающих приобрести данные для авторизации в указанной платежной системе, с помощью учетной записи, к которой уже осуществлена привязка паспортных данных другого лица. Таким образом, приобретя такую учетную запись, мошенник далее не стеснен какими-либо ограничениями в действиях по электронному счету, и фактически не оставляет возможности отследить именно его.

Помимо данного удобства, успех мошеннических действий обеспечивается также тем, что мошенники, как правило, являются хорошими психологами, использующими соответствующие навыки в целях наиболее эффективного воздействия на собеседника и достижения своей цели в виде завладения его денежными средствами. Однако, стоит также отметить, что главной причиной успешности действий мошенников является именно невнимательность самих потерпевших или их недостаточная осведомленность о том, каким образом, теоретически, возможно дистанционно осуществить списание денежных средств с их счета. Именно излишняя доверчивость или неумение быстро ориентироваться в психологически некомфортной, стрессовой ситуации, которой успешно пользуются злоумышленники, приводит зачастую к значительным финансовым потерям со стороны потерпевшего. Исходя из этого, закономерно, что особенной опасности стать жертвой такого преступления всегда подвержены самые социально незащищенные категории лиц – несовершеннолетние и лица престарелого возраста.

Помимо указанных факторов, существенный рост количества преступлений, связанных с хищением денежных средств в информационном пространстве, очевидно, связан с пандемией COVID-19, поскольку большое количество людей было вынуждено, находясь дома, перевести свою деятельность в цифровую среду. Так, согласно статистике состояния преступности за 2020 год, количество зарегистрированных преступлений, совершенных с использованием сети «Интернет», составило 300337, что на

91,3% больше количества аналогичных преступлений, совершенных в 2019 году. Кроме того, стоит отметить, что более 80% данных преступлений составляют кражи и мошенничества[1].

Предметом мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий, в обычном понимании, являются денежные средства, поскольку передача иных предметов потерпевшим преступнику дистанционным образом существенно затруднена. Учитывая специфику исследуемого вида преступлений, деньги преступник получает в электронном, безналичном виде.

Однако на сегодняшний день, помимо ставших уже привычными электронных денег, существует и развивается такое сравнительно новое явление, как криптовалюта, правовая природа которой в законодательстве многих стран, включая Россию, на данный момент, не определена.

В соответствии с действующим законодательством, приравнивание криптовалюты к деньгам невозможно, поскольку, в частности, согласно ч.1 ст.75 Конституции Российской Федерации, «Денежной единицей в Российской Федерации является рубль. Денежная эмиссия осуществляется исключительно Центральным банком Российской Федерации. Введение и эмиссия других денег в Российской Федерации не допускаются»[2]. Из этого следует, что признание криптовалют на территории России в качестве денежных единиц, являлось бы прямым нарушением конституционного положения.

Со стороны Центрального банка России, Росфинмониторинга, а также ряда депутатов Государственной думы, поступали предложения о введении полного запрета в отношении каких-либо операций с криптовалютами, от

---

[1] Краткая статистика состояния преступности в Российской федерации за январь-декабрь 2020 года. Официальный сайт МВД РФ. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 28.01.2021).

[2] Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г.) // Официальный интернет-портал правовой информации. 2020. URL: http://www.pravo.gov.ru/ (дата обращения 10.10.2020).

выпуска, до использования в качестве платежного средства. Однако такая позиция широко критиковалась различными экспертами в сфере цифровых прав. И действительно, в случае установления такого запрета, данный шаг можно было бы назвать попыткой отрицать очевидное, поскольку криптовалюта, так или иначе, постепенно входит в мировую практику экономического оборота, в связи с чем, вместо запретительных мер, конструктивными действиями представляется установление полноценного правового регулирования данного объекта.

Шагом в направлении к установлению правового режима в отношении криптовалют в России, стало принятие 31 июля 2020 года Федерального закона № 259 «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»[1]. На первый взгляд, представляется, что в данном законе должно содержаться легализованное понятие криптовалюты, однако, при детальном изучении законодательного текста, обнаруживается, что данный термин был заменен на «цифровые финансовые активы и цифровая валюта».

Так, согласно части 2 статьи 1 данного закона, под цифровыми финансовыми активами понимаются «цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном настоящим Федеральным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы».

[1] Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 г. № 259-ФЗ // СЗ РФ. 2020. №31. Ст. 5018.

Понятие цифровых финансовых активов, само по себе, включает следующие виды:

1) цифровые ценные бумаги – активы, подтверждающие определенные права обладателя, своего рода аналоги традиционных ценных бумаг, но выраженные в виде цифровой записи в информационной системе. Оборот финансовых активов, относящихся к данному виду, осуществляется в соответствии с законодательством, регулирующим рынок ценных бумаг;

2) криптовалюта – активы, используемые в качестве предмета купли-продажи, а равно средства накопления или обмена на различные товары или услуги, то есть выполняющие функции денег в традиционном их понимании;

3) цифровые знаки – вид цифровых активов, не относящихся ни к одному их вышеуказанных, и подтверждающих права владельца в отношении договоров гражданско-правового характера.

Решение законодателя о замене в нормативном тексте устоявшегося в употреблении термина «криптовалюта» новыми категориями – «цифровые финансовые активы» и «цифровая валюта» - представляется неоправданным и малоэффективным, поскольку таким образом лишь создается потенциальная возможность к появлению ненужных разночтений в отношении терминологии[1].

Относительно места цифровых финансовых активов в системе гражданского оборота, можно отметить, например, то, что согласно пункту 18 статьи 3 Федерального закона «О национальной платежной системе»[2] они не могут быть отождествлены с электронными денежными средствами. В то же время, Федеральным законом от 18 марта 2019 года №34[3] в Гражданский

---

[1] Ситник А.А. Цифровые валюты: проблемы правового регулирования // Актуальные проблемы российского права. 2020. №11. С. 105. URL: https://cyberleninka.ru/article/n/tsifrovye-valyuty-problemy-pravovogo-regulirovaniya (датаобращения: 30.01.2021).

[2] Федеральный закон «О национальной платежной системе» от 27 июня 2011 г. № 161-ФЗ // СЗ РФ. 2011. №27. Ст. 3872.

[3] Федеральный закон «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» от 18 марта 2019 г. № 34-ФЗ // СЗ РФ. 2019. №12. Ст. 1224.

кодекс РФ были внесены изменения, согласно которым, так называемые, цифровые права были отнесены к «иному имуществу», участвующему в гражданском обороте.

Таким образом, несмотря на то, что полноценного и системного регулирования криптовалюты в российском законодательстве, на данный момент, нет, можно отметить положительную динамику изменений в указанной сфере.

При этом, одновременно с признанием положительных сторон, связанных с введением криптовалют в оборот и их «популяризацией», существует и обратная сторона, связанная с тем, что повышение частоты использования данного объекта закономерно повышает вероятность его применения в целях совершения тех или иных преступлений.

Пригодность криптовалюты для совершения преступлений, а, следовательно, и то, что она вызывает интерес со стороны преступников, объясняется рядом особенностей, присущих данному объекту, благодаря его технологической природе. Среди таких особенностей можно выделить:

1) анонимность, обеспечиваемая благодаря использованию различных методов криптографии (шифрования) и систем распределенного реестра (блокчейн-технологий). Это обстоятельство существенно затрудняет фактическую идентификацию лица, совершающего преступление с использованием криптовалюты. Вместе с тем, проведение транзакций посредством использования систем распределенного реестра, оставляет определенный цифровой след, который позволяет восстановить историю произведенных операций и определить, таким образом, лицо, которое данные операции совершило;

2) транснациональность, заключающаяся в том, что в отношении операций с использованием криптовалюты невозможно установить какие-либо границы, будь то государственные или таможенные. Благодаря данной особенности, криптовалюты являются потенциально привлекательными для

совершения трансграничных преступлений и, как следствие, для лиц, связанных с международными преступными сообществами;

3) существование криптовалюты исключительно в сети «Интернет» и, как следствие, ее приспособленность для данной сети и совершения в ней различных операций. При этом, благодаря такой приспособленности, криптовалюта может широко использоваться (и используется фактически) при расчетах в теневом сегменте Интернета – так называемом, «Даркнете» - для проведения операций по оплате незаконных товаров или услуг, например, наркотиков;

4) открытость блокчейна для хранения различных данных, приводящая в возможности внесения в него различных вредоносных программ, посредством использования которых злоумышленники могут получать доступ к персональной информации пользователей и даже осуществлять списание денежных средств[1].

Также, учитывая то, что криптовалюты существуют в информационно-телекоммуникационной сети «Интернет», и используются в ней же, закономерно, что и преступления, элементом криминалистической модели которых являются цифровые финансовые активы, также совершаются в данной сети.

Исходя из этого, стоит отметить ряд особенностей, характеризующих преступления, совершаемые в цифровом пространстве сети «Интернет»[2]:

1) высокая степень скрытности совершаемых преступных деяний, объясняемая спецификой цифрового пространства, позволяющего использовать различные средства анонимизации, шифрования данных и т.д.;

---

[1] Сидоренко Э.Л. Криминологические риски оборота криптовалюты // Экономика. Налоги. Право. 2017. № 6. С. 151.

[2]Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. №24. С. 46-47. URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 30.01.2021).

2) дистанционный характер совершаемого преступления, в том числе, подразумевающий возможность нахождения преступника на территории другого государства, относительно жертвы преступления;

3) динамическое развитие цифровой среды, благодаря которому постоянно появляются новые и изменяются старые способы возможного совершения преступлений с использованием цифровых и телекоммуникационных технологий, включая мошенничество, в криминалистической модели которого, в качестве одно из элементов, присутствуют цифровые финансовые активы;

4) особенности цифровых и телекоммуникационных технологий, позволяющие автоматизировать процесс совершения преступлений, в результате чего само происходит множество однотипных эпизодов совершения того или иного преступного посягательства, даже без прямого участия злоумышленника в каждом из этих эпизодов;

5) такой элемент состава мошенничества, как обман или злоупотребление доверием, во взаимодействии с дистанционным и анонимным характером преступлений, совершаемых с использованием цифровых и телекоммуникационных технологий, существенно повышают степень латентности данных преступлений, что также затрудняет обнаружение и дальнейшее расследование указанных преступных действий.

Благодаря перечисленным выше особенностям, присущим цифровым финансовым активам, и чертам, характерным для преступлений (в частности, мошенничеств), совершаемых с использованием цифровых и телекоммуникационных технологий, сами цифровые финансовые активы, рассматриваемые в качестве элемента криминалистической характеристики преступления, могут выступать в двух качествах:

1) в качестве средства совершения преступления – например, использоваться для оплаты незаконного товара;

2) в качестве предмета преступления – например, в случае хищения криптовалюты, в том числе, путем совершения мошеннических действий.

Первая из указанных возможностей обеспечивается, в первую очередь, за счёт анонимности криптовалют, благодаря чему преступнику представляется, что, если он использует данный способ оплаты при финансовых операциях, сущность которых находится вне закона, его будет невозможно отследить и он, таким образом, избежит ответственности.

Характерными примерами, в данном случае, выступает оплата оружия, наркотиков, и иных запрещенных уголовным законом товаров или услуг, распространение которых осуществляется в «Даркнете». Также, криптовалюта может выступать в качестве средства совершения преступлений, связанных с террористической деятельностью, например, ее финансирования (часть 1.1 статьи 205.1 Уголовного кодекса РФ).

Еще одним направлением возможного применения цифровых финансовых активов в качестве средства совершения преступления, является легализация имущества, приобретенного незаконным образом (статьи 174 и 174.1 Уголовного кодекса РФ), при которых действия лица заключаются в приобретении криптовалюты за счет незаконно полученных средств, после чего данные активы через обменные биржи «трансформируются» в деньги, в привычном понимании этого слова, имеющие объяснимый источник.

Таким образом, говоря о цифровых финансовых активах, как о средстве совершения преступления, стоит отметить, что они могут использоваться либо для непосредственной оплаты того или иного объекта, ограниченного в обороте или полностью изъятого, либо для облегчения совершения преступления, как в случае с легализацией денежных средств, полученных преступным путем[1].

Говоря о цифровых финансовых активах, как предмете преступлений, совершаемых с использованием цифровых и телекоммуникационных технологий, наибольший интерес, как с точки зрения объекта исследования в данной работе, так и с позиции наибольшей актуальности, на сегодняшний

[1] Коренная А.А., Тыдыкова Н.В. Криптовалюта как предмет и средство совершения преступлений // Всероссийский криминологический журнал. 2019. №3. С. 411-412.

день, представляют именно хищения, в частности, совершаемые в форме мошенничества.

Безусловно, расширение круга участников оборота криптовалют приводит и к повышению количества совершаемых в данной сфере хищений. Так, многими авторами отмечается наметившаяся в последние годы устойчивая тенденция к существенному росту числа преступлений, связанных с хищениями цифровых финансовых активов[1].

В связи со специфической природой криптовалюты, и отсутствия полноценного системного регулирования ее правовой сущности в российском пространстве, открытым, до сих пор, является вопрос о том, возможно ли вообще признание криптовалюты предметом хищений. Определенные шаги по направлению к разрешению этого спора были сделаны, посредством внесения упомянутых выше изменений в Гражданский кодекс РФ, предусматривающих отнесение цифровых прав к «иному имуществу».

Однако, несмотря на это, дискуссии продолжаются. Основным «камнем преткновения» является то, что, согласно традиционному пониманию, предмет хищения должен быть так или иначе материально выражен в объективной действительности. В данном ключе, отличие криптовалюты от, например, безналичных денег, заключается в том, что безналичные денежные средства, хранящиеся, например, в кошельке системы Qiwi, все же, имеют реальное материальное обеспечение в виде денежных знаков соответствующей валюты. Криптовалюта же такого материального обеспечения не имеет, поскольку она сама существует лишь в цифровом пространстве и появление новых ее единиц обеспечивается не эмиссией в классическом ее понимании, а совокупностью вычислительных мощностей технических устройств, задействованных в, так называемом, «майнинге».

---

[1] Сидоренко Э.Л. Криминальное использование криптовалюты: международные оценки. URL:http://lexandbusiness.ru/view-article.php?id=8675 (дата обращения 01.02.2021).

При этом, например, А.В. Хабаров в своих работах уже длительное время назад выразил позицию, согласно которой предметом преступного посягательства может быть любое имущество, признаваемое таковым гражданским законодательством, если уголовный закон не содержит специального изъятия в отношении конкретного вида имущества[1]. То есть, если руководствоваться данной точкой зрения, получается, что внесенные в Гражданский кодекс РФ изменений должно было поставить точку в вопросе, можно ли признавать криптовалюту предметом хищений.

Но в то же время, существуют и противники такого подхода. Так, например, Н. Шатихина отмечает, что действующее в России на данный момент уголовное право под предметом хищения понимает именно «овеществленное» имущество, то есть выраженное в материальном объекте, а следовательно, криптовалюта не может считаться предметом преступлений, связанных с хищением, в том числе, в форме мошенничества[2]. Схожей позиции придерживается и В.В. Хилюта, указывая на то, что криптовалюта не может выступать в качестве предмета хищений, поскольку признание ее таким предметом приведет к распаду всей системы преступлений против собственности, из-за того, что сама криптовалюта существенно отличается по своей природе от других, традиционных, предметов таких преступлений[3].

При безусловном признании аргументированности обеих позиций, нам представляется, что современные реалии, когда цифровые технологии в общем, и цифровые финансовые активы в частности, внедряются в самые различные сферы человеческой деятельности, отрицание возможности считать их предметом хищений может не только быть неконструктивным, но

---

[1] Хабаров А.В. Преступления против собственности: влияние гражданско-правового регулирования: автореф. дис. ... канд. юрид. наук. Тюмень, 1999. С. 10-11.

[2] Шатихина Н. Несколько ремарок к вопросу о криптовалюте как предмете хищения URL:https://zakon.ru/blog/2017/10/18/neskolko_remarok_k_voprosu_o_kriptovalyute_kak_predmete_hischeniya (дата обращения 02.02.2021).

[3] Хилюта В.В. Криптовалюта как предмет хищения (или к вопросу о переформатировании предмета преступлений против собственности) // Библиотека уголовного права и криминологии. 2018. № 2. С. 67-68.

и принести существенный вред общественному порядку, безопасности, и отношениям собственности. Вероятно, стоит отойти от привычного, материального понимания предмета хищений, поскольку к этому, фактически, обязывает окружающая действительность, в которой отношения собственности складываются отнюдь не только вокруг материальных объектов, а порой, фактическая экономическая ценность цифровых финансовых активов, похищенных у собственника, кратно превосходит ценность иного, материального, имущества данного лица.

Учитывая легкость обращения криптовалют в специализированных системах в сети «Интернет», совершение в отношении них хищений, в первую очередь, в форме мошеннических действий, представляется преступлением, не отличающимся особой сложностью для преступника, по сравнению с иными мошенническими действиями, совершаемыми с использованием цифровых и телекоммуникационных технологий, однако способным причинить потерпевшему очень существенный материальный вред.

Стоит отметить также, что несмотря на специфическую природу криптовалюты, способы, с которыми мошенники воздействуют на потенциальную жертву преступления с целью завладеть принадлежащими ей цифровыми финансовыми активами, с сущностной точки зрения, не отличаются от тех способов, которые применяются при мошенничестве в отношении традиционных денег, совершаемом в цифровом пространстве или пространстве телекоммуникационных систем.

Наиболее распространенными примерами мошеннических действий в отношении криптовалюты являются случаи, когда некое лицо, предоставляющее в цифровом пространстве услуги, схожие с банковскими, и аккумулирует у себя определенное количество криптовалюты различных пользователей, присваивает данные средства и просто исчезает, после чего выявить данное лицо становится очень затруднительно, учитывая

анонимность криптовалюты и используемые в цифровом пространстве методы шифрования данных.

Если же подходить к вопросу о подобных преступлениях с точки зрения отрицания возможности криптовалют быть предметом хищения, получится, что подобные действия злоумышленников нельзя будет соответствующим образом квалифицировать, из-за отсутствия состава преступления, и, следовательно, эти лица избегут ответственности, несмотря на то, что их действия причинили реальный ущерб потерпевшему лицу.

Таким образом, нам представляется, что предмет хищения необходимо понимать в широком смысле и относить к нему любое имущество, которое признано таковым гражданским законодательством России. Только так возможно избежать существенного отставания нормативной правовой базы от современных технологических реалий. Следовательно, цифровые финансовые активы могут выступать в качестве элемента криминалистической модели преступлений, совершаемых с использованием цифровых и телекоммуникационных технологий в общем, а в частности, применительно к такому преступлению, как мошенничество, они являются предметом, на который направлено преступное посягательство злоумышленника.

2 ОСОБЕННОСТИ ПРОВЕРКИ СООБЩЕНИЯ О ПРЕСТУПЛЕНИИ И ТАКТИКИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА, СОВЕРШАЕМОГО С ИСПОЛЬЗОВАНИЕМ ЦИФРОВЫХ И ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

2.1 Обстоятельства, подлежащие установлению в ходе проверки информации о совершении мошенничества с использованием цифровых и телекоммуникационных технологий

Уровень кибермошенничества сегодня, к сожалению, растет. Прошедший 2020 год связан с пандемией и соответствующим реагированием мирового сообщества на сложившуюся ситуацию, а также со значительным ростом киберпреступности в мире и России. По ряду признаков сегодня можно утверждать, что именно благодаря пандемии «сложилась» новая преступная отрасль, которая имеет место на территории Российской Федерации или вблизи ее границ, и непосредственно угрожает самому государству и гражданам[1]. Такие выводы делает заместитель председателя правления Сбербанка Станислав Кузнецов. Учитывая то, что услугами Сбербанка пользуется значительная часть граждан России, за счет чего он оперирует огромными объемами данных, включая финансовые, и, следовательно, отмечаемые его руководством проблемы имеют, так или иначе, глобальный характер, и затрагивают практически каждого.

Также, согласно словам Кузнецова, на данный момент, примерно каждый 11 звонок является либо попыткой мошенников, либо автоматизированным спамом. Следовательно, количество таких «атак» в отношении граждан является внушительным. Вместе с тем, особенности, присущие как самому мошенничеству в общем, так и его проявлению в

[1] Сбербанк заявил о росте кибермошенничества в 2020 году в два раза. URL: https://1prime.ru/finance/20201201/832469386.html (дата обращения 28.03.2021).

цифровом пространстве, определяют данный вид преступлений, как латентный, поскольку далеко не каждая жертва обмана, получившая в его результате определенный материальный ущерб, поймет, что в отношении нее было совершено преступление. Кроме того, на эту особенность мошенничества накладываются такие характеристики преступлений, совершаемых с использованием цифровых и телекоммуникационных технологий, как дистанционность и анонимность, обеспечиваемые способами взаимодействия преступника и жертвы через сеть. И третьим фактором, способствующим высокой степени латентности изучаемого вида преступлений, является то, что далеко не каждая жертва телефонного или интернет-мошенничества, даже осознавая, что в отношении нее было совершено преступное действие, обратиться с соответствующим заявлением в правоохранительные органы. В первую очередь, это касается случаев, когда материальный ущерб не является крупным для потерпевшего, что, условиях низкой, в среднем, правовой грамотности населения, и сложившегося мнения о том, что правоохранительные органы работают недостаточно эффективно и не смогут раскрыть такое преступление, приводит к мысли, что обращение с заявлением приведет лишь к волоките и трате времени, а не к достижению результата в виде восстановления справедливости.

Вышеуказанные факторы оказывают существенное влияние не только на сложность расследования и разрешения уголовных дел о мошенничествах, совершаемых с использованием цифровых и телекоммуникационных технологий. Даже стадия возбуждения уголовных дел по таким преступлениям имеет свою специфику, обеспечиваемую теми же обстоятельствами.

По мнению аналитиковGroup-IB, в настоящее время, в сфере мошенничества с использованием цифровых и телекоммуникационных технологий, наблюдается основной тренд по персонализации применяемых в целях хищения инструментов, а также таргетирование совершаемых атак. Таким образом, не только повышается эффективность мошеннический

действий, за счет их «индивидуального» обращения к конкретному потерпевшему, но и затрудняется работа по обнаружению и выявлению совершаемого преступления и самого преступника[1].

В частности, мошенники используют индивидуальные ссылки, содержание которых отображается только одному пользователю, рассылку личных сообщений в социальных сетях и мессенджерах, а также мошеннические сайты, передающие введенные на них данные пользователя преступнику и сохраняющие их для последующего автоматического заполнения форм на следующих этапах мошенничества.

В этой связи, важным является вопрос о предмете доказывания, или, выражаясь в принятой в Уголовно-процессуальном законодательстве России терминологии, обстоятельствах, подлежащих доказыванию при расследовании и разрешении уголовного дела. В общем виде, перечень этих обстоятельств содержится в статье 73 Уголовно-процессуального кодекса России[2]. Вместе с тем, дискуссионным является вопрос о том, является ли указанный перечень характерным для уголовного процесса на всех его стадиях. При прямом толковании текста данной статьи, можно сделать вывод, что предмет доказывания является идентичным на всем протяжении производства по уголовному делу.

Однако, существует и иное мнение, согласно которому предмет доказывания на различных стадиях процесса отличается количеством обстоятельств, которые необходимо установить, и «глубиной» их исследования[3].

При сравнении данных точек зрения, представляется, что вторая в большей степени отражает реальное положение вещей и в целом, задачи уголовного процесса. Наличие определенной разницы в предмете

---

[1]Group-IB: 59% онлайн-мошенничества приходятся на социальные сети. URL: https://www.anti-malware.ru/news/2021-01-27-111332/34844 (дата обращения 28.03.2021).

[2] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СЗ РФ. 2001. № 52. Ст. 4921.

[3] Арсеньев В.Д. Доказывание фактических обстоятельств в отдельных стадиях советского уголовного процесса // Труды Иркутского университета. 1969. Т.45, вып.8, ч.4. С.77.

доказывания между различными стадиями дает основания для разграничения стадий между собой, поскольку то, какие обстоятельства необходимо установить на каждой стадии процесса, обусловлено целями и задачами этой стадии.

Так, исходя из данного подхода, для принятия процессуального решения о возбуждении уголовного дела, необходимо установить данные, на основании которых может быть сделан положительный вывод о том, что само преступление, фактически, имело место[1].

Следовательно, говоря о стадии возбуждения уголовного дела, хотя законом прямо и не предусмотрен предмет доказывания, характерный для нее, круг устанавливаемых обстоятельств можно вывести из статьи 140 Уголовно-процессуального кодекса РФ, согласно смыслу которой, для возбуждения уголовного дела необходимо наличие повода и основания. Исходя из этого, можно заключить, что установление наличия данных обстоятельств и входит в предмет доказывания на данной стадии.

При этом, ряд авторов, определяя предмет доказывания на стадии возбуждения уголовного дела, ограничивает его только этими двумя обстоятельствами, полагая, что, исходя из толкования норм уголовно-процессуального законодательства, наличия легального повода и выявленного основания для возбуждения дела достаточно[2].

Представлена в науке уголовного процесса и другая точка зрения относительно предмета доказывания на данной стадии. Ее представители полагают, что помимо указанных выше обстоятельств, необходимо также установить наличие или отсутствие оснований для отказа в возбуждении уголовного дела[3]. Однако, анализ законодательного текста позволяет усомниться в правильности такого подхода, поскольку, согласно части

---

[1] Алексанова К.С. Особенности предмета и пределов доказывания в стадии возбуждения уголовного дела // Ростовский научный журнал. 2018. № 4. С. 65-71.

[2] Ведищев Н.П. Новый закон: новые проблемы у адвокатов // Адвокат. 2013. № 9. С. 14.

[3] Быков Л.А. Законность возбуждения уголовного дела / В кн.: Возбуждение уголовного дела: учебно-методические материалы / Л.А. Быков, Н.В. Маслов, В.И. Ремнев. // Красноярский государственный университет. Красноярск, 2000. С. 69.

первой статьи 148 Уголовно-процессуального кодекса РФ, отказ в возбуждении уголовного дела возможен, при условии отсутствия оснований для возбуждения дела. Следовательно, установление наличия основания для возбуждения производства, автоматически означает и установление отсутствия оснований для отказа в таком решении, и наоборот. Таким образом, выделение такого третьего элемента предмета доказывания на стадии возбуждения уголовного дела, фактически, дублирует другой его элемент.

Модификация способов совершения различных преступлений, включая мошенничество, обусловленное ростом уровня технологий и их повсеместным внедрением, закономерно влечет формирование тенденции к изменению поведения потенциальных жертв преступления в цифровой сфере. Безусловно, каждое частное лицо стремится максимально обезопасить себя от возможных посягательств со стороны злоумышленника, предпринимая, для этого, различные меры, в зависимости от уровня своих возможностей. Так, например, 8 декабря 2020 года, пресс-служба банка «Тинькофф» сообщила, что банком, совместно с крупнейшими мобильными операторами России: «Tele2», «Мегафон» и «МТС» - была запущена система, направленная на предотвращение совершения мошеннических действий в отношении клиентов, посредством телефонных звонков. Принцип действия данной системы заключается в постоянном обмене информацией между банком и операторами сотовой связи. Так, в момент звонка происходит автоматическая синхронизация данных, позволяющая определить подозрительного участника разговора, сведения о котором отправляются в банк для последующей проверки.

Однако, как отмечалось ранее, меры, предпринимаемые конкретными лицами в целях собственной защиты, существенно различаются, в зависимости от технических, а также финансовых возможностей данного лица, в связи с чем, физическое лицо не в состоянии эффективно предупреждать совершение в отношении себя мошеннических действий с

использованием цифровых и телекоммуникационных технологий, и противодействовать им. Следовательно, помимо персональных мер защиты, необходимы также меры публичного характера, то есть исходящие от государства.

В частности, среди таких мер можно выделить формирование новых специализированных подходов, применяемых компетентными органами и лицами при расследовании преступлений, совершаемых в цифровой среде.

Как было нами отмечено выше, при рассмотрении способов совершения мошенничества при использовании цифровых и телекоммуникационных технологий, эти способы имеют определенную специфику, существенно осложняющую деятельность правоохранительных органов, направленную на обнаружение и дальнейшее расследование таких преступлений. В числе подобных особенностей, в первую очередь, выделяется то, что личность преступника в значительной мере скрыта и находится вне досягаемости, благодаря использованию злоумышленником различных технологий переадресации (VPN, динамический IP-адрес, прокси-сервера, Sim-карты, зарегистрированные на другое лицо, или не зарегистрированные вообще). Также, само цифровое пространство подвержено постоянным изменениям, что способствует возможности для динамического совершенствования способов преступных посягательств.

Вместе с тем, помимо названных черт, характеризующих преступность, отметить стоит и существование способов, позволяющих, посредством использования цифровых технологий, автоматизировать преступные действия, начиная от рассылки SMS-сообщений, и заканчивая созданием вредоносного программного обеспечения, в автоматическом порядке похищающего данные пользователя, включая, вероятно, информацию о его банковских счетах, паролях и количестве располагаемых денежных средств.

Кроме того, ведение противоправной деятельности в сетевом пространстве располагает к созданию преступных групп разной степени устойчивости, которые характеризуются, зачастую, отсутствием четко

определенного лидера и разделения ролей между соучастниками, а также большой территориальной удаленностью членов группы друг от друга.

Все названные особенности, присущие таким преступлениям, как мошенничество с использованием цифровых и телекоммуникационных технологий, обуславливают, в общем, выраженную специфику механизма совершения преступного посягательства, который, в свою очередь, определяет и тактику производства следственных действий уполномоченными лицами, при ведении расследования по уголовному делу.

В целях наиболее полного понимания специфики обстоятельств, подлежащих установлению на стадии возбуждения уголовного дела в отношении мошенничеств, совершаемых с использованием цифровых и телекоммуникационных технологий, целесообразно провести анализ каждого из них по отдельности.

Так, говоря о поводе к возбуждению уголовного дела, в первую очередь, стоит отметить, что повод, в понимании уголовно-процессуального закона, представляет собой юридический факт, возникновение которого влечет появление у уполномоченных лиц обязанности принять предоставленную информацию о преступлении, проверить ее, с точки зрения достоверности и наличия оснований к возбуждению дела, и, впоследствии, принять соответствующее процессуальное решение. Данные признаки повода к возбуждению уголовного дела отражают его процессуальную сущность.

С точки зрения материальной природы, по мнению Н.Е. Павлова, поводы к возбуждению уголовного дела представляют собой определенные источники информации о каком-либо преступном деянии[1]. При этом, согласно точке зрения данного автора, такой источник информации становится поводом, в полноценном смысле, только, после того, как поступившая информация подвергается процессуальному оформлению, регистрации, и проверке.

---

[1] Павлов Н.Е. Производство по заявлениям, сообщениям о преступлениях: учебное пособие / Н.Е. Павлов. Волгоград, 1980. С. 10.

Легальный перечень поводов для возбуждения уголовного дела закреплен в части 1 статьи 140 Уголовно-процессуального кодекса РФ. Данный перечень, по своей форме, является закрытым, однако, например, В.Е. Козлов, говоря об особенностях, присущих преступлениям, связанным с использованием цифровых и телекоммуникационных технологий, предложил несколько расширенный перечень поводов, при наличии которых возможно начало проверки поступившей информации[1]. По его мнению, к таким поводам относятся:

1) заявление о преступлении, полученное от:

- должностного лица какого-либо учреждения, предприятия или организации;

- физического лица;

2) сообщение о преступлении, источником которого являются сведения, полученные иными способами:

- при непосредственном обнаружении уполномоченными органами или должностными лицами сведений, свидетельствующих о наличии признаков того или иного преступления;

- при проведении проверки полученной из оперативных источников информации об уже совершенном, либо только готовящемся преступлении, связанном с использованием цифровых и телекоммуникационных технологий;

- при проведении различных мероприятий оперативно-розыскного характера;

- по результатам контрольно-ревизионных проверок;

- при задержании с поличным лица, совершившего преступление;

- при обнаружении признаков преступления, совершенного с использованием цифровых и телекоммуникационных технологий, в ходе уголовного производства по делам об иных преступлениях;

---

[1] Козлов В.Е. Теория и практика борьбы с компьютерной преступностью: справочное издание / В.Е. Козлов. М., 2002. С. 76.

- из информации, источником которой являются средства массовой информации.

Ссылаясь на результаты собственного исследования, В.В. Коломинов указывает, что «в подавляющем большинстве случаев, поводом для возбуждения уголовных дел в отношении мошенничеств, совершенных с использованием цифровых и телекоммуникационных технологий, выступает заявление потерпевшего лица – доля таких случаев в общем числе возбужденных уголовных дел по данной категории преступлений составляет 80%. 15% подобных уголовных дел возбуждается на основании информации, выявленной, в том или ином виде, сотрудниками правоохранительных органов, а оставшиеся 5% приходятся на такой повод, как получение сведений о преступлении из средств массовой информации»[1].

Как следует из приведенных данных, такой повод для возбуждения уголовного дела, как явка преступника с повинной, не является характерным. Это положение объясняется высокой степенью латентности данной категории преступлений, и сравнительно сложным процессом идентификации лица, совершившего противоправное деяние.

Помимо повода, для возбуждения уголовного дела, согласно действующему законодательству, необходимо наличие основания, которое, в соответствии с положением части 2 статьи 140 Уголовно-процессуального кодекса РФ, представляет собой совокупность достаточных данных, свидетельствующих о признаках преступления. По мнению ряда авторов, основание включает в себя две составляющие: материальную и процессуальную.

Так, материальной стороной является наличие таких признаков преступления, как общественная опасность и противоправный характер. При этом, стоит отметить, что общественная опасность является признаком, не

[1]Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 88.

входящим в понятие состава преступления, в то время, как противоправный характер, напротив, подразумевает, что совершенное деяние нарушает какой-либо из уголовно-правовых запретов, то есть попадает под действие одной из статей Особенной части Уголовного кодекса РФ.

При установлении наличия противоправного характера деяния, основополагающую роль играет выявление таких элементов состава преступления, как объект и объективная сторона. Так, в случае с мошенничеством, совершаемым с использованием цифровых и телекоммуникационных технологий, необходимо установить наличие объекта хищения, которым могут выступать денежные средства или цифровые финансовые активы, а также факта наличия деяния, в результате совершения которого данный объект был похищен злоумышленником у владельца.

Процессуальную сторону основания возбуждения уголовного дела составляет категория «достаточные данные», закрепленная в части 1 статьи 140 Уголовно-процессуального кодекса РФ, указывающие на обозначенные выше признаки преступления. В широком смысле, исходя из анализа норм, «достаточные данные» выступают в качестве критерия принятия многих процессуальных решений, таких как, например, решение о производстве обыска (ч. 1 ст. 182 УПК РФ), привлечения лица в качестве обвиняемого (ч. 1 ст. 171 УПК РФ). В каждом конкретном случае вопрос о достаточности данных для возбуждения уголовного дела разрешается компетентным должностным лицом по своему внутреннему убеждению с учетом всей совокупности собранных доказательств (ч. 1 ст. 17 УПК РФ)[1].

После получения повода для возбуждения уголовного дела, в целях выявления предусмотренного основания, необходимо проведение предварительной проверки, в соответствии с положениями статьи 144 Уголовно-процессуального кодекса РФ. При этом, учитывая специфику

[1] Барсуков Е.А., Белоусов И.В. Предмет доказывания в стадии возбуждения уголовного дела // Центральный научный вестник. 2017. № 11. С. 40-41.

мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий, определяется также и специфика проверочных действий.

Субъекту, производящему предварительную проверку, частью 1 статьи 144 Уголовно-процессуального кодекса РФ предоставлено право производить достаточно большое количество специфических действий, как самостоятельно, так и привлекая к их производству специалиста, обладающего определенным набором специальных знаний.

Действия уполномоченного субъекта, во многом определяются тем, от кого получена информация о совершенном преступлении. Таким субъектом, сообщающим эти сведения, может быть, как физическое лицо, так и представитель юридического лица или публично-правового образования. Учитывая, что коллективные субъекты оперируют гораздо большим объемом данных, чем физические лица, для проверки сообщения о мошенничестве, совершенном в отношении них, необходимо произвести большее количество проверочных действий. В частности, это может быть получение объяснений от всех сотрудников, в целях выявления сведений, которыми они обладают, а также проверки возможной причастности данных лиц к преступлению. Также целесообразно истребование документов, требование о проведении документальных проверок, в ходе которых могут быть обнаружены данные, свидетельствующие о совершенном преступлении.

Однако, согласно исследованиям В.В. Коломинова, лишь 26% уголовных дел о мошенничествах, совершаемых с использованием цифровых и телекоммуникационных технологий, возбуждаются по заявлению представителей юридических лиц, из чего следует, что подавляющее большинство таких преступлений совершается в отношении физических лиц.

Закономерно, что при получении сведений о преступлении от физического лица, количество возможных проверочных действий снижено[1].

Специфика проведения предварительной проверки по данной категории преступлений обусловлена особенностями способа совершения мошенничества с использованием цифровых и телекоммуникационных технологий, а также применяемыми преступником средствами. Так, учитывая дистанционный характер совершения мошеннических действий, прямой контакт злоумышленника с жертвой исключен в любом случае, из-за чего выявить субъекта совершения преступления становится более затруднительно, чем в случае с мошенничествами, совершаемыми «традиционными» способами.

Первоочередным действием, которое необходимо произвести, в целях проверки сообщения о совершенном преступлении, относящемся к исследуемой категории, является получение объяснений от лица, потерпевшего от данного преступного деяния. Учитывая скрытый характер как мошенничества в общем, так и совершаемого с использованием цифровых технологий, именно эти объяснения выступают, на стадии возбуждения уголовного дела, основным источником информации о признаках преступления и условиях, которые могли способствовать его совершению.

Существенное влияние на производимые проверочные действия оказывает также сложившаяся на момент проведения этой проверки ситуация, касающаяся характера взаимоотношений между преступником и жертвой преступления. Типичными, в этой связи, являются две ситуации:

1) совершение преступлений в отношении данного потерпевшего еще не окончено, или же имеет место повторяющиеся преступные действия. В этом случае, между злоумышленником и жертвой сохраняется определенная

---

[1]Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. С. 88.

связь, благодаря которой процесс выявления личности преступника становится потенциально проще для уполномоченных органов. Однако, такие случаи составляют лишь около 20% от всех мошенничеств, совершаемых в цифровой среде;

2) преступление в отношении данного потерпевшего полностью совершено, и связь между ним и злоумышленником отсутствует. В таком случае, выявить преступника становится сложнее, поскольку нет возможности каким-либо образом выйти с ним на связь.

Таким образом, на стадии возбуждения уголовного дела в отношении мошенничества, совершенного с использованием цифровых и телекоммуникационных технологий, установлению подлежат, в первую очередь, наличие повода для принятия решения о возбуждении дела, а также основания, в целях выявления которого необходимо производство предварительной проверки. В ходе выполнения проверочных действий должны быть обнаружены такие признаки преступления, как общественная опасность и противоправный характер, включающий в себя объективные элементы состава преступления. Учитывая специфику исследуемого вида преступлений, для установления данных обстоятельств целесообразно получать объяснения от потерпевших лиц, истребовать документы, при их наличии, а также производить осмотр технических средств, посредством использования которых было совершено преступное посягательство. Данные осмотры, в целях получения наибольшего количества значимой информации, стоит производить с привлечением специалистов в области работы с такими средствами. Также, не исключены случаи, когда для получения достаточной информации, целесообразно назначить производство экспертизы технического устройства (компьютера, телефона и т.д.).

2.2 Особенности производства отдельных следственных действий на первоначальном этапе расследования мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий

При расследовании мошенничества, совершенного с использованием цифровых и телекоммуникационных технологий, и, особенно, на его первоначальном этапе, вовсе не каждое из возможных следственных действий может привести к благоприятному, с точки зрения следствия, результату. Более того, перечень таких следственных действий, пусть и не является исчерпывающим, сравнительно невелик, что обуславливается спецификой самого преступления, относящегося к рассматриваемому виду. Конкретной причиной, в этой связи, можно назвать крайне малое количество информации о преступлении, которой располагают уполномоченные лица в начале расследования, что объясняется латентным характером мошенничества. Кроме того, следует учесть и ограниченность числа способов, которыми, потенциально, можно эту информацию получить, что является следствием дистанционного характера совершения преступления, практически не оставляющего материальных следов.

Основываясь на этом, можно выделить следующие следственные действия, производство которых на первоначальном этапе расследования мошенничества с использованием цифровых и телекоммуникационных технологий является наиболее желательным и эффективным:

1) допрос потерпевшего лица, свидетелей (при их наличии) и подозреваемого или обвиняемого (при условии его обнаружения);

2) осмотр места происшествия и технических устройств, посредством которых было совершено преступное посягательство;

3) различные виды экспертиз.

Каждое из приведенных следственных действий имеет свою специфику производства, определяемую характерными чертами исследуемого преступления. Данные специфические черты будут рассмотрены в данном параграфе.

Говоря о специфике расследования данного вида мошенничества, помимо особенностей, касающихся отдельных следственных действий,

безусловно, необходимо также отметить лицо, непосредственно производящее расследование, то есть следователя или дознавателя. Выполняющее следственные действия в отношении «компьютерного» или «телефонного» мошенничества уполномоченное лицо должно обладать соответствующей компетенцией в данной сфере, то есть иметь реальное представление о том, какие особенности могут характеризовать такие преступные действия и, следовательно, способствовать установлению личности преступника и раскрытию преступления. Этот факт, как и то, что сетевая преступность становится более распространенной, как в абсолютных цифрах, так и в отношении к другим видам преступлений, обуславливает необходимость как можно более массового формирования у сотрудников правоохранительных органов компетенций в цифровой сфере и навыков практической работы в ней.

На данный момент, наиболее ярким примером профессиональных в изучаемой области кадров в структуре правоохранительных органов, является специализированное Управление «К» Министерства внутренних дел России, в число задач которого входит выявление, пресечение, раскрытие и предупреждение мошенничества в сфере компьютерной информации[1]. Однако, нельзя, сегодня, с уверенностью сказать, что каждый следователь правоохранительных органов обладает в достаточной степени необходимыми знаниями и навыками, которые могут позволить наиболее эффективно вести расследование по уголовным делам, связанным с совершением мошенничества с использованием цифровых и телекоммуникационных технологий. Данный факт обостряет вопрос, связанный с необходимостью привлечения следователем или лицом, производящим дознание, специалиста, обладающего соответствующими знаниями, для осуществления следственных действий.

---

[1] Управление «К» МВД России. Сайт МВД РФ. URL: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (дата обращения: 11.02.2021)

Определяя особенности, присущие следственным действиям, производимым при расследовании преступлений, связанных с использованием технологических средств, в число которых входит также и исследуемый вид мошенничества, Е.С. Шевченко отмечает, что для вербальных действий в ходе расследования, помимо указанного выше привлечения специалиста или использования собственных специальных знаний следователя, характерно[1]:

1) специфическое определение содержания допроса;

2) сравнительно малое количество времени, необходимое преступнику для того, чтобы скрыться или иными способами затруднить продвижение расследования, благодаря динамичности цифрового пространства;

3) возможность использования субъектами, производящими расследования, ресурсов, предоставляемых цифровыми и телекоммуникационными технологиями, включая ресурсы сети «Интернет».

Что касается невербальных следственных действий, безусловно, для них также характерны определенные особенности, такие как:

1) необходимость наличия жесткой логики в выстроенной последовательности применения специальных знаний в такой узкой сфере, как выявление и изъятие следов, оставленных преступником в цифровой среде;

2) невозможность конструирования единого универсального набора действий, выполнение которых надлежащим образом могло бы гарантировать положительный результат расследования. Благодаря способности телекоммуникационных сетей к динамичному изменению, на практике может складываться огромное количество разнообразных следственных ситуаций, похожих друг на друга лишь отчасти, в следствие чего лицу, производящему расследование, в каждой такой ситуации

[1] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. … канд. юрид. наук. М., 2012. С. 10-11.

необходимо применять методы индуктивной логики и, таким образом, определять свои действия;

3) обязательное применение в ходе расследования специализированных технико-криминалистических средств, способствующих выявлению виртуальных следов преступления.

Необходимо также отметить, что важную роль в определении необходимых к первоочередному производству следственных действий, а также их наиболее эффективной последовательности, играет проведенная на стадии возбуждения уголовного дела по факту «цифрового» или «телефонного» мошенничества предварительная проверка, в ходе которой уполномоченный субъект получается первоначальное ориентирующее понимание общей следственной ситуации.

Учитывая характер и особенности способа совершения мошенничества с использованием цифровых и телекоммуникационных технологий, на первоначальной стадии проведения расследования, наиболее вероятно, что одним из крайне небольшого количества источников значимой информации является лицо, в отношении которого данное преступление было совершено. Следовательно, представляется, что в первую очередь необходимо провести допрос данного лица, с целью получения и легального закрепления его показаний в качестве доказательства по уголовному делу.

Однако, перед допросом должна быть проведена серьезная подготовительная работа, основной целью которой является выяснение степени «погруженности» допрашиваемого лица в сферу цифровых технологий, навыка их использования и уровня владения специальной терминологией. Безусловно, что решающую роль при подготовке допроса играет взаимодействие следователя со специалистом в данной области, и исключением из этого правила может быть только ситуация, в которой следователь сам обладает достаточным уровнем специальных знаний и опыта практической работы по расследованию схожих преступлений.

Вместе с тем, Н.Н. Егоров указывает, что в случае, если допрашиваемое лицо очень хорошо разбирается в технической стороне использования цифровых и телекоммуникационных технологий, а также имеет существенный опыт работы с ними, к участию в допросе целесообразно непосредственно привлечь специалиста, присутствие которого поспособствует созданию более комфортной для допрашиваемого ситуации, в которой он сможет беспрепятственно сообщить информацию, содержащую большое количество специфических терминов или технических деталей[1].

При этом, допрос, касающийся такого специфического преступления, имеет ряд особенностей с точки зрения содержания и поставленных задач, из которых закономерно проистекает набор задаваемых вопросов. В частности, в ходе допроса необходимо установить следующие обстоятельства[2]:

1) способ, который был использован злоумышленником для связи с потерпевшим лицом: телефонный звонок, SMS-сообщение, рассылка электронных писем, переписка в социальных сетях и т.д.;

2) уровень владения потерпевшим лицом техническими устройствами, посредством использования которых было совершено преступление;

3) информация об установленном на техническом устройстве программном обеспечении;

4) номер телефона, электронный адрес, ссылка, с которых преступник выходил на связь с жертвой преступления;

5) время установления контакта между преступником и потерпевшим;

6) когда и как потерпевший узнал о совершенном в отношении него мошенничестве;

7) содержание действий, которые, по словам злоумышленника, необходимо было совершить жертве преступления;

---

[1]Егоров Н.Н. Вещественные доказательства: уголовно-процессуальный и криминалистический аспекты / Н.Н. Егоров. М.: Юрлитинформ, 2007. С. 197.

[2] Никулина О.А. Расследование мошенничества с использованием мобильной связи // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2019. № 1. С. 59.

8) количество денежных средств или цифровых финансовых активов, которые преступник требовал передать, а также мотивация данной передачи, то есть те действия, за совершение которых, по словам злоумышленника, происходит оплата;

9) способ передачи объекта преступления: банковский перевод, перечисление единиц криптовалюты на специализированный виртуальный кошелек, звонок по указанному номеру, переход по ссылке и т.д.;

10) описание лица, в том объеме, в котором допрашиваемое лицо владеет соответствующей информацией.

Помимо допроса, определенные особенности при расследовании мошенничества, совершенного с использованием цифровых и телекоммуникационных технологий, существуют также в иных следственных действиях. Так, в числе первых, при ведении предварительного следствия, необходимо производство осмотра места происшествия. Специфика данного мероприятия обусловлена тем, что, в отличие от преступлений, совершаемых «традиционными» способами, такое мошенничество не оставляет материальных следов, вместо которых уполномоченный субъект должен взаимодействовать со следами виртуальными. В отличие от допроса, данное следственное действие является невербальным, то есть использующим иные способы познания значимой информации[1].

Учитывая особенности механизма совершения преступления и природы оставляемых им следов, список объектов производимого осмотра существенно отличается от традиционного принятого, включающего в себя исключительно материальные объекты, находящиеся в конкретном помещении или на местности, и содержит[2]:

---

[1]Россинский С.Б. Результаты «невербальных» следственных и судебных действий как вид доказательств по уголовному делу. М.: Юрлитинформ, 2015. С. 153.

[2] Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. …докт. юрид. наук. Воронеж, 2001. С. 15-16.

1) помещение, в котором непосредственно расположено техническое устройство, посредством использования которого злоумышленником было совершено преступное посягательство;

2) само техническое устройство (компьютер, мобильный телефон), использованное для совершения преступления и хищения принадлежащих потерпевшему денежных средств или цифровых активов, а также установленные на нем программы;

3) каналы передачи информации между потерпевшим и преступником – переписка в социальной сети или мессенджере, звонки с использованием сотовой сети или компьютерных приложений и т.д.;

4) устройства, предназначенные для хранения цифровой информации – карты памяти, диски и т.д.;

5) сама цифровая информация, обнаруженная как на компьютере или мобильном телефоне, так и на устройствах ее хранения.

Помимо осмотра места происшествия, важным следственным действием, применяемым при производстве расследования по уголовному делу о мошенничестве с использованием цифровых и телекоммуникационных технологий, является экспертиза (например, компьютерная).

Как и при расследовании любого преступления, время, затрачиваемое на получение необходимой информации, играет одну из решающих ролей в обеспечении успеха в виде окончательного раскрытия совершенного деяния. Следовательно, при производстве процессуальных действий необходимо стремиться к достижению искомого результата в минимальные сроки. Проведение экспертизы в отношении обнаруженных объектов, содержащих в себе виртуальные следы преступления или иную важную для следствия информацию, направлено именно на достижение данной цели. Значимым качеством, отличающим экспертизу от осмотра или иных следственных действий, является заведомо более высокий уровень профессионально компетенции производящего ее лица, за счет чего обеспечивается

возможность более детального познания объекта и обнаружения содержащихся в нем следов, указывающих на лицо, совершившее преступление, или иные существенные обстоятельства[1].

Принципиально важным для следствия является исследование технически сложных устройств и информации, находящейся в их памяти. Так, например, на сегодняшний день, исследование данных, содержащихся в памяти мобильного телефона, позволяет не только обнаружить данные о звонках или поступающих и отправленных сообщениях, но и установить место нахождения лица в определенный момент времени, что также может поспособствовать обнаружению данного лица и установлению личности преступника.

Помимо обозначенных и, в целом, привычных следственных действий, при расследовании мошенничества, совершенного при использовании цифрового пространства, представляется целесообразным использование самим следствием ресурсов, предоставляемых этим пространством. Так, в частности, в целях получения информации о преступлении, в отношении которого ведется деятельность уполномоченных лиц, порой, имеет смысл изучить данные, содержащиеся, например, в социальных сетях, через которые злоумышленник может выходить на связь с потенциальной жертвой преступления, или просто получать о ней информацию, которая позднее будет им использована при взаимодействии с ней через иные каналы связи.

Исходя из обозначенного выше, необходимо указать, что особенности, свойственные следственным действиям, производимым при расследовании преступлений, совершенных с использованием цифровых и телекоммуникационных технологий, обусловлены, в первую очередь, спецификой механизма совершения таких преступлений и природой оставляемых им следов. Представляется, что эффективность деятельности

[1]Пропастин С.В. Осмотр или судебная экспертиза: выбор в пограничных ситуациях (на примере обнаружения и исследования компьютерной информации) // Современное право. 2013. № 6. С. 131.

следователя по подобным уголовным делам, находится в прямой зависимости от компетентности данного лица в сфере цифровых технологий, из чего следует, что в условиях повышения количества киберпреступлений, необходимым является повышение квалификации сотрудников правоохранительных органов в указанной сфере.

Таким образом, при учете совокупности всех факторов, обуславливающих отличия изучаемого вида преступлений от иных видов, лицо, ведущее расследование, должно, в первую очередь, грамотно и ответственно подойти к составлению плана своих дальнейших действий, чтобы избежать возможной потери виртуальных следов из-за небрежно произведенного мероприятия. При планировании как отдельного следственного действия, так и всего расследования в целом, в виду его специфики, целесообразно обращаться к лицам, обладающим специальными знаниями в данной сфере, чтобы предусмотреть максимально возможное количество деталей и не упустить существенных обстоятельств. Также, необходимо обратить внимание на то, что важную роль в определении плана расследования играет первоначальная проверка поступившей информации о преступлении, из чего следует, что проведение данной проверки также должно быть вдумчивым, что позволит на начальной стадии определить направление и общие черты будущих действий.

ЗАКЛЮЧЕНИЕ

Такие преступления, как мошенничество, совершаемое с использованием средств цифровых и телекоммуникационных технологий, являются весьма распространенными в современном мире, что обусловлено повсеместной распространенностью данных технологий и устройств, позволяющих использовать их, производя определенные действия в цифровой среде.

Будучи безусловно полезными в повседневной жизни, с одной стороны, цифровые технологии и телекоммуникационные сети также являются потенциально удобным средством для тайного или открытого хищения денежных средств, при отсутствии физического контакта между преступником и жертвой преступления. В свою очередь, отсутствие этого контакта способно существенно затруднить и внести особую специфику в процесс расследования данного преступления, что и объясняет необходимость всестороннего анализа таких мошеннических действий с позиции криминалистики.

Только полноценное изучение и систематизация полученных данных об элементах криминалистической характеристики преступлений, относящихся к данному типу, позволит в достаточной мере повысить эффективность подхода к работе лиц, расследующих сходные преступления, в будущем.

Проведенное при подготовке данной выпускной квалификационной работы исследование позволяет сделать следующие выводы:

1) проведенный анализ криминалистического моделирования в целом, криминалистической модели мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий в частности, а также отдельных элементов, составляющих эту модель, позволяют подчеркнуть, в первую очередь, существенную значимость метода моделирования при расследовании и раскрытии преступлений, относящихся

к изучаемой категории. Структурированное изучение сведений о типичных элементах криминалистической характеристики таких преступлений, совершенных в прошлом, повысит эффективность расследования сходных по родовым признакам преступлений в будущем. Кроме того, безусловно, все элементы, составляющие указанную криминалистическую характеристику, находятся в тесной и непосредственной взаимосвязи друг с другом, и их изучение должно носить системный характер, учитывающий особенности каждого из элементов и их взаимозависимостей;

2) способ совершения преступления, являясь одним из основных элементов криминалистической характеристики, представляет собой сложную систему, включающую несколько различных по содержанию групп возможных моделей поведения субъекта, на различных стадиях преступления. Применительно к мошенничеству с использованием цифровых и телекоммуникационных технологий, именно способ является элементом, наиболее ярко характеризующим специфику данной категории преступлений, по сравнению с иными сходными категориями. Способ совершения преступления в каждой конкретной криминальной ситуации представляет собой определенную комбинацию различных действий, выбор которых зависит от иных элементов криминалистической характеристики преступления – психофизиологических особенностей личности преступника и обстановки преступного деяния. Изучение и структурирование наиболее типичных способов совершения таких преступлений, при выявлении закономерности выбираемого преступником способа в зависимости от иных обстоятельств конкретного преступного деяния, позволит также существенно повысить эффективность работы органов расследования;

3) традиционно, под предметом мошенничества, совершаемого при использовании цифровых и телекоммуникационных технологий, понимаются денежные средства, пусть представленные в безналичном виде на банковском счете или электронном кошельке, но все же, обеспеченные денежными знаками в материальном понимании. Вместе с тем, динамичное

развитие общества, имеющее место благодаря развитию цифровых технологий, требует соответствующего развития законодательной базы. Так, на сегодняшний день, в разных государствах все шире применяется, криптовалюта, являющаяся принципиально новым, относительно традиционных денег, явлением, попытки урегулировать которое в России привели к появлению юридического термина «цифровые финансовые активы», включенные в перечень имущества в гражданско-правовом смысле. Учитывая это, а также тот факт, что хищение цифровых финансовых активов мошенническим способом, может принести существенный материальный вред, представляется, что данный вид имущества также должен быть безоговорочно включен в список возможных предметов преступления, относящегося к исследуемой категории;

4) мошенничество, совершаемое с использованием цифровых и телекоммуникационных технологий, имеет существенную специфику, относительно преступлений, совершаемых «традиционными» способами, не только в разрезе криминалистического изучения, но и в ходе производства по уголовному делу о таком мошенничестве, на различных его стадиях. Так, на стадии возбуждения уголовного дела, при проведении предварительной проверки, необходимо, в первую очередь, установить реальное наличие основания для принятия соответствующего процессуального решения. При этом, учитывая особенности преступлений, относящихся к изучаемой категории, позволяющие относить их к преступлениям с высокой степенью латентности, проведение предварительной проверки зачастую имеет решающее значение, поскольку дает уполномоченному лицу ориентирующее представление о сложившейся ситуации. Проводя предварительную проверку, следует, в первую очередь, обратить внимание на объяснения потерпевшего лица, и осмотреть технические устройства, использованные при совершении деяния. К производству данных действий надлежит привлекать специалиста, обладающего необходимыми знаниями в области цифровых технологий;

5) закономерно, что определенные особенности характерны и для следственных действий, производимых после возбуждения уголовного дела по факту мошенничества, совершенного с использованием цифровых и телекоммуникационных технологий. В частности, эти особенности, наиболее ярко проявляются на первоначальном этапе расследования. Они (особенности) напрямую обусловлены специфическим механизмом совершения преступления, не подразумевающим прямого контакта между преступником и потерпевшим, а также особенной природой оставляемых таким деянием следов, являющихся, по большей части, не материальными, а виртуальными отображениями преступления и личности, совершившей его. Качественное взаимодействие следствия с такими следами возможно только при наличии у следователя соответствующих компетенций, связанных с цифровой сферой, или же при условии постоянного участия в следственных действиях специалиста в данной области. В противном случае, учитывая неустойчивость и неочевидность виртуальных следов, они могут быть либо упущены, либо и вовсе безвозвратно утеряны, что приведет к невозможности получить необходимую доказательственную информацию. С точки же зрения производства вербальных следственных действий, первостепенное значение имеет допрос потерпевшего лица и преступника, в случае быстрого выявления его личности. Это обусловлено фактическим отсутствием очевидных для сторонних лиц проявлений совершенного мошенничества. При этом, тактика производства допроса напрямую зависит от уровня владения цифровыми технологиями допрашиваемым лицом, наличия у него практических навыков и знаний в сфере функционирования виртуального пространства. Подготовка к такому допросу, а в ряде случаев, и само производство данного следственного действия, требует консультативного участия лица, обладающего специальными знаниями.

Исходя из перечисленного, стоит заключить, что для мошенничества, совершаемого с использованием цифровых и телекоммуникационных технологий, характерны существенные особенности, как с точки зрения

анализа криминалистической характеристики данного вида преступлений, так и для производимым по соответствующим делам расследования. Учитывая все существующие специфические черты, очевидно, что максимизация эффективности борьбы с такими преступлениями возможна только при непрерывном и системном изучении характерных для них элементов, структурировании получаемой информации, а также повышения квалификации сотрудников правоохранительных органов в сфере цифровых технологий, поскольку только при условии наличия у сотрудника необходимых знаний и навыков, возможно достижение позитивного результата, подразумевающего раскрытое преступление.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

РАЗДЕЛ I НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ И ИНЫЕ ОФИЦИАЛЬНЫЕ АКТЫ

1 Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г.) // Официальный интернет-портал правовой информации. 2020. URL: http://www.pravo.gov.ru/ (дата обращения 28.01.2021).

2 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СЗ РФ. 2001. № 52. Ст. 4921.

3 Федеральный закон «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» от 31 июля 2020 г. № 259-ФЗ // СЗ РФ. 2020. №31. Ст. 5018.

4 Федеральный закон «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» от 18 марта 2019 г. № 34-ФЗ // СЗ РФ. 2019. №12. С. 1224.

5 Федеральный закон «О национальной платежной системе» от 27 июня 2011 г. № 161-ФЗ // СЗ РФ. 2011. №27. Ст. 3872.

РАЗДЕЛ II ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1 Group-IB: 59% онлайн-мошенничества приходятся на социальные сети. URL: https://www.anti-malware.ru/news/2021-01-27-111332/34844 (дата обращения 28.03.2021).

2 Аверьянова, Т.В. Криминалистика: учебник. Том I / Т.В. Аверьянова, И.В. Александров, А.И. Бастрыкин и др. / под общ. ред. А.И. Бастрыкина. М.: Изд-во Экзамен, 2014. 511 с.

3 Алексанова, К.С. Особенности предмета и пределов доказывания в стадии возбуждения уголовного дела / К.С. Алексанова // Ростовский научный журнал. 2018. № 4. С. 65-71.

4 Арсеньев, В.Д. Доказывание фактических обстоятельств в отдельных стадиях советского уголовного процесса / В.Д. Арсеньев // Труды Иркутского университета. 1969. Т.45, вып.8, ч.4. С. 77.

5 Астишина, Т.В. Проблемы расследования преступлений, связанных с мошенническими действиями, совершенных с использованием средств сотовой телефонной связи / Т.В. Астишина, Е.В. Маркелова // Вестник Казанского юридического института МВД России. 2014. №2. С. 94-98.

6 Ахматов, Х.А.Криптовалюта в Российской Федерации: позиция банка России / Х.А. Ахматов, И.А. Панченко // Сб. науч. тр. вузов России «Проблемы экономики, финансов и управления производством». 2017. № 41. С. 8-11.

7 Барсуков, Е.А. Предмет доказывания в стадии возбуждения уголовного дела / Е.А. Барсуков, И.В. Белоусов // Центральный научный вестник. 2017. № 11. С. 39-41.

8 Бахин, В.П. Криминалистическая характеристика преступлений как элемент расследования / В.П. Бахин // Вестник криминалистики. 2000. № 1. 56 с.

9 Белкин, Р.С. Криминалистическая энциклопедия / Р.С. Белкин. М.: Мегатрон XXI, 2000. 334 с.

10 Белкин, Р.С. Курс криминалистики. В 3–х т. Т. 3 / Р.С. Белкин. М.: Юристъ, 1997. 480 с.

11 Бессонов, А.А. Способ преступления как элемент его криминалистической характеристики / А.А. Бессонов // Пробелы в российском законодательстве. 2014. №4. С. 171-173.

12 Бойцов, Ю.М. Проблемы проверки, выявления и раскрытия мошенничества с использованием мобильных средств связи / Ю.М.

Бойцов // Вестник Санкт-Петербургского Университета МВД. 2016. № 2. С. 107-112.

13 Бутенко, О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия / О.С. Бутенко // LexRussica. 2017. № 4. С. 49-60.

14 Быков, Л.А. Законность возбуждения уголовного дела / В кн.: Возбуждение уголовного дела: учебно-методические материалы / Л.А. Быков, Н.В. Маслов, В.И. Ремнев. // Красноярский государственный университет. Красноярск, 2000. 259 с.

15 В МВД созданы подразделения по борьбе с IT-преступлениями. IZ.RU Сайт газеты Известия. URL: https://iz.ru/973398/2020-02-07/v-mvd-sozdany-podrazd (дата обращения: 15.10.2020).

16 Ведищев, Н.П. Новый закон: новые проблемы у адвокатов / Н.П. Ведищев // Адвокат. 2013. № 9. С. 13-16.

17 Винокуров, С.И. Криминалистическая характеристика преступления, ее содержание и роль в построении методики расследования / С.И. Винокуров // Методика расследования преступлений. Общие положения: Материалы научно-практической конференции. М., 1976. С 101-104.

18 Гавло, В.К. Судебно-следственные ситуации: психолого-криминалистические аспекты: монография / В.К. Гавло, В.Е. Клочко, Д.В. Ким. Барнаул: Издательство Алтайского университета, 2006. 226 с.

19 Гилязов, Р.Р. Способы совершения мошенничеств с использованием средств сотовой телефонной связи как элемент криминалистической характеристики / Р.Р. Гилязов // Евразийский юридический журнал. 2014. № 12. С. 167–169.

20 Денисов, С.Л. Понятие «Криминалистическая характеристика преступления» / С.Л. Денисов // Гуманитарные, социально-экономические и общественные науки. 2015. №5. С. 67-69.

21 Егоров, Н.Н. Вещественные доказательства: уголовно-процессуальный и криминалистический аспекты / Н.Н. Егоров. М.: Юрлитинформ, 2007. 304 с.

22 Ермолович, В.Ф. Криминалистическая характеристика преступлений / В.Ф. Ермолович. Минск: Амалфея, 2001. 279 с.

23 Жукова, Н.А. Расследование и раскрытие преступлений, совершенных посредством sms-сообщений: метод. указания / Н.А. Жукова, Ю.А. Ковтун и др. М.: ДГСК МВД России, 2014. 40 с.

24 Журкина, О.В. К вопросу о способах совершения мошенничества с использованием сотовой (подвижной) связи / О.В. Журкина, И.В. Бондаренко // Вопросы российского и международного права. 2015. № 3 - 4. С. 19-30.

25 Зуйков, Г.Г. Криминалистическое учение о способе совершения преступления: автореф. дис. … докт. юрид. наук. / Г.Г. Зуйков. М., 1970. 31 с.

26 Карепанов, Н.В.Некоторые вопросы выявления и исследования следов преступлений / Н.В. Карепанов // Российское право: Образование. Практика. Наука. 2019. №3. С. 49-60.

27 Козлов, В.Е. Теория и практика борьбы с компьютерной преступностью: справочное издание / В.Е. Козлов. М., 2002. 336 с.

28 Колесниченко, А.Н. Общие положения методики расследования отдельных видов преступлений / А.Н. Колесниченко. Харьков, 1965. 170 с.

29 Коломинов, В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. / В.В. Коломинов. Иркутск, 2017. 211 с.

30 Коренная, А.А. Криптовалюта как предмет и средство совершения преступлений / А.А. Коренная, Н.В. Тыдыкова // Всероссийский криминологический журнал. 2019. №3. С. 408-415.

31 Краткая статистика состояния преступности в Российской федерации за январь 2020 года. Официальный сайт МВД РФ. URL: https://мвд.рф/reports/item/19655871/ (дата обращения: 16.10.2020).

32 Краткая статистика состояния преступности в Российской федерации за январь-декабрь 2020 года. Официальный сайт МВД РФ. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 28.01.2021).

33 Кудрявцев, В.Н.Объективная сторона преступления: монография / В.Н. Кудрявцев. М., 1960. 245 с.

34 Лабутин, А.А. «Мобильные» мошенничества: основные способы совершения / А.А. Лабутин // Вестник Казанского юридического института МВД России. 2013. № 12. С. 50-55.

35 Литвинов, Н.Д.Особенности, причины и тенденции развития дистанционного мошенничества лицами, отбывающими наказание в местах лишения свободы / Н.Д. Литвинов, А.Н. Федоров // Научно-исследовательские публикации. 2015. №13. С. 63-72.

36 Литвинов, Н.Д. Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения / Н.Д. Литвинов, А.Н. Федоров // JSRP. 2015. №12. С. 73-80.

37 Лоер, В. Криминалистика: учебник / В. Лоер. М. 2000. 129 с.

38 Лозовский, Д.Н. Особенности расследования преступлений, совершенных путем смс-сообщений / Д.Н. Лозовский, И.Р. Ульянова // Гуманитарные, социально-экономические и общественные науки. 2016. № 12. С. 144-147.

39 Майтесян, А.М.Мошенничество в сети интернет и способы защиты от него / А.М. Майтесян // Международный журнал гуманитарных и естественных наук. 2020. №5-4. С. 69-70.

40 Машлякевич, В.А. К вопросу о структуре и содержании криминалистической характеристики мошенничеств, совершаемых с использованием средств телефонной связи / В.А. Машлякевич // Алтайский юридический вестник. 2016. № 14. С. 102-106.

41 Мещеряков, В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. …докт. юрид. наук. / В.А. Мещеряков. Воронеж, 2001. 387 с.

42 Никулина, О.А. Расследование мошенничества с использованием мобильной связи / О.А. Никулина // Преступность в сфере информационных и телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений. 2019. № 1. С. 57-61.

43 Номоконов, В.А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропина // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 45-55.

44 Образцов, В.А.Фикции в криминальной, оперативно-розыскной и следственной практике / В.А. Образцов, Л.В. Бертовский, Н.Л Бертовская. М.: Юрлитинформ, 2011. 408 с.

45 Павлов, Н.Е. Производство по заявлениям, сообщениям о преступлениях: учебное пособие / Н.Е. Павлов. Волгоград. 1980. 56 с.

46 Пропастин, С.В. Осмотр или судебная экспертиза: выбор в пограничных ситуациях (на примере обнаружения и исследования компьютерной информации) / С.В. Пропастин // Современное право. 2013. № 6. С. 129 - 132.

47 Россинский, С.Б.Результаты «невербальных» следственных и судебных действий как вид доказательств по уголовному делу / С.Б. Россинский М.: Юрлитинформ, 2015. 224 с.

48 Салихов, Т.Ю.Поиск и изъятие электронных носителей информации / Т.Ю. Салихов // Совершенствование следственной деятельности в условиях информатизации: сборник материалов Международной научно-практической конференции, 2018. С. 287-292.

49 Сбербанк заявил о росте кибермошенничества в 2020 году в два раза. URL: https://1prime.ru/finance/20201201/832469386.html (дата обращения 28.03.2021).

50 Сидоренко, Э.Л. Криминологические риски оборота криптовалюты / Э.Л. Сидоренко // Экономика. Налоги. Право. 2017. № 6. С. 147-154.

51 Сидренко, Э.Л. Криминальное использование криптовалюты: международные оценки. URL: http://lexandbusiness.ru/view-article.php?id=8675 (дата обращения 01.02.2021).

52 Ситник, А.А.Цифровые валюты: проблемы правового регулирования / А.А. Ситник // Актуальные проблемы российского права. 2020. №11. С. 103-113.

53 Три года тюрьмы за телефонное мошенничество. URL: https://ribalych.ru/2016/03/24/tri-goda-tyurmy-za-telefonnoe-moshennichestvo/ (дата обращения 28.09.2020).

54 Управление «К» МВД России. Сайт МВД РФ. URL: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (датаобращения: 11.02.2021).

55 Хабаров, А.В. Преступления против собственности: влияние гражданско-правового регулирования: автореф. дис. ... канд. юрид. наук. / А.В. Хабаров. Тюмень, 1999. 24 с.

56 Хилюта, В.В. Криптовалюта как предмет хищения (или к вопросу о переформатировании предмета преступлений против собственности) / В.В. Хилюта // Библиотека уголовного права и криминологии. 2018. № 2. С. 58-68.

57 Шаевич, А.А. Об особенностях некоторых элементов криминалистической характеристики мошенничеств, совершаемых с использованием средств мобильной связи / А.А. Шаевич, В.А. Родивилина // В сборнике: Актуальные проблемы науки и практики. сборник научных трудов. Хабаровск, 2018. С. 447-451.

58 Шатихина, Н. Несколько ремарок к вопросу о криптовалюте как предмете хищения URL: https://zakon.ru/blog/2017/10/18/neskolko_remarok_k_voprosu_o_kriptovalyute_kak_predmete_hischeniya (дата обращения 02.02.2021).

59 Шебалин, А.В. Расследование хищений средств сотовой связи: дис. … канд. юрид. наук. / А.В. Шебалин. Томск, 2010. 224 с.

60 Шевченко, Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. … канд. юрид. наук. / Е.С. Шевченко. М., 2012. 29 с.

РАЗДЕЛ III ПОСТАНОВЛЕНИЯ ВЫСШИХ СУДЕБНЫХ ИНСТАНЦИЙИ МАТЕРИАЛЫ СУДЕБНОЙ ПРАКТИКИ

1 Приговор Кудымкарского городского суда Пермского края от 17 января 2014 года по делу № 1-10/2014. URL: https://sudact.ru/regular/doc/L5zD7vIBXl5O/ (дата обращения 06.10.2020).

2 Приговор Чулымского районного суда Новосибирской области от 20 марта 2015 г. по делу № 1-200/2014. URL: https://sudact.ru/regular/doc/KrAcjzfvYNbJ/ (дата обращения 07.10.2020).

3 Приговор Промышленного районного суда города Самары от 13 февраля 2019 года по делу № 1-10/2019. URL: https://sudact.ru/regular/doc/qnhprHQxwRLQ/ (дата обращения 06.10.2020).

4 Приговор Волжского районного суда Самарской области от 14 января 2020 г. по делу № 1-242/2019. URL: https://sudact.ru/regular/doc/cPdsiyJgw5JR/ (дата обращения 19.12.2020).

5 Приговор Когалымского городского суда Ханты-Мансийского автономного округа от 7 мая 2020 года по делу №1-19/2020. URL: https://sudact.ru/regular/doc/UvHCmAkAvGLH/ (дата обращения 06.10.2020).

6 Приговор Красногорского городского суда Московской области от 08 сентября 2020 г. по делу № 1-222/2020. URL: https://krasnogorsk--mo.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=case&ca

se_id=142605937&case_uid=03ac451d-aafe-448b-b9e6-fa620e52afda&delo_id=1540006 (датаобращения 23.12.2020).