МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра уголовно-правовых дисциплин

РЕКОМЕНДОВАНО К ЗАЩИТЕ В ГЭК
Заведующий кафедрой, кандидат
юридических наук, доцент,
заслуженный юрист РФ
_____В.И. Морозов
06 декабря 2022 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
магистерская диссертация

ТЕОРИЯ И ПРАКТИКА РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА

40.04.01 «Юриспруденция»
Магистерская программа «Магистр права»

Выполнил работу
студент 3 курса
заочной формы обучения — Билан Артём Николаевич

Руководитель
канд. юрид. наук, доцент — Абдулвалиев Алмаз Фирзярович

Рецензент
следователь отдела по
расследованию тяжких и особо
тяжких преступлений СУ УМВД
России по г. Нижневартовск — Князева Анна Андреевна

Тюмень
2022

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Мошенничество – это одно из распространённых преступлений против собственности. Так, в 2021 году, согласно официальным данным судебной статистики, за совершение всех видов мошенничеств, которые предусмотрены в ст.ст. 159, 159.1-159.6 УК РФ, было осуждено 20,6 тыс. чел. В первой половине 2022 г. – 11,5 тыс. чел. [81].

В силу распространённости и давности существования мошенничества наука криминалистики подробно изучила это преступление: способы его совершения, особенности личности мошенника и, конечно же, сформулировала множество рекомендаций для тактики его расследования. Однако мошенничество – это преступление, у которого постоянно появляются новые способы совершения.

В частности, одна из современных тенденций преступлений против собственности – это хищения чужого имущества, совершаемые с использованием электронных средств платежей [Россинская, с. 77].

Очевидно, что правоохранительные органы должны иметь полное представление о том, как противодействовать такого рода преступлениям и как раскрывать новые мошеннические схемы. Это особенно актуально сейчас, в период пандемии и финансово-экономических проблем, когда многие люди, во-первых, испытывают серьёзные финансовые трудности и вследствие чего легко уязвимы для мошенников и, во-вторых, больше времени проводят в интернет-пространстве.

Масштабность и распространённость мошенничества побуждает отечественного законодателя предусматривать меры по противодействию данному виду преступлений, причём не только уголовно-правовыми средствами. Так, в Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» летом 2021 г. были внесены изменения, направленные на то, чтобы телефонные мошенники не имели возможности покупать сим-карты и использовать их для звонков потенциальным потерпевшим. В частности,

закон обязал, что продавать сим-карты можно лишь в стационарных точках продаж. Тем самым запрещается продажа сим-карт на улице и в других местах, где можно легко продавать их в обход обязательной регистрации сим-карты в сети [3].

Также можно отметить Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» от 27 июня 2018 г. № 167-ФЗ. Указанный нормативно-правовой акт внёс изменения в ряд федеральных законов, объединённые одной целью – противодействовать кибермошенничеству как распространённому виду мошенничества. В частности, банки были наделены правом блокировать подозрительные транзакции без согласия на то владельца карты, являющегося клиентом банка [4].

Несмотря на вышесказанное, современная наука криминалистики недостаточно внимания уделяет разработке методики по расследованию компьютерных преступлений, в том числе кибермошенничества. Дело в том, что отличительной особенностью кибермошенничества является использование сети «Интернет» для совершения обмана или введения в заблуждение в виртуальном пространстве. Будучи относительно молодым видом преступности, кибермошенничество ещё не настолько глубоко и всесторонне изучено наукой криминалистики, в отличие, например, от традиционных способов мошенничества.

С одной стороны, уже выработанные и апробированные практикой тактические рекомендации по расследованию преступлений активно применяются и в отношении кибермошенничества, и новых видов мошенничества в целом.

С другой стороны, многие элементы криминалистической характеристики мошенничества значительно меняются, делая прежние методики не настолько эффективными, как раньше. В частности, существенно меняется личность мошенника – преступники становятся

моложе, и они обладают другим набором знаний и навыков: владение информационными технологиями, умение притворяться в сети «Интернет» другим человеком и т.д.

Соответственно, и наука, и практика нуждаются в новой разработке криминалистического обеспечения по тактике расследования таких преступлений. Таким образом, нужно изучить теорию и практику расследования мошенничества, чтобы предложить новые рекомендации по расследованию мошенничества.

Объектом исследования выступает криминалистическая характеристика мошенничества, а также теория и практика его расследования. Предметом исследования выступают закономерности осуществления преступных посягательств при мошенничестве, а также закономерности работы правоохранительных органов по их расследованию.

Цель исследования – изучить теоретические и практические проблемы расследования мошенничества.

Задачи исследования:

1) рассмотреть понятие, виды и криминалистическую характеристику мошенничества;

2) дать характеристику способам совершения мошенничества;

3) рассмотреть типичные следственные ситуации и программы расследования мошенничества;

4) исследовать тактику проведения отдельных следственных действий при расследовании мошенничества;

5) изучить криминалистические особенности кибермошенничества;

6) рассмотреть практику организации расследования кибермошенничества;

7) изучить тактику проведения отдельных следственных действий при расследовании кибермошенничества.

Методологической базой исследования послужили такие методы исследования, как описательный, структурно-функциональный и системный,

которые позволили собрать, проанализировать необходимую информацию и сделать выводы о проделанном исследовании.

Нормативную базу исследования составило отечественное законодательство, которое регулирует уголовную ответственность за совершение мошенничества (УК РФ), а также порядок проведения следственных действий при расследовании подобных преступлений (УПК РФ).

Практическую базу исследования составили уголовные дела по делам о мошенничестве. Было исследовано более 50 приговоров, вынесенных в период за 2018-2022 гг.

Теоретическую базу исследования составили научные статьи, учебные пособия, диссертации и научные монографии учёных и специалистов в области криминалистики. Одни исследователи посвятили свои труды криминалистической характеристике мошенничества в целом: Р.С. Белкин, В.И. Гладких, М.А. Простосердов, Е.Р. Россинская, Н.П. Яблоков и др.

Другие, в свою очередь, посвятили свои работы отдельным аспектам или видам мошенничества. Например, К.А. Виноградова предложила методику расследования мошенничества в сфере кредитования [Виноградова, с. 12], А.В. Чумаков – при получении выплат [Чумаков, с. 18], Э.Д. Нугаева – при оказании оккультных услуг [Нугаева, с. 47], С.Р. Низаева – в области оборота жилья [Низаева, с. 11].

Структура работы определена целями и задачами исследования и состоит из введения, трёх глав, включающих семь параграфов, заключения и списка использованной литературы и источников.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА

1.1. Мошенничество: общая криминалистическая характеристика

Одним из видов хищений является мошенничество. Согласно ч. 1 ст. 159 УК РФ, мошенничество представляет собой такое хищение чужого имущества (либо приобретение права на него), которое совершается посредством обмана либо злоупотребления доверием [1]. Следует рассмотреть общую криминалистическую характеристику этого преступления.

В основе совершения мошенничества лежит то, что преступник совершает какие-либо действия, связанные с обманом лица (или с злоупотреблением доверия). В результате таких действий имущество (или право на него) переходит от одного лица к другому. Обман и злоупотребления доверия как способы совершения мошенничества предопределяют криминалистическую характеристику рассматриваемого преступления [Атаманов, с. 25].

Вообще, уголовное законодательство знает несколько видов мошенничества. В ст. 159 УК РФ раскрывается основной состав, в то время как в ст.ст. 159.1-159.6 – частные разновидности мошенничества, например, в сфере компьютерной информации. Тем не менее, основные признаки мошенничества одинаковы для всех видов.

Наука криминалистики, раскрывая мошенничество, предлагает отталкиваться от следующих элементов криминалистической характеристики данного преступления:

1) Следовая картина мошенничества крайне разнообразна. Если выделять наиболее типичные следы, образуемые при совершении мошеннических действий, то можно отметить следующие:

– документы, которые остаются у потерпевшего после того, как его имущество было похищено (например, поддельный платёжный документ, квитанция, чек и др.);

– следы пальцев рук преступника, которые могут быть оставлены на месте происшествия, а также на предметах, которые были переданы им для потерпевшего;

– различные предметы, которыми пользовался преступник, но оставил на месте происшествия (например, ручка) [Драпкин, с. 721].

Несомненно, этим следовая картина мошенничества не исчерпывается. Развитие способов совершения мошенничеств обуславливает появление новых видов следов. Например, компьютерные мошенничества (или кибермошенничества, о которых пойдёт речь в третьей главе настоящего исследования) оставляют за собой ряд нетипичных для «традиционного» мошенничества следов вроде следы применения программ для несанкционированного доступа к компьютерным данным [Федотов, Зебницкая, с. 24].

Следует привести пример из судебной практики, который иллюстрирует следовую картину мошенничества. Бердюжский районный суд Тюменской области рассмотрел уголовное дело о мошенничестве: А, будучи главой компании, осуществляющей автобусные перевозки граждан, использовал своё служебное положение. Он внёс ложные сведения в документы компании, чтобы получить деньги, полагающиеся по муниципальному контракту для компенсации расходов на льготный проезд. Им было похищено 13 тыс. рублей. Суд признал А. виновным, основываясь на следующих вещественных доказательствах, содержавших следы мошенничества: реестры граждан, перевезенных автобусами компании и имеющих льготы; ведомости учёта граждан, воспользовавшихся льготой на оплату проезда; билетно-учётные листы за 2018-2020 гг. [66].

2) Обстановка совершения мошенничества отличается от многих других преступлений (в том числе других видов хищений) тем, что

исследуемое преступление не является насильственным. Добровольная передача имущества ведёт к тому, что внешних признаков совершения преступления существенно меньше, либо их нет вовсе.

Особенности обстановки во многом определяются сферой, где оно совершается, например, строительство, страхование, образование и т.п. Например, изменение порядка обеспечения населения жильём стало причиной роста мошенничеств, совершаемых при покупке, долевом участии в строительстве, обмене жилья [Белкин, с. 620].

Из-за этого усложняется расследование мошенничеств. В отличие от разбоя, где свидетель может подтвердить, что имущество было передано потерпевшим преступнику под насилием (или под угрозой его применения), при мошенничестве свидетелю гораздо труднее подтвердить, что имел место обман и, как следствие, преступный умысел [Яблоков, с. 420].

3) Время совершения мошенничества не конкретизировано. Оно, как показывает практика, совершается в различное время суток и в различные периоды времени.

4) Места совершения мошенничества разнообразны:

– место проживания потерпевшего;

– помещение, где мошенники заключали с ним договоры, получали ценные бумаги;

– территория мошенника (офисы, помещения, занимаемые мошеннической фирмой);

– нейтральная территория (т.е. помещения, не связанные ни с потерпевшим, ни с мошенником; которые были арендованы мошенниками на очень короткий срок для совершения преступления).

5) Личность преступника – мошенника. Предлагается остановиться на указанном элементе криминалистической характеристики мошенничества подробнее.

Анализ правоприменительной практики показывает, что типичный мошенник – это лицо зрелого возраста. Это обусловлено тем, что совершение

данного преступления требует обмануть потерпевшего или злоупотребить его доверием. Соответственно, для этого нужно обладать такими чертами личности, как хитрость, ловкость, умение использовать слабости человека и т.п. Всё это предполагает наличие жизненного опыта.

В криминалистической науке разработана подробная классификация мошенников. Как правило, выделяют следующие виды мошенников [Бунина, Мовсесян, с. 25]:

а) случайные мошенники, т.е. те, которые осуществляют мошенничество впервые, под влиянием обстоятельств или других лиц;

б) лица, ранее осуждённые за мошенничество. Их, в свою очередь, подразделяют на:

– мошенников-рецидивистов, которые осуществляют главным образом мелкое мошенничество;

– мошенников-многократных (так называемых «закоренелых») рецидивистов;

в) мошенники-гастролёры;

г) мошенники, которые осуществляют длящиеся мошенничества, заключающиеся в длительном получении материальных благ.

Мошенник является «коммерческим» преступником. Их действия направлены на получение имущественной выгоды за счёт других лиц без применения насилия – вместо этого они используют сведения, которые являются ложными (например, вымышленные имя, место работы и т.д.).

Мошенники, как правило, относятся к числу людей, которые являются хорошими специалистами и даже профессионалами в какой-либо области, профессии. Нередко преступники, осуждённые за мошенничество, работали в экономической, финансовой и других сферах, например, бухгалтерами, банкирами, брокерами. Также они часто занимали руководящие должности в коммерческих предприятиях.

Исследователи, описывая типичного мошенника, часто наделяют их следующими чертами: умные, образованные, умеющие мыслить

нестандартно, разбирающиеся в законодательстве, психологически устойчивые, вызывающие доверие у окружающих, разбирающиеся в различных областях жизни человека и т.д. Также отмечается, что мошенники в большинстве случаев не злоупотребляют ни алкоголем, ни наркотиками, что позволяет им лучше контролировать себя при совершении преступлений [Быкова, с. 96].

Также исследователи отмечают, что мошеннику присущи «развитый интеллект, сила убеждения, изощренная настойчивость в реализации преступного замысла. Непосредственный контакт с потерпевшим требует общительности, умения поддерживать разговор на разные темы, определённой смелости [Быкова, с. 97].

Несомненно, разные виды и способы совершения мошенничества предполагают специфические черты мошенника. Так, А.В. Шатилов делает вывод о том, что основными характеристиками мошенника, который является участником организованной группы, являются: склонность ко лжи, артистизм в поведении, коммуникабельность, умение работать в группе, учёт интересов других участников преступной организации [Шатилов, с. 193].

В целом анализ личности мошенников говорит о том, что в их основу положены устоявшиеся формы, виды и способы совершения рассматриваемых преступлений. Однако сегодня, учитывая современные технологии и растущий профессионализм мошенников, они значительно изменились.

6) Личность потерпевшего. Во многих случаях потерпевшие стали жертвами мошенничества из-за своего виктимного поведения, выразившегося в согласии с предложениями мошенников приобрести для них определённые блага незаконным путём, в обход установленного порядка. Такие жертвы мошенничества не принимали необходимых мер предосторожности, благоприятствовали созданию ситуации совершения преступления, а иногда и провоцировали его совершение [Лазарев, с. 183].

Следует отметить, что личности мошенника и потерпевшего неразрывно связаны между собой. Видится обоснованным полагать, что мошенник использует черты своей личности для того, чтобы черты личности потерпевшего побудили его совершить действия, выгодные для первого. Речь идёт в первую очередь о харизме, которой может обладать преступник, чтобы воспользоваться доверчивостью жертвы. Популярными среди мошенников становятся достижения так называемой «социальной инженерии» (подробнее о ней – в следующем параграфе настоящего исследования).

Что касается потерпевших, то многие из них, как было отмечено ранее, являются доверчивыми. Например, в 2020-2021 гг. были зафиксированы многочисленные случаи, когда мошенники, притворяясь иностранцами в сети «Интернет», завязывали знакомства с россиянками (как правило, незамужними). Мошенник-«иностранец» сперва входил в доверие, затем высказывал заинтересованность в отношениях (в том числе создании семьи), и в итоге давал обещание приехать в Россию. Далее у «иностранца» возникали какие-либо проблемы, например попадание в больницу или задержка в аэропорту. Цель – побудить жертву оказать финансовую помощь, чтобы как можно скорее встретиться с «иностранцем» [79].

Очевидно, что, используя описанную выше схему мошенничества, преступники пользовались не только доверчивостью потерпевших, но и слабыми и уязвимыми местами их личности, а именно: одиночество; недостаток любви; низкая самооценка; стремление найти мужа; поспешность в принятии решений; потребность в общении и близости; и др.

Несомненно, названные выше элементы криминалистической характеристики мошенничества – лишь основные. В науке криминалистики существует множество подходов, которые предполагают более широкий перечень таких элементов.

Например, Д.В. Лазарев считает, что характеризовать мошенничество следует, опираясь, помимо прочего, на такие элементы, как физическая и

психическая деятельность субъекта. То есть объективная и субъективная стороны, представляющие собой уголовно-правовые элементы состава мошенничества, с позиций науки криминалистики трансформируются в часть криминалистической характеристики рассматриваемого преступления [Лазарев, с. 58].

В свою очередь, Н.В. Быкова предлагают относить к важному элементу расследования мошенничества такой элемент, как установление связи между участниками преступной группы (если оно совершено группой лиц) [Быкова, с. 43]. Очевидно, что установление таких связей – крайне важно для расследования преступления. Сюда же исследователь относит действия по использованию и реализации похищенного имущества.

Следует согласиться с тем, что криминалистическая характеристика мошенничества может рассматриваться широко. Она тем самым может включать широкий набор разнообразных элементов, куда наряду с традиционными для всех видов преступлений (вроде предмета, личности потерпевшего и др.) могут входить специфические, свойственные именно для мошенничества.

Представляется, что одна из особенностей мошенничества – это специфические характер взаимоотношений между преступником и потерпевшим. Ранее было отмечено, что и тот, и другой имеют свои отличительные черты. Если развивать упомянутую выше идею Н.В. Быковой, то можно предложить такой криминалистический признак мошенничества как характер взаимоотношений между мошенником и потерпевшим. Это целесообразно по нескольким причинам:

– во-первых, это отражает одну из особенностей мошенничества – значительная часть способов совершения данного преступления может подразумевать близкие связи между мошенником и потерпевшим (подробнее о способах совершения мошенничества – в следующем параграфе настоящего исследования);

– во-вторых, это неразрывно связано с методикой и тактикой расследования мошенничества, которая предполагает обязательное выявление связей между всеми участниками преступления и потерпевшим. Иными словами, разработка такой связи как элемента криминалистической характеристики может положительно отразиться на развитии методики (равно как и наоборот);

– в-третьих, это может стать основой для дальнейшего теоретического осмысления мошенничества с точки зрения не только криминалистики, но и других наук, например криминологии. Так, на основе предлагаемого критерия можно предположить развитие типологии так называемого социального мошенничества.

Сама связь между мошенником и потерпевшим может выражаться в следующем. Первый, совершая преступление, осуществляет множество этапов, которые можно включить в механизм совершения мошенничества. Каждый из таких этапов может подразумевать различные способы взаимодействия между ними. Кроме того, какие-либо этапы могут отсутствовать.

Сперва мошенник определяет жертву. Для этого он может отталкиваться от таких признаков, как пол, возраст, финансовое положение и др. Здесь он выбирает, каким способом и когда вступит с будущим потерпевшим в контакт: по телефону, личная беседа, с использование сети «Интернет» или иначе.

Другая важная стадия – это применение «легенды». Мошенник может придумать и инсценировать перед жертвой ситуацию, чтобы убедить её совершить действия в его пользу. Например, представиться сотрудником социальной службы или правоохранительных органов.

После того, как мошенничество было совершено, взаимоотношения между мошенником и потерпевшим могут быть прекращены, для чего первый скрывается. Так, он может сообщить последнему ложные сведения о том, где будет находиться в будущем.

Таким образом, криминалистическая характеристика мошенничества показывает, насколько исследуемое преступления является разнообразным и стремительно меняющимся. Типичными выделяемыми элементами криминалистической характеристики мошенничества являются: следовая картина; обстановка и место совершения; личность преступника и потерпевшего. Представляется, что названными элементами криминалистическая характеристика исследуемого преступления не исчерпывается.

В качестве нового элемента криминалистической характеристики мошенничества предлагается рассматривать связи (или характер отношений) между мошенником и потерпевшим. Этот элемент отразит одну из важнейших особенностей мошенничества – наличие близкой связи между мошенником и потерпевшим, ведь нередко преступление совершается в результате сложных, продуманных и последовательных действий преступника: поиск жертвы, применение «легенды», скрытие от потерпевшего и т.п.

Кроме того, характер отношений между мошенником и потерпевшим органично сочетает в себе другие элементы мошенничества, такие как способ его совершения, личность преступника и др. Более того, этот элемент неразрывно связан с методикой и тактикой расследования мошенничества, которая предполагает обязательное установление связей между всеми участниками преступления и потерпевшим. Наконец, он не только более точно отразит социальную направленность мошенничества, но и сможет положительно повлиять на развитие тактики и методики расследования.

1.2. Характеристика способов совершения мошенничества

Как было сказано ранее, мошенничество может быть совершено самыми разнообразными способами. Следует рассмотреть распространённые

способы мошенничества, а также те, что получают своё распространение сегодня.

В предыдущем параграфе было указано, что мошенничество совершается путём обмана либо путём злоупотребления доверия. Обман может быть выражен в таких действиях мошенника, как умышленное сообщение недостоверной информации или как умолчание правдивых сведений. Первое действие является примером активного обмана, а второе – пассивного.

В свою очередь, введение в заблуждение может быть выражено в том, что мошенник использует поддельные документы, товары или другие предметы, чтобы побудить потерпевшего передать своё имущество (или право на него). Например, поддельный документ о наличии у мошенника права собственности на жилище, чтобы «продать» его. Другой распространённый способ введения в заблуждение – это использование обманных приёмов, например, во время игры в азартные игры.

Для каждого мошенничества, по сути, может быть характерен собственный способ совершения преступления. Однако типичные схемы совершения этого преступления позволяют классифицировать такие способы. Например, в науке предлагается классификацию обмана:

1) обман относительно действительных намерений (обещает жертве совершить какие-либо действия в дальнейшем и не совершает их);

2) обман в предмете преступления: в его свойствах, качестве, количестве (продажа заведомо сломанной вещи под видом исправной);

3) обман в каких-либо фактах или событиях (обман в фактах и событиях, которые уже произошли, и обман в событиях, которые якобы должны произойти в будущем;

4) обман в личности виновного (представление чужим именем);

5) обман в игре (заведомо проигрышные азартные игры);

6) так называемый «цыганский обман» (наведение порчи на недруга, предсказывание судьбы и т.п.);

7) обман влечении или целительстве (снятие порчи, излечение несуществующей болезни, использование заведомо ложных методов лечения) [Яблоков, с. 723].

Получается, что обман при мошенничестве крайне разнообразен как по своему содержанию, так и по проявлению. В самом общем виде обман можно свести тому, что мошенник обманывает насчёт предмета преступления (как правило, предмет сделки). Также он может обмануть насчёт оснований получения имущества и/или собственной личности.

Наиболее типичный случай обмана – это обман касательно намерений. Он состоит в том, что мошенник обещает оказать потерпевшему какую-либо услугу (выполнить работу или передать товар), однако он изначально не собирается исполнять взятые на себя обязательства. В частности, мошенник может обещать передать товар позже взамен на плату, но, получив деньги, скрывается от потерпевшего.

Следует привести пример из судебной практики, который иллюстрирует такой способ совершения мошенничества, как обман. Калининский районный суд г. Тюмени рассмотрел уголовное дело по обвинению К., который совершил мошенничество следующим способом. Он обманул потерпевшую П., выдав себя за представителя коммерческого предприятия, принимающего вклады граждан для последующего возврата с прибылью в виде процентов. Однако на деле П. никак не был связан с компанией, от лица которой он принял у П. деньги на сумму 200 тыс. руб. в качестве займа. Чтобы убедить П. в законности сделки, К. воспользовался документами, печатями и штампом с факсимильной подписью директора предприятия, где он трудился на момент совершения преступления. Подделав документы, он получил деньги П., после чего не стал вносить их в кассу организации, а потратил на собственные нужды [71].

Более сложным способом совершения мошенничества признаётся злоупотребление доверием. Под ним в общем виде принято понимать разновидность обмана, когда преступник пользуется доверительными

отношениями с кем-либо (как правило, с собственником имущества), чтобы реализовать свою корыстную цель.

Как и при обмане, мошенник может использовать доверие других лиц для совершения мошенничества. Наиболее частые случаи – это использование доверия родственников или коллег, которые нередко становятся потерпевшими. Также распространено злоупотребление доверием, когда мошенник принимает на себя те обязательства, которых у него на самом деле быть не может в силу закона. Например, он получает денежные средства по договору кредита, однако не намеревается возвращать их банку.

Мошенничество путём злоупотребления доверием чаще всего встречается при завладении имуществом, вверенным виновному на основе договорных отношений специального поручения, хранения, поставки, наследования или распоряжения.

На практике можно встретить ситуации, когда мошенники, обманывая в своих намерениях, создают фиктивные компании, чтобы в дальнейшем от имени последних совершать мошеннические сделки. Такого рода практика достаточно распространена, и эту схему можно представить, как часто используемый мошенниками алгоритм, включающий в себя следующие последовательные действия [Белкин, с. 860]:

– во-первых, мошенники создают и регистрируют компанию (например, общество с ограниченной ответственностью). Внешне такая компания может не вызывать подозрений, однако её руководители изначально не намерены осуществлять легальную предпринимательскую деятельность;

– во-вторых, такая компания рекламирует свои «услуги», которые внешне также выглядят законно. Однако для подобных объявлений характерно то, что предлагаемые фиктивными компаниями товары, работы или услуги дешевле, чем в среднем на рынке. Это же касается других

преимуществ: срок поставок товаров значительно меньше; скорость выполнения работы быстрее; и т.п.;

– в-третьих, такого рода компания, заключая договоры, требует аванс или предоплату;

– в-четвёртых, мошенники, получив деньги, выводят их из компании и присваивают себе, а затем скрываются. Компания может быть ликвидирована или реорганизована.

Как неоднократно отмечалось, способы совершения мошенничества даже в рамках одного вида рассматриваемого преступления отличаются крайне широким разнообразием. Учёные-криминалисты часто уделяют пристальное внимание какой-либо одной разновидности мошенничества, в рамках которой подробно изучают сложные мошеннические схемы. Так, мошенничества в области экономической деятельности совершаются следующими наиболее типичными способами:

– практике известны многочисленные факты мошеннических хищений под видом получения банковского кредита, когда создаётся коммерческая организация, которая после получения и присвоения кредита прекращает существование, а её руководители скрываются;

– создание финансовой пирамиды. Основная идея этого способа мошенничества состоит в создании какой-либо организации, осуществляющей различные мошеннические манипуляции с ценными бумагами: привлечение максимального количества денежных средств от физических и юридических лиц в обмен на выпущенные данной организацией ценные бумаги, обещание высоких годовых прибылей по ним и непродолжительное исполнение этого обещания за счет привлечения еще большего количества вкладчиков и т.п. При этом никакого «эффективного использования» привлечённых средств не производится, они не вкладываются в улучшение производства, развитие обещанного бизнеса, а просто похищаются мошенниками [Атаманов, с. 80].

В отдельную группу можно выделить такие способы совершения мошенничества, которые совершаются вне предпринимательской сферы и связаны с обманом отдельных граждан. Среди них предлагается отметить следующие:

– завладение имуществом потерпевшего под предлогом гадания или знахарства;

– похищение имущества граждан путём незаконных сборов под видом представителей контрольных или правоохранительных органов, уполномоченных организаций (например, за парковку, за посещение общественных мест и т.п.);

– хищение имущества потерпевшего под предлогом получения его во временное пользование, напрокат или путём займа у знакомых без намерения возврата [Грунтовая, с. 16];

– мошенничества, основанные на банковских операциях. Здесь возможно огромное количество способов. Например, мошенник может побудить предпринимателя заключить «выгодную» сделку, представившись агентом или представителем реально существующей торговой компании. Для этого он может создать Интернет-сайт такой компании, идентичный настоящему, где предприниматель заплатит не реальной фирме, а мошеннику.

Другой способ, также основанный на банковских операциях и получивший распространение в последнее время – это звонок мошенника, который представляется сотрудником службы безопасности банка. Связь между ним и жертвой происходит следующим образом: сперва он связывается с жертвой по телефону, после чего применяет «легенду»: представляется сотрудником службы безопасности банка и инсценирует попытку хищения денег с кредитной карты. Далее он предлагает различные варианты. Один из них – перевод денег на специальный «защищённый» счёт, который на самом деле является счётом мошенника. Другой способ – установить специальное приложение для защиты, которое в

действительности будет удалённо управлять телефоном или компьютером жертвы [80].

Сложность многих способов мошенничества обусловило групповой характер рассматриваемого преступления во многих случаях. Очевидно, что продолжительная деятельность, например, фиктивной коммерческой компании, требует, чтобы была создана преступная группа с распределением ролей. Такие группы, как правило, устойчивы, а их деятельность продолжительна.

Также следует отметить, что в своей преступной среде мошенники специализируются на каком-либо определённом виде и способе мошенничества. Преступная среда данной категории лиц характеризуется тем, что в ней заранее распределяются сферы и области преступного влияния и мошеннического «бизнеса».

Так, в Тюменской области в последние годы распространён вид мошенничества, при котором работники транспортных компаний, получая денежные средства по муниципальным или государственным контрактам для компенсации льгот на транспортные услуги, вносят изменения в документы, чтобы похитить деньги. Ранее был приведён пример подобной схемы мошенничества. Ещё один пример: Голышмановский районный суд Тюменской области рассмотрел уголовное дело по обвинению К., который аналогичным способом похитил 1,5 млн рублей. Он также, будучи генеральным директором транспортной организации, предоставлял поддельные документы о перевозках граждан в льготном порядке, чтобы получить компенсацию расходов со стороны государственных органов власти [69].

Нужно подчеркнуть, что для мошенничества характерно постоянное появление новых способов. Они могут появляться из-за новых технологий (как кибермошенничество), из-за естественного развития общественных отношений (например, появление нового вида банковской услуги

закономерно влечёт новый вид мошенничества, связанный с ним) или из-за каких-либо обстоятельств, повлиявших на жизнь общества [Сафонов, с. 91].

Примером последнего может стать пандемия коронавирусной инфекции. Исследователи и практики уже изучают новые мошеннические схемы, которые появились непосредственно из-за пандемии. Следует раскрыть некоторые из них.

Один из новых способов мошенничества – это предложение выплатить компенсацию за пребывание в карантине. Мошенники, используя сеть «Интернет», распространяют ложные сведения о том, что государство якобы выплачивает всем без исключения гражданам выплаты из-за карантина. В объявлении о такой выплате может содержаться ссылка на интернет-сайт, который является двойником официального сайта (например, Минздрава России). На нём можно заполнить анкету о получении денег, но для осуществления выплаты предлагается оплатить комиссию (для создания электронной подписи, проверки данных «получателя» выплаты и т.п.). В итоге люди, которые не разобрались в законах, принятых в период пандемии, оплачивают комиссию и остаются без выплаты [Еськова, Рябчиков, с. 69].

Другой способ – это предоставление заведомо ложной информации о том, что родственник потерпевшего находится в больнице с коронавирусной инфекцией. На телефон потерпевшего поступает звонок от имени «врачей», мнимых сотрудников Роспотребнадзора или иных ведомств. Родственникам сообщают, что у их близких оказался положительный тест на коронавирус. Затем сообщается, что их увезли в больницу или изолировали в обсерваторе. После предлагается перевести деньги на счёт «медучреждения» для улучшения условий содержания больного. Дополнительно могут следовать предложения насчёт покупки дорогих медицинских препаратов, средств профилактики и гигиены, якобы рекомендованных для защиты от коронавируса [Белицкий, с. 36].

Также в качестве примера можно привести новые схемы мошенничества на фоне мобилизации в России. Так, один способ

предполагает, что человек, который притворяется работником военкомата, обещает «потерять» повестку, за что потерпевший должен заплатить. Другой способ предполагает, что потерпевшему за деньги обещают, что он будет убран из списка граждан, подлежащих мобилизации. Эти и другие способы мошенничества явно пользуются тем, что потерпевшие испытывают страх в связи с мобилизацией.

Значительная часть новых способов мошенничества связана с появлением новых финансовых активов вроде криптовалют, токенов, электронных денег и т.п. Из-за того, что правовой статус многих из перечисленных предметов в России до конца не урегулирован, они не являются объектом уголовно-правовой охраны. Как следствие, мошенники активно пользуются этим.

Например, мошенничество при облачном майнинге (т.е. добыче криптовалюты с помощью удалённых компьютерных мощностей) состоит в том, что компания, предлагающая услуги удалённого майнинга, берёт с пользователей плату для того, чтобы приобрести оборудование, добывать на нём криптовалюту и платить вознаграждение пользователям. Однако на деле умысел мошенников направлен на то, чтобы получить деньги и не выплачивать вознаграждение либо выплачивать, но в течение непродолжительного времени. Этот способ мошенничества часто сочетается с другими, например, создание фальшивых сайтов-двойников известных компаний. Этот и иные подобные способы можно объединить понятием «кибермошенничество».

Также для современного мошенничества характерна его трансграничность (или транснациональность). Описанные выше способы мошенничества, если они связаны с применением сети «Интернет» или других информационных технологий, часто совершаются из-за границы, т.е. мошенник и потерпевший находятся в разных государствах.

Так, в городе Днепр, как отмечают многие СМИ, находится «столица телефонного мошенничества». Из этого города российским гражданам

поступает колоссальное число звонков от работников более чем 1 тыс. колл-центров [78].

Наконец, следует отметить, что мошенники, разрабатывая и реализуя новые способы совершения мошенничества, активно прибегают к положениям различных наук, в частности психологии и социологии. Так, в последнее время получила популярность идея «социальной инженерии». Под ней в общем виде можно понимать совокупность приёмов и методов для психологического манипулирования человеком. Иными словами, обладая навыками социальной инженерии, мошенники могут побудить человека совершить определённое действие, не применяя при этом очевидные уговоры и насилие.

Так, А. покушался на мошенничество следующим образом: он звонил случайным людям, представлялся сотрудником полиции и сообщал им о том, что их родственник стал виновником ДТП. Далее он сообщал о том, что высока вероятность привлечения родственника к уголовной ответственности. И сразу предлагал перевести ему денежные средства за «освобождение» от уголовной ответственности. Также А. совершал другие звонки, где представлялся следователем, сотрудником прокуратуры и т.д. [74].

Н.И. Старостенко отмечает, что «обстановка совершения мошенничеств с использованием методов социальной инженерии – это система взаимосвязанных элементов в виртуальной среде и в пространственно-временных условиях, в которых удаленно совершаются мошеннические действия, сопровождающиеся использованием техник социальной инженерии» [Старостенко, с. 74].

Многие из рассмотренных ранее способов совершения мошенничества предполагают обращение к идеям социальной инженерии. Например, совершение телефонных звонков, когда мошенники представляются сотрудниками банков или органов власти; имитация мошенником другой личности (родственника, иностранца); и т.д.

Примером можно считать такой способ, как «дорожное яблоко»: злоумышленник оставляет на видном месте (парковка офиса, лифт и т.п.) флеш-карту или карту памяти. Чтобы привлечь больше внимания жертвы, помечает её надписью, например, «сведения о сокращении штата». Из-за любопытства человек, нашедший «дорожное яблоко», подсоединяет подброшенное устройство к своему компьютеру. В результате включается вредоносная программа, направленная на сбор данных (например, о паролях к электронным кошелькам или о банковских картах).

Таким образом, приведённая характеристика способов совершения мошенничества доказывает, что исследуемое преступление является крайне разнообразным с точки зрения его криминалистической характеристики. В самом общем виде способы можно описать как обман и злоупотребление доверием.

И обман, и злоупотребление доверием при совершении мошенничества имеют множество проявлений, которые можно называть «мошенническими схемами». Для каждого вида мошенничества характерно несколько основных схем, которые имеют множество вариаций. Например, создание финансовой пирамиды может подразумевать её маскировку под производственный кооператив или под другую разновидность юридического лица.

Можно утверждать, что современных способов совершения мошенничества характерные следующие основные черты:

– во-первых, постоянное обновление и появление новых способов совершения мошенничества. Наглядным примером является «кибермошенничество», которое уже включает в себя целый ряд различных мошеннических схем, где задействованы компьютеры, сеть «Интернет» и другие информационные технологии;

– во-вторых, разные способы мошенничества могут комбинироваться друг с другом. Например, мошенничество при облачном майнинге сочетает в себе черты финансовой пирамиды, а также предполагает создание сайта-двойника;

– в-третьих, новые способы мошенничества возникают стремительно из-за изменений, которые происходят в жизни общества. Например, много новых способов мошенничества возникло за последнее время из-за пандемии и из-за мобилизации. То есть преступники находят способы воспользоваться текущими условиями жизни, новыми технологиями и другими изменениями. Следовательно, это приводит к устареванию устоявшихся на практике методик по расследованию мошенничества;

– в-четвёртых, способы мошенничества всё чаще основаны на положениях науки (психологии, социологии и др.). Выражением этого является применение «социальной инженерии», т.е. приёмов и методов для психологического манипулирования человеком. Следовательно, механизм совершения мошенничества становится всё более сильно зависимым от личностей преступника и потерпевшего.

ГЛАВА 2. ОСОБЕННОСТИ МЕТОДИКИ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА

2.1. Типичные следственные ситуации и программы расследования мошенничества

Рассмотренная в первой главе настоящего исследования криминалистическая характеристика мошенничества во многом предопределяет особенности расследования данного преступления. Следует перейти к рассмотрению типичных следственных ситуаций при расследовании мошенничества.

Для всех видов мошенничества характерны следующие группы наиболее распространённых следственных ситуаций: простые и сложные. Первые имеют место в тех случаях, когда следователь владеет сведениями касательно события мошенничества, о потерпевшем и о мошеннике. При этом преступник не скрывается [26, с. 44].

Основная задача следователя в подобного рода ситуациях состоит в установлении факта совершения мошенничества указанным лицом, наличия в его действиях преступного обмана или злоупотребления доверием. Направление расследования определяется потребностью получить максимальную информацию о преступлении, отграничить законную сделку от сделки, имеющей мошеннический характер.

Решение указанной задачи достигается выдвижением и проверкой таких общих типовых версий, как:

– мошенничество имело место при обстоятельствах, указываемых потерпевшим;

– мошенничества не было – налицо оформление законной сделки, добросовестное заблуждение потерпевшего.

В свою очередь, сложные следственные ситуации бывают следующих видов [11, с. 420]:

1) следователь владеет сведениям насчёт события преступления, а также о потерпевшем и о мошеннике. Однако виновное лицо скрылось. В случае совершения группового мошенничества эта ситуация может состоять в том, что лишь один из мошенников был задержан, а другие виновные – скрылись;

2) следователю известны событие преступления и сведения о потерпевшем лицо. Однако информации о мошеннике нет, или их очень мало. Подобного рода следственные ситуации складываются, как правило, когда мошенник – это лицо, неизвестное для потерпевшего;

3) следователь владеет информацией и о мошеннике, и о потерпевшем. Однако сам факт совершения преступления не очевиден, так как оно было совершено способом, хорошо замаскированным и внешне похожим, например, на законную сделку с имуществом;

4) есть информация о событии преступления и преступнике, но отсутствует или крайне недостаточна информация о потерпевшем. Подобные ситуации встречаются при непосредственном обнаружении фактов мошенничества со стороны конкретного липа в ходе оперативно-розыскных мероприятий или расследования, при проведении контрольных мероприятий в созданных и функционирующих предприятиях и фирмах, при ряде видов банковского мошенничества, когда потерпевший неизвестен.

При возникновении перечисленных выше ситуации главная задача следователя заключается в следующем – он должен выявить и разыскать мошенника и потерпевшего, после чего установить обстоятельства мошенничества.

В рамках методики расследования мошенничества следует отдельно выделить типовые версии о том, где может находиться скрывающийся от следствия мошенник. Это необходимо для его розыска. Чаще всего следователи исходят из трёх типовых версий [Анненков, с. 45]:

– во-первых, мошенник мог покинуть город (или другой населённый пункт), где было совершено мошенничество (и где он, вероятно, жил);

– во-вторых, мошенник мог покинуть дом, но не город – он прячется у родных, друзей или других знакомых;

– в-третьих, мошенник живёт там же, где и до совершения преступления, однако с поддельными документами о личности.

В соответствии с конкретной исходной информацией эти версии могут быть дополнены версиями о наличии у мошенника профессиональных навыков или знаний, вероятных местах совершения им других преступлений и т.д.

Теперь следует перейти к программам расследования мошенничества в типичных следственных ситуациях.

Если мошенничество было совершено знакомым потерпевшего (т.е. имеет место первая из приведённых выше следственных ситуаций), то следователь должен опираться на сведения, представленные в заявлении потерпевшего о преступлении. Здесь рекомендуется провести следующие следственные действия и ОРМ:

1) допрос потерпевшего;

2) выемку предметов или документов, имеющих значение для расследуемого события (расписок, обязательств, денежных и вещевых «кукол» и др.);

3) осмотр места происшествия, обнаруженных изъятых предметов, документов;

4) назначение экспертиз по исследованию этих предметов и документов (почерковедческой, технико-криминалистической, товароведческой. дактилоскопической, целого по частям и т.п.);

5) задержание и личный обыск подозреваемого;

6) допрос подозреваемого;

7) обыск по месту жительства или работы подозреваемого, у его родственников и знакомых;

8) следственный эксперимент;

9) очную ставку между потерпевшим и подозреваемым;

10) допрос свидетелей.

Нельзя не отметить, что при групповом мошенничестве «виновным» может выступать юридическое лицо (в том числе фиктивное). Поэтому следственные действия и ОРМ должны быть направлены в отношении юридического лица. Вместе с мероприятиями, названными выше, рекомендуется провести следующее [Шатилов, с. 195]:

1) выемка и осмотр учредительных и иных документов компании;

2) установление и допросы вкладчиков (если компания собирала деньги с частных лиц);

3) назначение инвентаризации и ревизий;

4) осмотр или обыск в служебных помещениях;

5) розыск имущества, денег и ценностей организации;

6) допросы должностных лиц и других сотрудников;

7) наложение ареста на банковские счета юридического лица.

Как правило, практические работники придерживаются приведённых программ расследования. Однако, очевидно, что ход расследования может потребовать внести изменения в перечень и в порядок проведения следственных действий. В частности, если мошенник после допроса в качестве подозреваемого признает свою вину, и будут установлены обстоятельства расследуемого мошенничества, то проведение очной ставки с потерпевшим становится не обязательным. Разумеется, при условии, что показания мошенника и потерпевшего не противоречат друг другу существенно.

Кроме того, программа расследования может предполагать, что порядок следственных действий меняется. Ещё один приём – это проведение нескольких действий в одно время, параллельно. Например, если мошенник был задержан практически сразу после совершения преступления, то рекомендуется незамедлительно провести тактическую комбинацию, включающую в себя:

– задержание и личный обыск мошенника;

– допрос потерпевшего;

– допрос свидетелей-очевидцев.

Также нужно отметить, что для расследования мошенничества могут быть полезны различные тактические операции. Распространённая операция – «задержание с поличным». Она включает в себя следственные действия и ОРМ, которые имеют единую цель – выявить и наблюдать за мошенником, чтобы затем осуществить подготовку для его задержания с поличным.

Таким образом, в основе типичных следственных ситуаций при расследовании мошенничества лежит, во-первых, характер взаимоотношений между мошенником и потерпевшим: они могут быть знакомы друг с другом или нет. Во-вторых, местонахождение мошенника: оно может быть известно или нет. При этом мошенник может скрываться в месте своего постоянного жительства, у знакомых или в другом населённом пункте.

Указанные факторы предопределяют программу расследования мошенничества. Она включает в себя комплекс следственных и оперативных мероприятий, которые должны не только установить личность мошенника, но и понять, каким именно способом он совершил мошенничество и было ли оно вообще.

Для расследования мошенничества крайне важно, чтобы следственные органы действовали быстро и оперативно, а также адаптировались под меняющийся ход расследования. Ключевая задача – это получение как можно больших сведений о событии преступления, что требует проведения осмотра места происшествия, допросов и обысков.

2.2. Тактика проведения отдельных следственных действий при расследовании мошенничества

Следует перейти к исследованию тактики проведения отдельных следственных действий при расследовании мошенничества.

Ранее было сказано, что наиболее типичные следственные действия, проводимые при расследовании изучаемого преступления, это допросы мошенника в качестве подозреваемого и потерпевшего; осмотр места происшествия; осмотр предметов. Следует рассмотреть их подробнее.

1. Допрос потерпевшего. Как правило, он является первым из числа проводимых следственных действий при расследовании мошенничества. Очевидно, что сведениями о мошеннике может владеть в первую очередь именно потерпевший: он может знать о факте мошенничества, о предмете хищения, о внешности мошенника и др.

Следователь, допрашивая потерпевшего, должен помнить, что он вёл себя виктимно. Соответственно, у потерпевшего может быть стремление не рассказывать следователю все обстоятельства совершённого преступления: какие-либо сведения могут быть скрыты или искажены. Например, из-за чувства стыда потерпевшего. Поэтому следователю следует разъяснить, что потерпевший не должен утаивать информацию от следствия, потому что в противном случае не получится изобличить мошенника и/или возместить ущерб от преступления [Шаталкина, с. 127].

При допросе потерпевшего нужно выяснить следующие обстоятельства: время, место, обстановку совершения преступления; обстоятельства и причины, по которым потерпевший оказался на месте преступления и встретился с мошенником; круг очевидцев и свидетелей мошенничества; способ обмана или злоупотребления доверием, способы, использованные преступником для похищения имущества; число мошенников и их приметы, а также действия, выполнявшиеся каждым членом преступной группы; каким имуществом или правом на имущество завладел виновный; какие предметы, документы и вещественные доказательства преступник оставил потерпевшему; как и в каком направлении скрылся мошенник; кому первому сообщил потерпевший о хищении у него имущества [Казинская, с. 122].

Разумеется, приведённый перечень не ограничивается указанными обстоятельствами. Многообразие способов совершения мошенничества требует конкретизировать предмет допроса в каждом уголовном деле. Например, если мошенник является знакомым потерпевшего, то рекомендуется выяснить характер их взаимоотношений с мошенником. Если же мошенник – неизвестное лицо, то нужно допросить потерпевшего о приметах преступника путём метода словесного портрета.

2. Осмотр места происшествия. После поступления заявления и допроса потерпевшего во всех случаях необходимо провести осмотр места происшествия. Особую важность приобретает осмотр в случаях, когда личность мошенника неизвестна. По результатам осмотра можно выяснить обстоятельства происшедшего события и на основе этого представить картину, способ совершения преступления, а в конечном счёте установить личность мошенника.

Как и допрос потерпевшего, особенности проведения осмотра зависят от конкретных обстоятельств мошенничества. В частности, способ совершения мошенничества влияет на последовательность осмотра. Например, когда мошенник использовал для обмана «вещевую куклу», то следователь должен найти на месте происшествия следующие следы: остатки упаковки от «вещевой куклы», остатки от её содержимого. Кроме того, при осмотре нужно найти следы, оставленные непосредственно мошенником: следы рук, ног, а также его транспортного средства [Зиннуров, с. 125].

Следует привести пример из судебной практики, где осмотр места происшествия сыграл ключевую роль в расследовании мошенничества. Ленинский районный суд г. Тюмени рассмотрел уголовное дело по обвинению Т., М. и Б. в групповом мошенничестве. Они работали в компании, которая оказывала сантехнические услуги. От имени этой компании они совершали обходы граждан (преимущественно пенсионеров и инвалидов), чтобы убедить последних в необходимости провести платные сантехнические работы. Каждый раз, после оказания таких услуг, они

заявляли о необходимости доплатить, мотивируя это тем, что сложность работ оказалась выше ожидаемой. Обманывая граждан, Т., М. и Б. получали от них денежные средства. Всего они заключили 8 договоров на платные сантехнические услуги на среднюю сумму около 30 тыс. руб. В ходе осмотра места происшествия на первоначальном этапе расследования уголовного дела были обнаружены следующие предметы, впоследствии ставшими вещественными доказательствами: кассовые чеки на оказание услуг потерпевшим; документы компании, от имени которой действовали Т., М. и Б.; договоры об оказании платных работ и услуг с потерпевшими; сантехническое оборудование; мастичные печати; кассовый аппарат; удостоверения [75].

3. Важное значение для успешного расследования мошенничества имеет осмотр предметов и документов, представленных потерпевшим или изъятых при осмотре места происшествия или обыске. По делам рассматриваемой категории подобными вещественными доказательствами являются: денежные и вещевые «куклы»; расписки мошенника; фальшивые кредитные бумаги; документы, которые касаются организации и функционирования созданных мошенниками юридических лиц; и др.

Если произошло мошенничество с использованием поддельных драгоценностей, то их осмотр необходим для того, чтобы понять, каким способом они были подделаны и как обработаны. Также на них, равно как и на других предметах, использованных мошенниками (например, фальшивые денежные купюры, поддельные визитные карточки и др.), могут быть следы пальцев рук мошенника.

При осмотре предметов и документов необходимо активно использовать помощь специалистов и технические средства. Информация, полученная при осмотре вещественных доказательств, может быть эффективно использована как в процессе розыска мошенника, так и при его изобличении в совершении преступления.

Следует привести пример из судебной практики, где осмотр предметов и документов оказался важен в ходе расследования мошенничества. С. захотел приобрести бытовую технику в кредит. С. заключил со своим знакомым Д. договор целевого займа на совместную покупку телевизора, пылесоса и другой техники на общую сумму 56 тыс. руб. Далее С. продал всё купленное имущество, тем самым обманув Д. В ходе расследования основным доказательством выступил договор целевого займа, заключённый между С. и Д. В отношении него был произведён осмотр предметов и документов: в нём содержались условия сделки, а также график платежей и дополнительное соглашение о комиссии. В итоге С. признан судом виновным по ч. 2 ст. 159 УК РФ [73].

4. Ещё одно важное следственное действия при расследовании мошенничества – это допрос свидетеля. Он может помочь получить более полное представление о личности мошенника: о его образе жизни, о профессиональных навыках, об имущественном положении и т.п. Также свидетель может рассказать на допросе о том, как мошенник и потерпевший связаны друг с другом.

Эти и другие показания свидетеля могут помочь следователю выяснить, насколько правдивы и точны показания потерпевшего, путём их сравнения. Например, если потерпевший в своих показаниях «завысил» ценность и стоимость похищенного у него имущества. Наконец, данное следственное действие может помочь разыскать скрывающегося преступника.

5. После задержания и личного обыска мошенника производится его допрос в качестве подозреваемого. Тактика допроса мошенника определяется конкретной ситуацией.

Как показывает практика, мошенники, оказавшись в роли допрашиваемых, дают показания. Однако они нередко пользуются своими качествами, чтобы приспособиться к обстановке, воспользоваться текущей

следственной ситуацией и запутать следователя. Например, они могут менять свои показания, исходя из обстоятельств, известных следствию.

В ходе допроса мошенника необходимо выяснить следующее: был ли он ранее знаком с потерпевшим и в каких взаимоотношениях с ним находился, при каких обстоятельствах у него оказалось имущество потерпевшего; применялись ли для этого какие-то противоправные или мошеннические действия, и если да, то какие; кто, кроме него, участвовал в совершении преступления и какова роль этих лиц; какой ущерб, по его мнению, был причинен потерпевшему; что явилось побудительной причиной преступления; и др. [Иванова, с. 122].

Предмет допроса, как и в случае с потерпевшим, зависят от вида и способа мошенничества. Так, В.Ю. Белицкий предлагает, если мошенничество было совершено путём создания финансовой пирамиды, которая маскировалась под легальную коммерческую организацию (например, производственный кооператив), допрашивать мошенника о том, что связано с деятельностью такой организации. Например, о рекламе: как она рекламировалась, кто осуществлял рекламу, где (если в сети «Интернет», то на каких сайтах), какие дополнительные способы привлечения денежных средств применялись и т.п. [Белицкий, с. 19].

Для того, чтобы допрос мошенника оказался более эффективным, рекомендуется использовать следующие приёмы. Во-первых, мошенника можно допросить таким образом, чтобы это было неожиданно для него. Например, в раннее время или когда он перемещается из одного места в другое. Также рекомендуется привлекать для участия в допросе лиц, которые значимы для мошенника.

Во-вторых, оказание психологического воздействия на подозреваемого. Нельзя забывать, что мошенник часто сам имеет психологические знания и навыки манипулирования людьми и сам может выступать субъектом, а не объектом психологического воздействия, вызывая у следователя определенные эмоции. Поэтому в ходе допроса следователь должен быть

лидером в формировании психоэмоциональной напряжённости. Мошенник может изобразить из себя невинного человека, жертву обстоятельств, либо властного человека, уважаемого в обществе, по сравнению с которым следователь не имеет никакого значения. Следователь должен проявлять эмоциональную стойкость, показывать свою твердость и значимость, чтобы иметь моральное превосходство.

Следует привести пример из судебной практики, где допрос подозреваемого наглядно иллюстрирует специфику расследования мошенничества. Ленинский районный суд г. Тюмени рассмотрел уголовное дело по обвинению А. в мошенничестве. Он взял деньги на сумму 1,5 млн. рублей в долг у автосалона, чтобы приобрести автомобиль, без намерения вернуть их. В ходе допроса А. в качестве подозреваемого показал, что он действительно получил деньги, но не для покупки автомобиля, а для организации совместного с потерпевшими бизнеса по перепродаже машин. А. заявил, что был готов вернуть часть суммы после того, как автосалон стал требовать уплаты долга, однако испугался входить в помещение автосалона, так как увидел возле него полицию. Также он заявил, что у сотрудников автосалона есть свободный доступ к кассе, из которой они берут свои зарплаты, поэтому работники могли воспользоваться этим, чтобы забрать денег больше, обвинив в хищении А. Тем самым он пытался запутать следствие [75].

6. Для закрепления и проверки показаний преступника, а также обнаружения данных, опровергающих показания подозреваемого, необходимо провести обыск по месту его жительства и работы. В ходе указанного следственного действия могут быть обнаружены орудия и средства совершения преступления, преступно добытое имущество и ценности, различные документы, переписка мошенника и другие вещественные доказательства, имеющие значение для дела.

Круг предметов и объектов, подлежащих обнаружению и изъятию, следует определять прежде всего исходя из данных, характеризующих

способ совершенного мошенничества, использовавшихся при этом орудий и средств. Так, если мошенничество было совершено с применением вещевой «куклы», то при обыске нужно искать предметы и вещи – заменители товара, переданного потерпевшему, остатки этих вещей и предметов, части упаковки, приготовленные для совершения новых преступлений.

Таким образом, тактика проведения отдельных следственных действий при расследовании мошенничества отражает разнообразие исследуемого преступления. Все проводимые в рамках расследования следственные действия должны носить системный характер, дополнять друг друга. Очевидно, что установление личности мошенника невозможно посредством лишь допроса потерпевшего, ведь мошенник мог совершить преступление под другим именем, выдавая себя за другую личность. Поэтому нужен и допрос свидетелей.

Для всех следственных действий при расследовании мошенничества также характерно то, что общие тактические приёмы могут быть легко дополнены частными рекомендациями, когда речь идёт о необходимости раскрыть какой-либо специфический вид или способ мошенничества. Например, Предмет допроса, как и в случае с потерпевшим, зависят от вида и способа мошенничества. если оно было совершено путём создания финансовой пирамиды, то целесообразно допрашивать мошенника о том, что связано с деятельностью подобной организации. Например, о продвижении и рекламе.

ГЛАВА 3. ПРОБЛЕМЫ РАССЛЕДОВАНИЯ КИБЕРМОШЕННИЧЕСТВА

3.1. Кибермошенничество как особая разновидность хищения

Понятием «компьютерная преступность» сегодня принято называть группу особо опасных экономических преступлений, совершаемых в информационной среде с использованием последних технологический достижений (компьютеры, смартфоны и другие устройства). В компьютерную преступность входят различные виды преступлений, в том числе мошенничество [Волеводз, с. 16].

Мошенничество в компьютерной сети (или кибермошенничество) – это новый вид преступности, получающий широкое распространение. Повсеместная компьютеризация и информатизация всех сфер человеческой деятельности, тотальное внедрение новых технологий неизбежно привели к криминализации этой области социально-экономической деятельности [Гафнер, с. 158].

Огромное количество самой разнообразной и сложной компьютерной и другой электротехники закономерно привели к появлению большого числа способов и видов кибермошенничества. Криминалисты отмечают, что для подобной разновидности мошенничества уже свойственно формирование специфической криминалистической характеристики. Поэтому исследователи обоснованно выделили такое мошенничество в системе компьютерных преступлений как самостоятельный вид – кибермошенничество.

Кибермошенничества совершается и развивается преимущественно в сети Интернет. Для правоохранительных органов является проблемой увеличение объёмов преступлений, совершаемых в Интернете, а также развитие технологий и компьютерных программ, предназначенных именно

для совершения кибермошенничества. Кроме того, это значительно затрудняет борьбу с киберпреступлениям, так как далеко не всегда удаётся сразу обнаружить виновных лиц.

Следует привести пример кибермошенничества. Г. работал на предприятии специалистом обслуживания и продаж. Согласно должностной инструкции Г. имел право пользоваться информационно-технологическим оборудованием и служебной сотовой связью для выполнения своих обязанностей. Имея доступ к базе данных с персональными данными абонентов сотовой связи, Г. неправомерно, используя пароли и номера телефонов, произвёл замену сим-карт 12 потерпевших. После чего Г. поменял пароли от платёжных систем, к которым были прикреплены предыдущие номера телефонов потерпевших с целью снять с них все денежные средства, т.е. совершить хищение. В итоге суд признал Г. виновным в совершении преступления, предусмотренного ч. 3 ст. 159.4 УК РФ (мошенничество в сфере компьютерной информации с причинением значительного ущерба гражданину, лицом с использованием своего служебного положения) с назначением наказания в виде одного года лишения свободы. Было установлено, что Г. не предпринимал попыток скрыть следы преступления. Кроме того, выяснилось, что все потерпевшие от кибермошенничества приобретали сим-карты в одном и том же месте, благодаря чему следствие сразу смогло определить место нахождение злоумышленника. Доказательствами по данному делу стали многочисленные сведения, полученные в ходе осмотра рабочего компьютера Г. о денежных транзакциях, совершённых на его денежные счета [76].

Лица, совершающие кибермошенничества, посягают не только на денежные средства граждан, но и на другие предметы: коммерческая и иная тайна, охраняемая законом; персональные данные; интеллектуальная собственность; имущественные права и многие другие.

Нужно отметить, что нередко кибермошенничество отождествляется с понятием «мошенничество в сети Интернет» или «интернет-

мошенничество». Однако помимо Интернета существуют другие компьютерные сети, и с помощью них также могут совершаться мошенничества. Речь идёт, в частности, о «Даркнете». Под «Даркнетом» можно понимать скрытую компьютерную сеть, которая использует нетипичные для Интернета технологии (доверенные «пиры», специальные порты и т.п.). Пользователи «Даркнета» нередко принимают участие в совершении преступлений, в том числе кибермошенничества. Например, они продают предметы, оборот которых ограничен или запрещён: наркотические средства, криптовалюту, оружие и т.п. Нередко сайты в «Даркнете» под видом продажи перечисленных предметов просто похищают деньги покупателей.

Помимо Интернета и Даркнета существуют компьютерные сети, на основе которых работают мессенджеры вроде «FireChat», «Serval Mesh», «Hike» и др. То есть они работают в автономных и самостоятельных сетях, что обеспечивает повышенный уровень анонимности и скрытности для мошенников. Однако в подобных сетях, как правило, ограниченное количество пользователей, поэтому они используются преимущественно для совершения наркопреступлений, а не кибермошенничества.

Если два десятилетия назад, когда в России сеть Интернет только получала распространение, и люди, как правило, критически относились ко всему тому, что читали/смотрели на различных информационных ресурсах, то сейчас он получил не просто повсеместное распространение, но и сами люди стали безраздельно ему доверять. Действительно, частыми способами совершения кибермошенничества является проведение мошеннических аукционов и лотерей. Также злоумышленники часто прибегают к розничной торговле в режиме онлайн, когда происходит привлечение покупателей низкими ценами на различные виды товаров. Потенциальные жертвы предварительно платят за товар, а мошенники доставляют более дешёвый товар (или не доставляют его вовсе). При этом малое количество граждан обращается в полицию, из-за чего кибермошенничество можно

охарактеризовать как преступление с высоким уровнем латентности [Атаманов, с. 140].

Исследователь Р.С. Атаманов, утверждая, что кибермошенничество разнообразно настолько, что требует разработку собственной типологии, делит рассматриваемые преступления на две основные группы [Атаманов, с. 12]:

– кибермошенничества, основанные преимущественно на использовании электронной почты, мессенджеров и/или иных средств обмена сообщениями как основных инструментов воздействия на жертву;

– кибермошенничества, где центральное место отводится применению сайтов.

При рассмотрении кибермошенничества, где посягательство на объект осуществляется преимущественно с использованием возможностей интернет-сайтов автором предложен список основных направлений деятельности мошенников:

1) создание сайта ненастоящих, выдуманных или замаскированных под реальную благотворительную или религиозную организацию, политическую партию, общественное движение и другие, которые якобы ведут сбор пожертвований [Бобровская, с. 364];

2) проведение спам-рассылки и создание сайтов с просьбой о материальной помощи под предлогами помочь людям, якобы попавшим в трудную жизненную ситуацию;

3) мошеннические онлайновые «банки», «финансовые пирамиды» и «инвестиционные фонды», которые обещают высокие проценты по вкладам, а на деле просто закрываются после сбора достаточного количества денежных средств [Бахтеева, с. 35];

4) рассылки и сайты о якобы обнаруженных уязвимостях и «секретных возможностях» в платёжных системах, благодаря которым можно умножить свои деньги, например, отправив их на специальный счёт. К особо изощрённым схемам относятся те, при которых жертва думает, будто она

обманывает мошенника, но в итоге сам становится обманутым [Галяутдинов, с. 399].

К особенностям обстановки совершения кибермошенничества относятся сохранение анонимности владельца мошеннического веб-сайта или рассылки (нередко для общения или другого взаимодействия с жертвами используются выдуманные имена), а также достаточный временной промежуток между приёмом заказа и его исполнением, что позволяет мошенникам обмануть как можно большее количество людей до тех пор, пока их мошенническая схема не будет раскрыта [Евлашкина, с. 54].

Обстановка кибермошенничества предполагает совершение деяния в сети Интернет, то есть в большинстве случаев есть определённый сайт.

Обобщённая схема совершения кибермошенничества состоит из следующих этапов [Коломинов, с. 49]:

1. Размещение (рассылка) заведомо недостоверной информации;

2. Взаимодействие с потенциальной жертвой;

3. Получение денежного перевода.

Также для кибермошенничества характерна собственная следовая картина. Все перечисленные выше действия неизбежно оставляют следы технического характера. Как правило, мошенники понимают, что оставляют подобные электронные следы, поэтому наиболее продвинутые предпринимают попытки не оставить следов, ведущих к ним, то есть прибегают к анонимизации. Кроме того, быстрая работа электронных платёжных систем затрудняет правоохранительным органам отслеживание мошенников.

К следам, которые образуются и сохраняются в ходе совершения кибермошенничества, можно отнести следующие [Грень, с. 76]:

– регистрационные данные на доменное имя;

– логи от взаимодействия с регистратором доменных имён;

– следы от проведения платежа этому регистратору;

– следы при настройке сервера, поддерживающего домен злоумышленников;

– следы от взаимодействия с хостинг-провайдером, у которого размещён веб-сайт: заказ, оплата, настройка, загрузка контента;

– следы от рекламирования веб-сайта: взаимодействие с рекламными площадками, системами баннерообмена, рассылка спама;

– следы от отслеживания активности пользователей на сайте.

При взаимодействии с потерпевшими мошенники оставляют следующие следы:

– следы при приёме заказов (по электронной почте, по мессенджерам, через веб- форму);

– следы от переписки.

Следует привести пример из судебной практики, иллюстрирующий особенности кибермошенничества. Н. создал интернет-магазин с вымышленными именем, логотипом, адресом и другими сведениями. Этот магазин якобы торговал бытовыми товарами. Чтобы замаскировать интернет-магазин под легальный, Н. зарегистрировал в налоговой инспекции коммерческую организацию по продаже бытовых товаров, и арендовал помещение. Также Н. привлёк в качестве инвестора Д., который не знал о преступных намерениях мошенника. Д. был сделан коммерческим директором компании, после чего на его имя был открыт банковский счёт, куда в конченом итоге поступали денежные средства потерпевших. В следующие дни Н. рекламировал магазин в сети «Интернет», предлагая низкие цены, скорую доставку и подделывая положительные отзывы «покупателей». Чтобы похитить как можно больше средств, Н. нанял удалённых сотрудников, которые не знали о его преступных намерениях, чтобы консультировать граждан. Потерпевшие, оплачивая покупку бытовой техники, её не получали, денежные средства Н. присваивал себе. В итоге он похитил более 500 тыс. руб. Суд признал его виновным по ч. 3 ст. 159 УК РФ [68].

Таким образом, кибермошенничество представляет собой один из видов компьютерных преступлений (или киберпреступлений). В самом общем виде оно состоит в том, что обман или злоупотребление доверием осуществляется мошенником посредством применения информационных технологий, среди которых сеть «Интернет», «Даркнет» и другие компьютерные сети.

В широком смысле кибермошенничество – это такое мошенничество, где любой из элементов преступления связан с сетевым пространством. Например, путём создания мошеннических интернет-сайтов предлагаются услуги/товары/работы, заведомо несуществующие, но вводящие в заблуждение граждан. В более узком – это мошенничество, где весь процесс совершения преступления сосредоточен в интернет-пространстве.

Для криминалистической характеристики кибермошенничества характерные следующие наиболее значимые отличия от «традиционного» мошенничества: 1) уникальная следовая картина, где центральное место занимают виртуальные следы; 2) меняющиеся черты личности мошенника: они становятся моложе, и они более продвинуты в вопросах, касающихся использования информационных технологий; 3) новые способы совершения преступлений, которые были невозможны до появления соответствующих технологий: создание интернет-сайтов двойников и т.п.

3.2. Организация расследования кибермошенничества

Криминалистическая методика расследования кибермошенничества подразумевает, что следователь должен рационально сочетать положения как классической методики расследования традиционного мошенничества, так и положения, касающиеся методик расследования компьютерных преступлений. Как было сказано ранее, ключевым структурным элементом криминалистической методики расследования кибермошенничества является способ совершения преступления. Если следователь располагает достоверной

информацией о способе кибермошенничества, то он сможет оптимизировать процесс выдвижения следственной версии относительно других элементов, составляющих предмет доказывания по уголовному делу данной категории.

Способы совершения кибермошенничества можно классифицировать не только по содержанию недостоверной информации, направленной на обман потерпевшего, но и в зависимости от характеристик лица, совершающего данное деяние. Так, кибермошенничество можно разделить на совершённое с использованием служебного положения, т.е. лицом, которое имеет законный доступ к компьютерной информации, в отношении которой было осуществлено противоправное воздействие [Барчуков, с. 61].

Очевидно, что чем большее количество лиц принимало непосредственное участие в совершении кибермошенничества, тем более сложной и проблемной является деятельность следователя по раскрытию подобных преступлений. Действительно, организованная преступная группа имеет больше возможностей, как финансовых, так и технических, чтобы совершить кибермошенничество в отношении большего числа лиц и, кроме того, возложить на того или иного участника группы роль по сокрытию электронных следов преступления.

В наиболее развитых организованных преступных группах мошенники обладают криминальной специализацией, которая выражается в распределении ролей. Так, в группу могут входить лица, которые непосредственно оказывают криминальное воздействие на компьютерную информацию для совершения хищения или приобретения прав на чужое имущество, другие же лица могут осуществлять другие функции, связанные, например, с рекламой мошеннического сайта или поиском и отбором потенциальных жертв [Мещеряков, с. 98].

Одной из проблем, имеющих место при расследовании кибермошенничества, является слабая разработка методики. Для того, чтобы сформировать эффективную криминалистическую методику по расследованию кибермошенничества, необходимо изучать производимые по

данным делам следственные действия и выработать тактические приёмы для их успешного производства [Волчкова, с. 29].

Исследователи и практики называют другие проблемы при организации расследования кибермошенничества. Например, А.Э. Пяткина, расследуя киберпреступления в целом, называет среди обстоятельств, которые затрудняют расследование кибермошенничеств, следующие [Пяткина, с. 181]:

– во-первых, «кибермошенника» выявить и найти гораздо сложнее. Типовые ситуации, связанные с местонахождением мошенника, здесь не актуальны. Дело в том, что он может находиться в другом городе или даже в стране. Кроме того, кибермошенника часто прибегают к тому, чтобы скрыться в интернет-пространстве путём изменения технических характеристик своей сети: смена IP-адреса, применение локальной сети и т.п.;

– во-вторых, многие следы кибермошенничеств существуют в течение короткого времени, после могут быть удалены безвозвратно;

– в-третьих, дистанционный характер совершения преступления;

– в-четвёртых, недостаточные квалификация и технологическая оснащённость сотрудников правоохранительных органов.

Специфические следы, оставляемые в результате совершения кибермошенничества, требуют совершенствовать текущие и разрабатывать принципиально новые тактические средства, а также высокотехнологичные устройства и приспособления для обнаружения и использования в процессе доказывания следов кибермошенничества.

Успех расследования кибермошенничества во многом предопределяется количеством и качеством оперативно-розыскной информации, полученной ещё до возбуждения уголовного дела. Субъекту расследования крайне желательно, учитывая специфику противоправного воздействия на компьютерную информацию при совершении мошенничества, иметь в своём распоряжении уже на этапе, предшествующем

возбуждению уголовного дела, максимально возможный объём сведений по основным аспектам предмета доказывания [Батюкова, с. 348].

Компьютерные технологии, задействованные при совершении кибермошенничества, предполагают особую логику в их применении, которая основана на строгой дисциплине, предъявляемой к мыслительному процессу. У преступников формируется своя собственная логика. Ей должен противостоять следователь и лица, которые ему содействуют. Важным требованием к следователю в таком случае является дисциплинированность, предполагающая способность к самоорганизации и сосредоточенности при решении непростых задач, а также готовность к изучению нового, так как данная сфера развивается стремительными темпами [Ручкин, Фомин, с. 69].

Как правило, исследователями предлагаются организационные изменения в системе правоохранительных органов. Так, А.Р. Братусин считает, что сформировалась потребность в новом специализированном органе, «возможно даже в статусе федерального агентства или министерства, который возьмет на себя решение задач по разработке и реализации Концепции информационной безопасности нового типа, которая будет способна в полной мере дать адекватный ответ на все возрастающие угрозы в информационной сфере» [Братусин, с. 28]. Эту идею следует поддержать, так как один из главных недостатков расследования кибермошенничества – недостаточная техническая квалификация следствия.

3.3. Тактика проведения отдельных следственных действий при расследовании кибермошенничества

Тактика проведения следственных действий при расследовании кибермошенничества в целом совпадает с той, что была рассмотрена во второй главе настоящего исследования. Тем не менее, нужно исследовать главные особенности осуществления следственных действий, которые отражают специфическую природу кибермошенничества.

1. Так, производство обыска (выемки) при кибермошенничестве связано с получением доказательств способа совершения преступления, совершённого с использованием компьютерной техники и телекоммуникационных сетей. Главной целью здесь является обнаружение и изъятие компьютерной техники, на которой остались следы киберпреступления, компьютерной информации, касающейся как самого мошенничества, так и лиц, совершивших это преступление (информация об их нахождении или перемещении), предметы, являющиеся результатом (продуктом) преступления (например, контрафактные компьютерные программы) и документы, содержащие важную информацию для уголовного дела [Русскевич, Фролов, с. 96].

Результаты проведённого обыска (выемки) по делам о мошенничестве в сети Интернет во многом зависят от подготовки к производству следственного действия. На подготовительном этапе обыска (выемки) следователь анализирует исходную информацию, определяет вид, содержание компьютерной информации, предположительно находящейся у преступника; выясняет, на каких материальных носителях может храниться искомая информация; какая компьютерная техника, относящаяся к совершённому кибермошенничеству, может находиться в месте обыска и т.д.

На обзорной стадии следователь внимательно осматривает всё помещение. Внимание следователя должно быть обращено в первую очередь на компьютерную технику, так как именно в ней хранится искомый объект – компьютерная информация. Обнаружив такую технику, рекомендуется обратить внимание на её количество, помещение, на способы подключения телекоммуникационных сетей. Важно изучить состояние техники – включена она или нет; подключены к ней съёмные носители информации или нет; и др. [Муратова, Антонов, с. 77].

После производства обыска (выемки) вся обнаруженная компьютерная техника, содержащая искомую информацию по расследуемому

мошенничеству, перед изъятием должна быть правильно упакована и опечатана.

Например, по при расследовании одного из случаев кибермошенничества следователи провели следующие следственные действия: допросы свидетелей, обыск и выемку на первоначальном этапе расследования. Благодаря этому было установлено, что кибермошенники разослали сотрудникам предприятия электронные письма. Прочтение этих писем активировало вредоносные программы, которые дали преступникам доступ к серверам и программному обеспечению предприятия. В итоге они управляли платёжными сообщениями и перевели на свои банковские счета деньги. Одним из важнейших доказательств по делу стал жёсткий диск с данными о вредоносном программном обеспечении. Суд квалифицировал содеянное по ч. 4 ст. 159.6 УК РФ [77].

2. Особенность допроса применительно к кибермошенничеству состоит в том, что задаваемые следователем вопросы должны учитывать специфику рассматриваемых преступлений. Ведь подозреваемый (обвиняемый) может быть знаком с потерпевшим только через сеть Интернет, а не в реальной жизни. Этот и другие особенности необходимо учитывать при составлении вопросов перед допросом подозреваемого или обвиняемого в кибермошенничестве.

Кроме того, как было указано ранее, предлагается новый элемент криминалистической характеристики мошенничества – характер отношений между мошенником и потерпевшим. Этот элемент, несомненно, должен повлиять на расследование кибермошенничества. Применительно к допросу он может выразиться в том, что следователь узнаёт от допрашиваемого о взаимоотношениях с кибермошенником/потерпевшим, учитывая специфику совершённого деяния.

Е.С. Шевченко, разработавший рекомендации для допроса подозреваемого по кибермошенничеству, рекомендует следователям прибегать к следующим приёмам [Шевченко, с. 9]:

1) привлечь для участия в допросе специалиста, чтобы использовать его специальные знания для более точного и конкретного разговора с допрашиваемым;

2) следователь должен быть готов к тому, что кибермошенник будет использовать свою осведомлённость в вопросах, связанных с компьютерными технологиями. Так, он может, отвечая на вопросы следователя, умышленно использовать много сложных терминов, понятий, жаргонизмов, которые могут быть не понятны следователю. Кроме того, такой способ ответов на вопросы облегчает возможность скрыть обстоятельства кибермошенничества. Это можно называть «интеллектуальным противодействием» при допросе [Ермакова, Менжега, с. 90].

Примером проведения допроса потерпевшего является следующее уголовное дело о кибермошенничестве: гражданке П. пришло сообщение о блокировке её банковской карты. Позже с неё были списаны 500 тыс. руб. В ходе допроса потерпевшая рассказала, что после сообщения она позвонила по указанному в нём номеру – ей ответил мужчина, представившийся сотрудником службы безопасности банка. Он попросил у неё номер банковской карты и кодовое слово [67].

3. Одно из важнейших следственных действий при расследовании кибермошенничества – это осмотр электронных носителей информации. Ведь зачастую только они могут содержать следы преступления. Цель проведения такого осмотра – обнаружить виртуальные следы, после чего сделать их копию на другом носителе компьютерной информации. Впоследствии полученные следу подлежат исследованию экспертами.

Следователь должен позаботиться о материально-техническом обеспечении осмотра, что позволит собрать максимальное количество информации, относимой к расследованию кибермошенничества.

Существуют следующие средства и приёмы, используемые для обнаружения электронных следов [Танасчишин, Климчук, с. 174]:

1) специальные программы: например, из файла данных, записанного в формате изображения по специальному алгоритму обрисовывается изображение;

2) программно-аппаратные средства для криминалистического исследования компьютерных носителей информации («EnCase Forensic Edition» и др.);

3) технические средства: мобильный комплекс по сбору и анализу цифровых данных «UFED»; мобильный подавитель работы смартфонов «Мозаика+» и др.

4. Результаты ведомственного расследования факта интернет-мошенничества могут использоваться следователем при проведении следственных действий и назначении судебных экспертиз. В частности, такая информация позволит: во-первых, формулировать более конкретные вопросы и задания эксперту при подготовке постановления о назначении экспертизы; во-вторых, более ясно представлять себе общую картину преступления, с меньшими трудностями подбирать специалистов для каждого следственного действия; в-третьих, выявить и разыскать сообщников интернет-мошенника, если они были [Смирнов, Кузина, с. 110].

Один из путей совершенствования тактики расследовании кибермошенничества – это появление новых и совершенствование уже существующих видов судебных экспертиз. Например, компьютерно-техническая экспертиза позволяет исследовать виртуальные следы кибермошенничества, в частности, программы, которые использовались мошенниками для несанкционированного доступа к учётной записи или электронному кошельку потерпевшего. К специфическим следам можно отнести «лог-файлы», которые представляют собой текстовый файл, содержащий историю о сетевых действиях пользователя компьютера, в том числе сетевые адреса, с которых осуществлялся запрос к компьютеру потерпевшего. В итоге следствие может установить, какому лицу принадлежит тот или иной сетевой адрес устройства.

Очевидно, что особенности расследования кибермошенничества не сводятся только к проведению следственных действий с учётом специфики виртуальных следов. Исследователями высказывается идея о повышенной роли непроцессуальных форм применения специальных знаний по данным делам. Так, Р.С. Атаманов считает, что следствие должно прибегать к следующему [Атаманов, с. 81]:

1) к консультациям следователя по вопросам, требующим специальных познаний;

2) к оказанию технической помощи следователю (например, помощь в установке отслеживающего программного обеспечения на компьютер подозреваемого в кибермошенничестве);

3) к использованию результатов проверок, проводимых работниками различных ведомств и инспекций;

4) к использованию материалов предварительного экспертного исследования различных объектов (например, вещественных доказательств); и др.

Е.С. Шевченко, развивая описанную выше идею, высказывает мысль о том, что сложность следственных действий при кибермошенничестве требует развития практики создания специальных следственно-оперативных групп. В них предлагается включать специалистов, которые обладают специальными знаниями и навыками для расследования киберпреступлений [Шевченко, с. 27].

С этой идеей следует согласиться. Дело в том, что кибермошенничества, как неоднократно отмечалось ранее, часто требуют исследования большого объёма компьютерных данных, представленных в виде различных и сложных для выявления и изучения виртуальных следов. Маловероятно, что следователь будет в состоянии сделать это так же эффективно, как и профессионал, который специализируется исключительно на киберпреступлениях.

Можно сделать вывод, при производстве следственных действий по делам о кибермошенничестве используются в основном стандартные, проверенные тактические приёмы, пригодные для раскрытия других видов преступлений. Однако кибермошенничество всегда требует от следователя и других субъектов, например специалиста, пристальное внимание обращать именно на компьютеры и другие технические устройства, так как без их пристального изучения невозможно обнаружить следы виртуального преступления, а значит, раскрыть данное деяние. Поэтому разработка методики расследования кибермошенничества, в том числе тактики производства следственных действий по данным делам, должна акцентироваться на возможности следователя ориентироваться в технологиях, понимать все способы совершения кибермошенничества, а также эффективно взаимодействовать с привлекаемыми специалистами.

Таким образом, тактика проведения отдельных следственных действий при расследовании кибермошенничества должна учитывать следующие ключевые моменты:

– во-первых, следователь может использовать тактику, характерную для расследования традиционных видов мошенничества, однако с учётом специфики кибермошенничества. В частности, учитывать, что виртуальные следы во многих случаях могут быть обнаружены только специалистами;

– во-вторых, любое следственное действие может потребовать специальных знаний. Например, допрос мошенника в качестве подозреваемого будет более полным и полезным для расследования, если следователь будет иметь представление о компьютерных технологиях и о новых способах мошенничества с применением последних;

– в-третьих, из двух названных особенностей следует, что организация расследования кибермошенничества требует постоянной поддержки следствия со стороны специалистов и экспертов. Поэтому следует поддержать предложение о создании специальных следственно-оперативных групп, куда могут быть включены специалисты, обладающие специальными

знаниями и навыками для расследования киберпреступлений. Сюда же следует отнести непроцессуальные формы применения специальных знаний по данным делам. Например, оказание технической помощи следователю;

– в-четвёртых, следователю рекомендуется обращать повышенное внимание на предложенный новый элемент криминалистической характеристики мошенничества – характер отношений между кибермошенником и потерпевшим. Применительно к допросу это может выразиться в том, что следователь узнаёт от допрашиваемого лица о взаимоотношениях с кибермошенником/потерпевшим. В частности, следователю рекомендуется узнать о том, с какой учётной записью потерпевший общался; под каким именем мошенник представился; сколько прошло времени с первого «контакта» и до момента совершения преступления; связывался или нет потерпевший с мошенником после того, как обнаружил хищение денежных средств; и др. Вопросы зависят от того, какой именно способ совершения кибермошенничества был использован преступником.

ЗАКЛЮЧЕНИЕ

Исследование теории и практика расследования мошенничества позволило прийти к следующим выводам:

1. Криминалистическая характеристика мошенничества показывает, насколько исследуемые преступления являются разнообразным и стремительно меняющимся.

Сделан вывод о неполноте криминалистической характеристики мошенничества без такого элемента, как связь (или характер отношений) между мошенником и потерпевшим. Предлагаемый элемент отразит одну из важнейших особенностей мошенничества – наличие близкой связи между мошенником и потерпевшим, ведь нередко преступление совершается в результате сложных, продуманных и последовательных действий преступника: поиск жертвы, применение «легенды», скрытие от потерпевшего и т.п.

Кроме того, характер отношений между мошенником и потерпевшим органично сочетает в себе другие элементы мошенничества, такие как способ его совершения, личность преступника и др. Более того, этот элемент неразрывно связан с методикой и тактикой расследования мошенничества, которая предполагает обязательное установление связей между всеми участниками преступления и потерпевшим. Наконец, он не только более точно отразит социальную направленность мошенничества, но и сможет положительно повлиять на развитие тактики и методики расследования.

2. Характеристика способов совершения мошенничества доказывает, что исследуемое преступление является крайне разнообразным с точки зрения его криминалистической характеристики.

Для расследования мошенничества наиболее важными являются следующие характерные черты способов совершения мошенничества:

– во-первых, постоянное обновление и появление новых способов совершения мошенничества. Наглядным примером является

«кибермошенничество», которое уже включает в себя целый ряд различных мошеннических схем, где задействованы компьютеры, сеть «Интернет» и другие информационные технологии;

– во-вторых, разные способы мошенничества могут комбинироваться друг с другом. Например, мошенничество при облачном майнинге сочетает в себе черты финансовой пирамиды, а также предполагает создание сайта-двойника;

– в-третьих, новые способы мошенничества возникают стремительно из-за изменений, которые происходят в жизни общества. Например, много новых способов мошенничества возникло из-за пандемии. То есть преступники находят способы воспользоваться текущими условиями жизни, новыми технологиями и другими изменениями. Следовательно, это приводит к устареванию устоявшихся на практике методик по расследованию мошенничества;

– в-четвёртых, способы мошенничества всё чаще основаны на положениях науки (психологии, социологии и др.). Выражением этого является применение «социальной инженерии», т.е. приёмов и методов для психологического манипулирования человеком. Следовательно, механизм совершения мошенничества становится всё более сильно зависимым от личностей преступника и потерпевшего.

3. В основе типичных следственных ситуаций при расследовании мошенничества лежит, во-первых, характер взаимоотношений между мошенником и потерпевшим: они могут быть знакомы друг с другом или нет. Во-вторых, местонахождение мошенника: оно может быть известно следствию или нет. При этом мошенник может скрываться в месте своего постоянного жительства, у знакомых или в другом населённом пункте.

Указанные факторы предопределяют программу расследования мошенничества. Она включает в себя комплекс следственных и оперативных мероприятий, которые должны не только установить личность мошенника,

но и понять, каким именно способом он совершил мошенничество и было ли оно вообще.

Для расследования мошенничества крайне важно, чтобы следственные органы действовали быстро и оперативно, а также адаптировались под меняющийся ход расследования. Ключевая задача – это получение как можно больших сведений о событии преступления, что требует проведения осмотра места происшествия, допросов и обысков.

4. Тактика проведения отдельных следственных действий при расследовании мошенничества наглядно отражает разнообразие исследуемого преступления.

Для всех следственных действий при расследовании мошенничества так или иначе характерно то, что общие тактические приёмы могут быть легко дополнены и развиты частными рекомендациями, когда речь идёт о необходимости раскрыть какой-либо специфический вид или способ мошенничества. Например, предмет допроса, как и в случае с потерпевшим, зависят от вида и способа мошенничества. Если оно было совершено путём создания финансовой пирамиды, то целесообразно допрашивать мошенника о том, что связано с деятельностью подобной организации. Например, о продвижении и рекламе.

5. Была исследована проблема расследования кибермошенничества. Оно представляет собой один из видов компьютерных преступлений (или киберпреступлений), где обман или злоупотребление доверием осуществляется мошенником посредством применения информационных технологий, среди которых сеть «Интернет», «Даркнет» и другие компьютерные сети.

В широком смысле кибермошенничество – это такое мошенничество, где любое из элементов преступления связан с сетевым пространством. Например, путём создания мошеннических интернет-сайтов предлагаются услуги/товары/работы, заведомо несуществующие, но вводящие в

заблуждение граждан. В более узком – это мошенничество, где весь процесс совершения преступления сосредоточен в интернет-пространстве.

Для криминалистической характеристики кибермошенничества характерные следующие наиболее значимые отличия от «традиционного» мошенничества:

1) уникальная следовая картина, где центральное место занимают виртуальные следы;

2) меняющиеся черты личности мошенника: они становятся моложе, и они более продвинуты в вопросах, касающихся использования информационных технологий;

3) новые способы совершения преступлений, которые были невозможны до появления соответствующих технологий: создание интернет-сайтов двойников и т.п.;

4) оно является в основном дистанционным, т.е. кибермошенник и потерпевший могут находиться как в разных городах, так и в разных странах, что также затрудняет расследование кибермошенничества.

6. Что касается тактики проведения отдельных следственных действий при расследовании кибермошенничества, то рекомендуется следующее:

– во-первых, следователь может использовать тактику, характерную для расследования традиционных видов мошенничества, однако с учётом специфики кибермошенничества. В частности, учитывать, что виртуальные следы во многих случаях могут быть обнаружены только специалистами;

– во-вторых, любое следственное действие может потребовать специальных знаний. Например, допрос мошенника в качестве подозреваемого будет более полным и полезным для расследования, если следователь будет иметь представление о компьютерных технологиях и о новых способах мошенничества с применением последних;

– в-третьих, из двух названных особенностей следует, что организация расследования кибермошенничества требует постоянной поддержки следствия со стороны специалистов и экспертов. Поэтому следует

поддержать предложение о создании специальных следственно-оперативных групп, куда могут быть включены специалисты, обладающие специальными знаниями и навыками для расследования киберпреступлений. Сюда же следует отнести непроцессуальные формы применения специальных знаний по данным делам. Например, оказание технической помощи следователю;

– в-четвёртых, следователю рекомендуется обращать повышенное внимание на предложенный новый элемент криминалистической характеристики мошенничества – характер отношений между кибермошенником и потерпевшим. Применительно к допросу это может выразиться в том, что следователь узнаёт от допрашиваемого лица о взаимоотношениях с кибермошенником/потерпевшим.

Таким образом, предложенные рекомендации по совершенствованию практики расследования кибермошенничества могут быть положены в основу дальнейшей разработки тактики расследования мошенничества.

СПИСОК ИСТОЧНИКОВ

Нормативные правовые акты

1.Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ: в послед. ред. // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

2.Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ: в послед. ред. // Собрание законодательства Российской Федерации. – 2001. – № 52 (ч. 1). – Ст. 4921.

3.Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»: в ред. от 30.12.2021 // Собрание законодательства РФ. – 2003. – № 28. – Ст. 2895.

4.Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части противодействия хищению денежных средств» от 27 июня 2018 г. № 167-ФЗ: в послед. ред. // Собрание законодательства РФ. – 2018. – № 27. – Ст. 3950.

Научная литература

5.Анненков С.И. Типичные следственные ситуации, возникающие по уголовным делам о мошенничестве / С.И. Анненков // Проблемы уголовного процесса, криминалистики и судебной экспертизы. – 2018. – № 1 (11). – С. 44-48.

6.Атаманов Р.С. Основы методики расследования мошенничества в сети Интернет: дисс. … канд. юрид. наук: 12.00.12 / Р.С. Атаманов. – М., 2012. – 182 с.

7.Атаманов Р.С. Криминалистическая характеристика мошенничества / Р.С. Атаманов // Российский следователь. – 2014. – № 41. – С. 12-14.

8.Барчуков В.К. Терминология мошенничества в сфере компьютерной информации / В.К. Барчуков // Пробелы в российском законодательстве. Юридический журнал. – 2017. – № 2 (18). – С. 60-62.

9.Бахтеева Д.А. Рост киберпреступности на фоне пандемии коронавирусной инфекции COVID-19 / Д.А. Бахтеева // Проблемы и перспективы развития уголовно-исполнительной системы России на современном этапе: сб. ст. – 2020. – С. 34-37.

10.Белицкий В.Ю. Предмет допроса сотрудников организации – «финансовой пирамиды», маскирующей свою деятельность под кредитный кооператив / В.Ю. Белицкий // Актуальные проблемы современности. – 2019. – № 3 (25). – С. 18-22.

11.Белицкий В.Ю. Распространённые виды мошенничеств в сети Интернет / В.Ю. Белицкий // Актуальные проблемы современности. – 2020. – № 2 (28). – С. 31-36.

12.Белкин Р.С. Криминалистика: учебник / Р.С. Белкин. – М.: Норма, 2020. – 928 с.

13.Бобровская М.В. Способ совершения дистанционного мошенничества как элемент его криминалистической характеристики / М.В. Бобровская // Криминалистика – наука без границ: сб. ст. – СПб, 2021. – С. 363-367.

14.Батюкова В.Е. Предупреждение кибермошенничества в период Covid-19 / В.Е. Батюкова // Образование и право. – 2020. – № 11. – С. 347-349.

15.Братусин А.Р. О необходимости подготовки на базе вузов МВД и Силовых Ведомств РФ специалистов в области информационной безопасности / А.Р. Братусин А.Р. // Проблемы современного педагогического образования. – 2019. – № 13. – С. 27-30.

16.Бунина А.Ф. Характеристика личности мошенников / А.Ф. Бунина, А.К. Мовсесян // Актуальные проблемы экономики, социологии и права. – 2018. – № 4. – С. 24-25.

17.Быкова Н.В. Выявление и раскрытие мошенничества в сфере страхования: дисс. … канд. юрид. наук: 12.00.09 / Н.В. Быкова. – М., 2009. – 205 с.

18.Виноградова К.А. Расследование мошенничества в сфере кредитования: дисс. … канд. юрид. наук: 12.00.12 / К.А. Виноградова. – М., 2018. – 282 с.

19.Волеводз А.Г. Противодействие компьютерным преступлениям / А.Г. Волеводз. – М.: Юрлитинформ, 2011. – 80 с.

20.Волчкова А.А. Проблемы противодействия киберпреступлениям правоохранительными органами / А.А. Волчкова // Уголовное право: стратегия развития в XXI в: сб. ст. – 2019. – С. 26-30.

21.Галченкова В.Ю. Использование специальных знаний при расследовании мошенничества, совершённого с использованием сети «Интернет» / В.Ю. Галченкова // Наука и бизнес: пути развития. – 2021. – № 11 (125). – С. 45-47.

22.Галяутдинов Р.Ф. Новые схемы кибермошенничества / Р.Ф. Галяутдинов // Евразийский юридический журнал. – 2022. – № 6 (169). – С. 398-400.

23.Гафнер В.В. Информационная безопасность: учебное пособие / В.В. Гафнер. – Ростов-на-Дону: «Феникс», 2012. – 174 с.

24.Гладких В.И. Компьютерное мошенничество / В.И. Гладких // Российский следователь. – 2014. – № 22. – С. 25-31.

25.Грень И.В. Компьютерная преступность / И.В. Грень. – Минск: «Новое знание», 2010. – 93 с.

26.Грунтовая Г.А. Некоторые особенности криминалистической характеристики мошенничеств с использованием электронных средств платежа / Г.А. Грунтовая // Вестник науки. – 2018. – Т. 5. № 6 (6). – С. 14-18.

27.Драпкин Л.Я. Криминалистика: учебник / Л.Я. Драпкин, В.Н. Карагодин. – М.: «Зерцало-М», 2011. – 768 с.

28.Евлашкина А.В. Криминалистическая характеристика отдельных видов мошенничества в сфере компьютерной информации / А.В. Евлашкина, М.В. Кардашевская // Актуальные проблемы кибербезопасности в сети Интернет: сб. ст. – 2020. – С. 52-55.

29.Едиджи Ф.А. Некоторые элементы криминалистической характеристики мошенничества / Ф.А. Едиджи, М.В. Головин // / Эпомен. – 2021. – № 55. – С. 179-185.

30.Ермакова Е.С. Особенности методики расследования киберпреступлений: проблемы и пути их преодоления / Е.С. Ермакова, М.М. Менжега // Сфера

знаний в вопросах культуры, науки и образования: сб. ст. – Казань, 2018. – С. 88-91.

31.Еськова Л.К. Новые преступные способы мошенничества в период пандемии коронавирусной инфекции / Л.К. Еськова, В.В. Рябчиков // Гуманитарные, социально-экономические и общественные науки. – 2020. – № 11. – С. 68-70.

32.Зиннуров Ф.К. Социальное мошенничество с использованием средств сотовой связи (ч. 2 ст. 159 УК РФ): учебно-практическое пособие / Ф.К. Зиннуров. – М.: ЮНИТИ-ДАНА; Закон и право, 2017. – 191 с.

33.Иванова В. Некоторые особенности криминалистической характеристики мошенничества / В. Иванова // Актуальные проблемы реализации российского права: сб. ст. – Рязань, 2018. – С. 95-97.

34.Казинская С.Н. Особенности допроса подозреваемого при расследовании мошенничества / С.Н. Казинская // Расследование преступлений: проблемы и пути их решения. – 2015. – № 1 (7). – С. 119-124.

35.Коломинов В.В. Мошенничество в сфере компьютерной информации как объект криминалистического познания / В.В. Коломинов // Вестник ВГУ. – 2014. – № 3(15). – С. 48-53.

36.Крамской В.В. Противодействие распространению кибермошенничества: новые возможности в расследовании и пути совершенствования законодательства / В.В. Крамской // Право: история и современность. – 2021. – № 2 (15). – С. 79-87.

37.Лазарев Д.В. Лжеэкспортное мошенничество: понятие, криминалистическая характеристика, программа расследования: дисс. … канд. юрид. наук: 12.00.09 / Д.В. Лазарев. – СПб., 2004. – 208 с.

38.Маилян А.В. Актуальные вопросы расследования и раскрытия кибермошенничества «фишинг» / А.В. Маилян // Философия права. – 2022. – № 2 (101). – С. 112-115.

39.Малыхина Н.И. Алгоритм действий следователя в типовых ситуациях расследования мошенничеств, совершённых с использованием сети

«Интернет» / Н.И. Малыхина, С.В. Кузьмина // Вестник Томского государственного университета. – 2021. – № 462. – С. 238-247.

40.Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации / В.А. Мещеряков. – Воронеж: Изд-во ВГУ, 2014. – 129 с.

41.Муратова Н.Г. Технология доказывания транснационального кибермошенничества / Н.Г. Муратова, И.О. Антонов // Проблемы криминалистики. – 2015. – № 8 (20). – С. 71-77.

42.Низаева С.Р. Расследование мошенничества в сфере оборота жилой недвижимости (проблемы теории и практики): дисс. … канд. юрид. наук: 12.00.12 / С.Р. Низаева. – Калининград, 2017. – 245 с.

43.Нугаева Э.Д. Особенности расследования мошенничества при оказании оккультных услуг: дисс. … канд. юрид. наук: 12.00.12 / Э.Д. Нугаева. – Уфа, 2018. – 251 с.

44.Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования: монография / А.Ф. Абдулвалиев и др. – Тюмень: Изд-во Тюменского государственного университета, 2021. – 376 с.

45.Простосердов М.А. Преступления против собственности: учебное пособие / М.А. Простосердов. – М.: РГУП, 2017. – 76 с.

46.Пяткина А.Э. Проблемы расследования киберпреступлений в условиях современной России / А.Э. Пяткина // Государственная служба и кадры. – 2021. – № 2. – С. 181-183.

47.Решняк О.А. Организация расследования мошенничеств, совершенных с использованием сети «Интернет», на первоначальном и последующем этапах / О.А. Решняк, С.А. Ковалев // Вестник Волгоградской академии МВД России. – 2020. – № 2 (53). – С. 106-111.

48.Россинская Е.Р. Криминалистика. Учебник / Е.Р. Россинская. – М.: Норма: Инфра-М, 2020. – 463 с.

49.Русскевич Е.А. Мошенничество в сфере компьютерной информации: монография / Е.А. Русскевич, М.Д. Фролов. – М.: ИНФРА-М, 2020. – 148 с.

50.Ручкин В.Н. Современные компьютерные технологии и криминалистика: учебное пособие / В.Н. Ручкин, В.В. Фомин. – Рязань: Академия ФСИН России, 2019. – 101 с.

51.Сабырбаева А. Электронные доказательства как новый вид доказательств при расследовании современных форм мошенничества / А. Сабырбаева // Журнал «Review of law sciences». – 2020. – № 9. – С. 215-220.

52.Сафонов О.М. Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений / О.М. Сафонов. – М.: Норма, 2015. – 122 с.

53.Смирнов В.М. Наиболее популярные схемы кибермошенничества в сети «Интернет» / В.М. Смирнов, А.В. Кузина // Тенденции развития науки и образования. – 2022. – № 86-1. – С. 110-113.

54.Старостенко О.А. Закономерности становления и развития кибермошенничества в России и за рубежом / О.А. Старостенко // Вестник Уральского юридического института МВД России. – 2021. – № 1. – С. 138-143.

55.Старостенко Н.И. Криминалистическое понимание механизма совершения мошенничества с использованием методов социальной инженерии / Н.И. Старостенко // Общество и право. – 2021. – № 1 (75). – С. 71-76.

56.Старцева Е.А. Тактические особенности производства следственного осмотра при расследовании мошенничества в сфере компьютерной информации / Е.А. Старцева // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2021. – № 1 (53). – С. 167-172.

57.Танасчишин А.А. Об опыте расследования мошенничества с использованием компьютерных технологий сети «Интернет» / А.А. Танасчишин, Ю.А. Климчук Ю.А. ИБ СД МВД России. – 2013. – № 1 (155). – С. 171-179.

58.Федотов А.А. Криминалистическая характеристика мошенничества / А.А. Федотов, А.К. Зебницкая // Вопросы науки и образования. – 2018. – № 28 (40). – С. 23-25.

59.Чумаков А.В. Особенности методики расследования мошенничества при получении выплат: дисс. … канд. юрид. наук: 12.00.12 / А.В. Чумаков. – Барнаул, 2018. – 239 с.

60.Шаталкина Н.А. Тактические задачи очной ставки при расследовании мошенничества / Н.А. Шаталкина // Вестник Барнаульского юридического института МВД России. – 2021. – № 1 (40). – С. 126-128.

61.Шатилов А.В. Нравственно-психологические характеристики личности мошенника – участника организованной преступной группы / А.В. Шатилов // Вестник Саратовской государственной юридической академии. – 2018. – № 6 (125). – С. 192-200.

62.Шевко Н.Р. Кибермошенничество в России: способы совершения и пути решения проблемы / Н.Р. Шевко // Вестник НЦБЖД. – 2021. – № 1 (47). – С. 125-130.

63.Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: автореф. дисс. … канд. юрид. наук: 12.00.12 / Е.С. Шевченко. – М., 2016. – 29 с.

64.Шут О.А. Мошенничество в социальных сетях и способы его осуществления / О.А. Шут // Вестник Омского университета. – 2020. – Т. 17. № 4. – С. 97-106.

65.Яблоков Н.П. Криминалистика. Учебник / Н.П. Яблоков. – М.: Юрист, 2019. – 781 с.

Материалы правоприменительной практики

66.Приговор Бердюжского районного суда Тюменской области от 6 октября 2020 г. по делу № 1-48/2020 [Электронный ресурс] // «Судебные и

нормативные акты РФ»: сайт. – URL: //sudact.ru/regular/doc/qOm2FGsOQB5N/ (дата обращения: 12.07.2021).

67.Приговор Октябрьского районного суда г. Иваново от 12 февраля 2020 г. по делу № 1-2/2020 [Электронный ресурс] // «Судебные и нормативные акты РФ»: сайт. – URL: //sudact.ru/regular/doc/prSVjvJC3dLu/ (дата обращения: 02.05.2022).

68.Приговор Яшкинского районного суда Кемеровской области от 8 июня 2021 г. по делу № 1-61/2021 [Электронный ресурс] // «Судебные и нормативные акты РФ»: сайт. – URL: //sudact.ru/regular/doc/C4YHMoqYbnHR/ (дата обращения: 02.05.2022).

69.Приговор Голышмановского районного суда Тюменской области от 30 июля 2020 г. по делу № 1-115/2020 [Электронный ресурс] // «Судебные и нормативные акты РФ»: сайт. – URL: //sudact.ru/regular/doc/wYyUJZbGO5oJ/ (дата обращения: 13.07.2021).

70.Приговор Бердюжского районного суда Тюменской области от 6 октября 2020 г. по делу № 1-48/2020 // «Судебные и нормативные акты РФ»: сайт. URL: //sudact.ru/regular/doc/qOm2FGsOQB5N/ (дата обращения: 09.01.2022).

71.Приговор Калининского районного суда г. Тюмени Тюменской области от 27 июля 2020 г. по делу № 1-185/2020 [Электронный ресурс] // «Судебные и нормативные акты РФ»: сайт. – URL: //sudact.ru/regular/doc/gBqW8N94lJmw/ (дата обращения: 12.07.2021).

72.Приговор Ленинского районного суда г. Тюмени Тюменской области от 3 февраля 2020 г. по делу № 1-1431/2019 [Электронный ресурс] // «Судебные и нормативные акты РФ»: сайт. – URL: //sudact.ru/regular/doc/8jc7KDZQEmm9/ (дата обращения: 13.07.2021).

73.Приговор Ленинского районного суда г. Тюмени Тюменской области от 27 июля 2020 г. по делу № 1-1070/2020 [Электронный ресурс] // «Судебные и нормативные акты РФ»: сайт. – URL: //sudact.ru/regular/doc/Zx9fGJsUtlV0/ (дата обращения: 13.07.2021).

74.Приговор Сургутского городского суда ХМАО-Югры от 16 декабря 2018 г. по делу № 1-1286/2018 // [Электронный ресурс]. Сайт «Судебные и нормативные акты РФ». – URL: http://sudact.ru/regular/doc/PzVIBnC3oCQx/ (дата обращения: 10.01.2022).

75.Приговор Ленинского районного суда г. Тюмени Тюменской области от 16 мая 2019 г. по делу № 1-20/2019 [Электронный ресурс] // «Судебные и нормативные акты РФ»: сайт. – URL: //sudact.ru/regular/doc/HxP89erYhSxq/ (дата обращения: 14.07.2021).

76.Апелляционное определение СК по гражданским делам Курганского областного суда от 16 января 2018 г. по делу № 33-180/2018 [Электронный ресурс] // СПС «Гарант»: сайт. – URL: https://www.garant.ru/files/4/5/1290354/apellyatsionnoe_opredelenie_sk_po_grag danskim_delam_kurganskogo_oblastnogo_suda_ot_16_yanvarya_2018_godu.doc (дата обращения: 09.01.2022).

77.Постановление Московского городского суда от 16 марта 2018 г. по делу № 4у-1053/2018 [Электронный ресурс] // СПС «Гарант»: сайт. – URL: https://base.garant.ru/301893533/ (дата обращения: 09.01.2022).

Интернет-источники

78. В «Сбербанке» назвали Днепр столицей телефонного мошенничества [Электронный ресурс] // «РИА Новости»: сайт. – URL: //sudact.ru/regular/doc/wYyUJZbGO5oJ/ (дата обращения: 02.05.2022).

79. Иностранные женихи-мошенники придумали новую схему развода россиянок [Электронный ресурс] // Газета «Московский комсомолец»: сайт. – URL: https://www.mk.ru/social/2021/01/26/inostrannye-zhenikhimoshenniki-pridumali-novuyu-skhemu-razvoda-rossiyanok.html (дата обращения: 02.05.2022).

80.Как обманывают мошенники [Электронный ресурс] // «ПАО Сбербанк»: сайт. – URL: https://www.sberbank.ru/ru/s_m_business/pro_business/kak-moshenniki-obmanyvayut-klientov-bankov/ (дата обращения: 12.09.2021).

81.Отчёт о числе осуждённых по всем составам преступлений Уголовного кодекса РФ за 2021 г. [Электронный ресурс] // Официальный сайт Судебного департамента при Верховном Суде РФ. – Режим доступа: http://www.cdep.ru/index.php?id=79&item=6121 (дата обращения: 02.05.2022).