

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования
«Уфимский юридический институт Министерства внутренних дел
Российской Федерации»

Кафедра криминалистики

ДИПЛОМНАЯ РАБОТА

на тему **«ОСОБЕННОСТИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ
СОВРЕМЕННЫХ СПОСОБОВ СОВЕРШЕНИЯ МОШЕННИЧЕСТВА
(ПО МАТЕРИАЛАМ ТЕРРИТОРИАЛЬНОГО
ОРГАНА ВНУТРЕННИХ ДЕЛ)»**

Выполнил
Власов Игорь Сергеевич
обучающийся по специальности
40.05.01 Правовое обеспечение
национальной безопасности
2016 года набора, 6101 учебной группы

Руководитель
заместитель начальника кафедры
кандидат юридических наук, доцент
Хакимова Эльмира Робертовна

К защите рекомендуется
рекомендуется / не рекомендуется

Начальник кафедры _____

Э.Д. Нугаева

подпись

Дата защиты: « ___ » _____ 2022 г. Оценка _____

ПЛАН

Введение.....	3
Глава 1. Уголовно-правовая и криминалистическая характеристики мошенничества	6
§ 1. Уголовно-правовая характеристика мошенничества	6
§ 2. Основные элементы криминалистической характеристики мошенничества	12
§ 3. Современные виды мошенничества.....	15
Глава 2. Раскрытие и расследование отдельных видов мошенничества.....	24
§ 1. Особенности раскрытия и расследования мошенничества в сфере кредитования.....	24
§ 2. Особенности раскрытия и расследования дистанционного мошенничества	30
Заключение	46
Список использованной литературы	50

ВВЕДЕНИЕ

Актуальность исследования обусловлена тем, что на протяжении столетий уголовно-правовая защита собственности считалась (и продолжает считаться) одним из важнейших направлений уголовной политики и от того, насколько эффективны были механизмы, обеспечивающие эту защиту, зависело политическое, экономическое и социальное будущее государства. В XXI веке новые криминальные угрозы, подрывающие устои постиндустриального мира, вынудили отечественного и законодателя активизировать деятельность по изменению сложившегося уголовно-правового регулирования отношений, связанных с охраной собственности, криминализировать ранее неизвестные посягательства на собственность, к числу которых относится, в том числе мошенничество.

В современном мире проблемы выявления и расследования новых видов мошенничества актуальны как никогда. В связи с развитием и повсеместным внедрением информационных технологий становится проще осуществлять данные преступления. Стоит отметить, что обстановка в стране также оказывает влияние на появление новых возможностей и способов совершения дистанционных мошенничеств.

Борьба в нашей стране с разными видами мошенничества всегда остается актуальной. Жизнь не стоит на месте, появляются новые формы мошенничества, само мошенничество приобретает достаточно большие масштабы. Формы мошенничества изменяются, и, наряду со «старыми» формами (карты, наперстки, денежные куклы), то есть так называемое «уличное» мошенничество, либо мелкое мошенничество, которое выражается в обманном действии при доставке товаров, либо при производстве определенных работ, за которые уплачен аванс.

В России из-за распространения коронавирусной инфекции и в связи с переходом на удаленную работу возникли новые причины и основания для использования безналичных расчетов. Заккрытие большинства точек продаж

также способствовало увеличению количества случаев мошенничества, т. к. владельцы инвестиционных фондов более позитивно, чем обычно, отреагировали на предложения товаров и услуг на онлайн-платформах, часто используемых мошенниками. Соответственно, современная реальность требует от правоохранительных органов совершенствования методов расследования рассматриваемых преступлений.

Степень научной разработанности темы. Проблемы расследования мошенничества на протяжении многих десятилетий рассматривались в междисциплинарных работах многих ученых в области уголовного, уголовно-процессуального права, криминологии, криминалистики. Отдельные вопросы темы освещались в работах И.С. Арзамерсаева, А.А. Денисова, Е.А. Зариповой, Н.А. Колесниковой, М.О. Потемкиной, О.В. Полстовалова, Н.П. Яблокова, Л.В. Яковлевой и др.

Объектом исследования выступают общественные отношения, возникающие в процессе раскрытия и расследования мошенничества.

Предметом исследования стали нормы уголовного и уголовно-процессуального законодательства Российской Федерации, регламентирующие деятельность по раскрытию и расследованию мошенничества.

Цель исследования является всестороннее изучение особенностей раскрытия и расследования современных способов совершения мошенничества.

Задачи исследования:

- дать уголовно-правовую характеристику мошенничества;
- описать основные элементы криминалистической характеристики мошенничества;
- рассмотреть типичные следственные ситуации и версии первоначального этапа расследования дел данной категории;
- выявить особенности проведения отдельных следственных действий, характерных производством именно на первоначальном этапе расследования.

Теоретическую базу исследования составляют фундаментальные теоретические положения общей теории права, труды российских ученых-

процессуалистов, а также ученых в иных областях научного знания, имеющих теоретическое значение для расследования дознавателем современных видов мошенничества.

Нормативная база исследования включает в себя Конституцию Российской Федерации, уголовно-процессуальное законодательство, иное федеральное законодательство РФ, а также судебные акты Верховного Суда РФ и материалы судебной практики, имеющие существенное значение для исследуемой темы.

Методы исследования. В работе использовались методы формальной логики, сравнительного правоведения, системного и структурно-функционального анализа.

Практическая значимость исследования состоит в том, что выводы, предложения и рекомендации автора могут быть использованы в законотворческом процессе и в правоприменительной деятельности.

Структура работы. Дипломная работа состоит из введения, двух глав, включающих в себя пять параграфов, заключения и списка использованной литературы.

ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ И КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКИ МОШЕННИЧЕСТВА

§ 1. Уголовно-правовая характеристика мошенничества

Обеспечение своевременного и действенного расследования мошенничества – весьма сложная и острая проблема, которая находится в зависимости от политической, социальной и экономической ситуации в стране.

В соответствии с уголовным законом мошенничество понимается как хищение чужого имущества или приобретение права на чужое имущество путем обмана или же злоупотребления доверием¹.

Норма общей части уголовного права устанавливает признаки о составе преступления, представляющие собой совокупность объективных и субъективных признаков, и в сумме определяют общественно-опасное деяние как преступление. В состав преступления входят: объект, объективная сторона, субъект, субъективная сторона. Рассмотрим их более подробно.

Известно, что объектом мошенничества являются материальные и нематериальные ценности, подвергающиеся преступному воздействию.

Предметом преступления являются вещи материальных или интеллектуальных ценностей, воздействуя на которые преступник нарушает общественные отношения, охраняемые уголовным законом. Предмет мошенничества должен обладать экономическим признаком, т. е. иметь стоимость, а также обладать юридическим признаком – мошенничество возможно только в отношении чужого имущества¹. При квалификации мошенничества, необходимо понимать, что предметом мошенничества не будет выступать интеллектуальная собственность, информация, идеи, иные результаты интеллектуальной собственности, а также коммерческая тайна,

¹ Филиппов А. Р. Феномен мошенничества в России XXI века: уголовно-правовая, криминологическая и социально-психологическая характеристика // Юридическая наука: история и современность. 2021. № 6. С. 134.

товарный знак и знак обслуживания. Однако если вся эта информация и идеи зафиксированы на материальном носителе, то они являются предметом рассматриваемого преступного деяния.

Объективная сторона – одна из частей преступления, характеризующаяся внешним проявлением опасного поведения, причинившего вред лицу, охраняемого уголовным законом.

Основными признаками объективного характера мошенничества являются изъятие и (или) обращение имущества в пользу мошенника или иных лиц, противоправность, безвозмездность, ущерб собственнику имущества или иному владельцу, следствия и причинная связь.

В качестве факультативных признаков мошеннического преступления можно назвать место, обстановку, время и способ совершения преступления².

Мошенничество в качестве преступления имеет материальный состав, т.е. обязательным признаком этого состава является наступление конкретного общественно опасного последствия, нанесение вреда, который четко прослеживается в диспозиции ст. 159 Уголовного кодекса Российской Федерации (далее – УК РФ).

Таким образом, наступление преступного результата – обязательный признак объективной стороны мошенничества. Так как последствия преступления не конкретизируются, то можно считать, что преступным результатом мошенничества будет хищение чужого имущества, либо приобретения права на него и все это приводит к причинению материального ущерба потерпевшему. Преступный результат при мошенничестве наступает, когда потерпевший уже не обладает своим имуществом, а право распоряжаться этим имуществом переходит к мошеннику.

Для того, чтобы привлечь лицо к уголовной ответственности за мошеннические действия, необходимо установить причинную связь между

¹ Зарипова Е. А. Некоторые проблемы квалификации мошенничества // Меридиан. 2021. № 3. С. 81.

² Чечель Г. И., Третьяк М. И. Мошенничество: вопросы квалификации // Общество и право. 2015. № 3. С. 63.

действием (бездействием) и общественным ущербом. Можно сказать, что это является причиной обмана (злоупотреблением доверия) и приобретением имущества (хищение имущества). То есть заблуждение потерпевшего – причина передать имущество преступнику, а причина такого заблуждения – обман.

А. А. Денисов выделяет два вида мошенничества: 1) хищение чужой собственности; 2) приобретение права собственности на чужое имущество. При этом говорит о способах совершения деяния: 1) злоупотребление доверием; 2) обман¹.

Обман мошеннического посягательства бывает: активным (сознательное искажение истины) и пассивным (умолчание об истине). Обязательное условие мошенничества: в любом случае потерпевший самовольно передает преступнику имущество и право на собственность. Обман, как правило, сочетается с мошенничеством, однако более реже злоупотребления доверием выступают в роли самостоятельного метода мошенников.

К примеру, основные виды мошенничества в сфере кредитования с использованием доверия:

- заключение договора займа без намеренного желания отдавать долг;
- получение предоплаты по договору купли-продажи без намеренного желания выполнять условия договора;
- финансовая пирамида;
- получение кредитов в банках, не желая их вернуть².

И. М. Парунов отмечает, что в современном мире можно выделить самые характерные черты мошенничества:

- межрегиональный характер действий мошенников (завладевают имуществом одного региона, а сбыт осуществляют уже в другом);

¹ Денисов А. А. Криминалистическая характеристика мошенничества // Тенденции развития науки и образования. 2021. № 6. С. 31.

² Едиджи Ф. А. Головин М. В. Некоторые элементы криминалистической характеристики мошенничества // Эпомен. 2021. № 55. С. 180.

- в больших и особо крупных масштабах деяния совершаются в основном организованной группой;

- в большинстве случаев созданные фиктивные фирмы, а при мошенничестве используют фальшивые и подложные документы, штампы, печати и т.д.;

- хорошая адаптация, быстрое распространение новых типов мошенников¹.

С. А. Коробов отмечает, что субъективная часть рассматриваемого деяния характеризуется умыслом. Для этого преступления самым типичным является заранее обдуманый умысел, но и он может возникнуть внезапно, когда преступления совершаются сразу после того, как возникает преступное намерение. Так, например, если мошенники обнаруживают заблуждение пострадавшего, они используют его в корыстных целях. Условия, которые необходимы для того, чтобы привлечь виновного к уголовной ответственности за мошенничество, - заключаются в установлении прямого намерения и обоснованной цели².

Для основного состава мошенничества характерны общие субъекты, применяются общепринятые положения уголовного законодательства, то есть вменяемые физические лица, достигшие 16 лет.

В то же время, учитывая то, что мошенникам сложно осуществлять какие-либо действия при отсутствии развитого интеллекта, то в этом случае на практике часто ставится вопрос о вменяемости. Поэтому сложность в квалификации этих деяний порождает выявление субъектов, определение направленности умысла. Неправильно определить хотя бы один элемент в составе преступления влечет за собой ошибочную квалификацию содеянного.

Помимо этого, А. М. Филиппов считает, что следует помнить о том, что развитие рыночных отношений, модернизация банковской отрасли, развитие

¹ Парунов И. М. Мошенничества, совершаемые на современном этапе развития общества. Гатчина, 2021. 165 с.

² Коробов С. А. Специфика криминалистической характеристики мошенничества // Молодой ученый. 2021. № 6. С. 223.

страхового рынка, инвестиционная деятельность, информационные технологии и предоставление новых услуг развивает новые виды и формы мошенничества, появление которых требует от законодателя реформы уголовных норм, поскольку установленные составы этого преступления в Уголовном Кодексе Российской Федерации не учитывают все особенности экономических отношений, которые затрудняют обеспечение защиты имущества и других ценностей граждан от мошеннических посягательств¹.

К примеру, объективная сторона мошенничества, совершенного в сфере кредитования, достаточно полно характеризуется специальным способом осуществления – представление кредитору любых заведомо ложных и (или) каких-либо недостоверных сведений². Так, Красноперекоский районный суд г. Ярославля рассмотрел в открытом судебном заседании в г. Ярославле материалы уголовного дела в отношении подсудимых Гурова Г. Ю., Мачулиной Ю. Г. и Уткиной В. С., установил факт совершения мошенничества в сфере кредитования, т.е. хищения денежных средств заемщиком путем предоставления банку заведомо ложных сведений, группой лиц по предварительному сговору. Судом было установлено, что <...> около 16 часов Гуров, находясь в помещении <...> и имея при себе ранее найденный им на улице паспорт гражданки РФ на имя <ФИО2>, предложил своей знакомой Уткиной В.С. совершить с использованием этого паспорта мошенничество, в ходе которого Уткина должна была представиться <ФИО2>, оформить в кредитной организации <...> по чужому паспорту на имя <ФИО2> потребительский кредит на приобретение дорогостоящей электронной техники, после чего она должна была приобрести эту технику на предоставленные банком кредитные средства и не возвращать кредит банку. Таким образом, подсудимые путем обмана и предоставления банку заведомо ложных сведений совместно похитили принадлежавшие <...> денежные средства в сумме 34999

¹ Филиппов А. Р. Указ. соч. С. 135.

² Хутуев В. А., Машекуашева М. Х. Некоторые вопросы квалификации мошенничества // Проблемы экономики и юридической практики. 2019. № 4. С. 123.

рублей, на которые ими путем безналичной оплаты был приобретен коммуникатор стоимостью 34999 рублей¹.

Вот еще один пример, Дзержинский районный суд города Ярославля рассмотрев в открытом судебном заседании уголовное дело в отношении Шафиуллина установил, что Шафиуллин М. Х. совершил мошенничество в сфере кредитования, то есть хищение денежных средств заемщиком путем предоставления кредитору заведомо ложных и недостоверных сведений, при следующих обстоятельствах: Шафиуллин М. Х., имея умысел на мошенничество в сфере кредитования, то есть хищение денежных средств заемщиком путем предоставления кредитору заведомо ложных и недостоверных сведений, из корыстной заинтересованности, в период с января 2016 года по 24 февраля 2016 года передал неустановленному лицу паспорт гражданина РФ на свое имя, с целью подделки оттиска штампа ОУФМС России по Ярославской области в Дзержинском районе г. Ярославля. Шафиуллин М. Х., завершая реализацию своего преступного умысла 24 февраля 2016 года в период с 14 часов 00 минут до 17 часов 00 минут, на основании договора займа № от 24 февраля 2016 года, заведомо не намереваясь выполнять его условия и осуществлять выплату заемных денежных средств, получил в кассе ООО МФО <данные изъяты>, расположенном по адресу: г. Ярославль, <адрес> денежные средства в сумме 3 000 рублей, тем самым их похитил путем мошенничества².

Таким образом, мошенничество является одновременно и чрезвычайно распространенным, и высоко латентным уголовно наказуемым деянием. Криминальная «палитра» внешних проявлений мошенничества разнообразна: наряду с «традиционными», классическими формами обмана, все чаще применяются способы, не имеющие аналогов в следственной практике (в том числе в истории криминалистики). Таким образом, неуклонный рост

¹ Приговор № 1-10/2015 1-159/2014 от 14 января 2015 г. по делу № 1-10/2015. [Электронный ресурс]. Режим доступа: URL: //http://sudact.ru. (дата обращения: 10.01.2022).

² Приговор суда по ч. 1 ст. 159.1 УК РФ № 1-5/2017 (1-329/2016) [Электронный ресурс]. Режим доступа: URL: //http://sudact.ru. (дата обращения: 10.01.2022).

мошеннических посягательств сопровождается их качественными изменениями.

Действия мошеннического характера занимают особое место в системе преступлений против собственности, поскольку обладают повышенной общественной опасностью, носят организованный характер (в основной своей массе), причиняют значительный ущерб как юридическим, так и физическим лицам. В связи с тем, что противоправные действия, способы и алгоритмы злоумышленников постоянно видоизменяются, усложняются (преступники все чаще прибегают к наукоемким стратегиям как явного, так и скрытого психологического воздействия, манипулирования), актуализируется потребность в поиске более эффективных (условно говоря, универсальных) форм социально-правового и организационного контроля за криминальной активностью мошенников.

§ 2. Основные элементы криминалистической характеристики мошенничества

Криминалистическая характеристика преступления – это особая система определенных криминалистически значимой информации о наиболее типичных, обязательно связанных между собой определенных элементов конкретных категорий преступлений, а также условий их совершения преступником. Однако, говоря об элементах состава такой криминалистической характеристики, можно сослаться на авторские методики по расследованию преступлений в сфере экономики, в которых С.А. Коробов выделяет следующие ее элементы:

- 1) определенный способ совершения конкретного преступления;
- 2) способ сокрытия;
- 3) предмет преступного посягательства;
- 4) сведения о личности преступника;
- 5) обстановку совершения преступления;

б) обстоятельства, способствовавшие совершению преступления;

7) механизм слеодообразования¹.

А. А. Денисов отмечает, что «криминалистическая характеристика преступлений – это совокупность взаимосвязанных фактов и построенных на них научных предположений, и пожеланий об особенно рядовых криминалистически важных особенностях преступлений, наличие информации о которых требуется следователям и дознавателям для организации и исполнения их всеобщего, полного, объективного и быстрого раскрытия и расследования»².

Определение криминалистической характеристики основывается на криминалистическом рассмотрении путей преступной деятельности, ее следов, обстановки, предметов посягательства, мотивов, личности преступника и жертвы и их связей. Наиболее значимым обстоятельством служит то, что научная группа «криминалистическая характеристика» располагает таким признаком, как динамичность. Этот признак выражается основным образом в том, что содержание криминалистической характеристики применяется ко многим видам и группам преступлений и может изменяться, иногда кардинально.

Мошенничество, то есть присвоение посторонней собственности или приобретение права на чужую собственность с помощью обмана или злоупотребления доверием, числится к ряду преступлений посягающих на собственность.

Например, Н. П. Яблоков считает, что главные особенности криминалистической характеристики мошенничества «наиболее ярко проявляются в непосредственном предмете преступного посягательства, способе, механизме и обстановке их совершения, типологических чертах

¹ Коробов С. А. Указ. соч. С. 223.

² Денисов А. А. Указ. соч. С. 32.

личности похитителей и преступной группы, а иногда и в особенностях наступивших преступных последствий»¹.

Остальные авторы выражают свои мнения на строение и сущность криминалистической характеристики мошенничества, также на перечень ее частей по уровню важности. Например, С. М. Астапкина считает, что «более важными звеньями криминалистической характеристики хищений в кредитной сфере являются:

- а) обстановка совершения хищений;
- б) исходная информация о хищении;
- в) способы совершения и сокрытия хищения;
- г) типичные следы;
- д) особенности личности преступника»².

Особенностью криминалистической характеристики компьютерных преступлений (немалая доля которых квалифицировалась как мошенничество), как считает Б. Б. Батров, «является факт того, что должны создавать криминалистически важные данные о личности правонарушителя, цели его преступного поведения, рядовых способах, предметах и местах посягательств и о потерпевшей стороне»³.

Мы считаем, что определенные подходы к структуре криминалистической характеристики считаются лучшими именно для тех видов мошенничества, для которых они были созданы. «Широкий» подход, который предложил Яблоков Н. П., может быть использован для общей характеристики мошенничества, независимо от сферы его совершения.

Представляется, что именно обстановка преступления является системообразующим элементом криминалистической характеристики мошенничества, совершаемого в определенной сфере. Она определяет способы

¹ Яблоков Н. П. Криминалистика: учебник. М.: Юрайт, 2019. С. 277.

² Астапкина С. М. Методика расследования мошенничества: монография. Волгоград, 2004. С. 78.

³ Батров Б. Б. Криминалистическая профилактика интернет-мошенничеств: проблемы раскрытия и расследования // Вестник Бурятского государственного университета. Юриспруденция. 2021. № 1. С. 22.

подготовки, совершения и сокрытия данных преступлений, особенности механизма слеодообразования, тесно связана с такими элементами, как свойства личности преступника и потерпевшего.

Таким образом, наиболее значимыми структурными элементами криминалистической характеристики мошенничества являются:

1. Обстановка мошенничества (типичные время, место и иные обстоятельства);
2. Способы подготовки, совершения и сокрытия мошенничества, а также присущие этой криминальной деятельности следы;
3. Характеристика мошенника и его соучастников, особенности их мотивации;
4. Характеристика потерпевших лиц;
5. Обстоятельства, способствовавшие мошенничеству.

§ 3. Современные виды мошенничества

Проводимые в конце XX – начале XXI века экономико-правовые и социально-политические преобразования активизировали научный поиск модели достижения эффективного развития российской государственности, ее экономики. В этих условиях развитие общества невозможно без формирования правовой базы, которая эффективно обеспечила бы экономическую безопасность государства. Государство, выступая гарантом стабильности отношений собственности на основе Конституции Российской Федерации обеспечивает устойчивое их развитие. Конституция как основной закон декларирует равенство всех форм собственности, равную их защиту.

Особую опасность среди видов преступлений в сфере телекоммуникационных технологий представляют мошенничества, в том числе с использованием ставших традиционными услугами операторов сотовой связи как смс-сообщений. Этим видом деятельности, как правило, занимаются

организованные преступные группы, оснащенные техническими средствами, отвечающими последним достижениям научного прогресса. С давних времен в мире существует мошенничество и исчезнет только вместе с человеком. Для обмана мошенники используют современные технологии, которые в современном мире постоянно развиваются. Большинство людей в нашем обществе хоть раз слышали про мошенников, но все равно находятся граждане, которые ведутся на их уловки. В среднем выманивают у доверчивого гражданина более 10 тысяч рублей за один звонок¹.

О.В. Полстовалов отмечает, что в период пандемии Covid-19 телефонные мошенники стали наиболее активными. Сегодня каждое четвертое преступление совершается посредством сотовой связи или сети Интернет. Поэтому важно разобраться в схемах телефонным мошенников и способах не попасться на их уловки².

Наиболее распространёнными являются следующие схемы мошенничества:

1. Пропущенные незнакомые номера.

Является наиболее распространённой схемой обмана телефонных мошенников. В данном случае весь расчет на то, что владелец телефона увидит пропущенный незнакомый номер и перезвонит. Мошенники при этом оформляют на используемый номер такой тариф, который предполагает платные входящие звонки. Причем, оплата может быть весьма высокой – до нескольких тысяч за минуту.

Доказать, что произошел обман будет очень сложно, ведь жертва сама совершает звонок мошенникам. Если это что-то важное, вам сами перезвонят позднее, а за входящие вызовы с вас точно плату не возьмут.

2. «Ваш родственник устроил ДТП».

¹ Яковлева Л. В. Современные способы совершения дистанционного мошенничества // Вестник Краснодарского университета МВД России. 2021. № 4. С. 77.

² Полстовалов О. В. К исследованию способов совершения организованных форм мошенничества в новой экономической реальности // Вестник Института права Башкирского государственного университета. 2020. № 3. С. 47.

Этот тип мошенничества чаще всего «отрабатывают» на пожилых людях, играя на их любви к близким и эмоциональности.

Преступник совершает звонок и сообщает, что ваш родственник спровоцировал ДТП, ему грозит суд и заключение. Но «есть возможность решить вопрос до суда». Естественно, не бесплатно, а за определенное – часто немаленькое – вознаграждение.

К сожалению, в такой стрессовой ситуации люди склонны идти на все условия мошенников, не подвергая предлагаемую им информацию какой-либо критической оценке. Обманутые снимают со счетов последнее и передают похитителям. Те в свою очередь стараются действовать как можно быстрее, подгоняют и запугивают, не давая опомниться.

Чтобы не попасться на обман в такой ситуации достаточно позвонить кому-либо из родных и уточнить ситуацию. Первым делом стоит выяснить обстоятельства, а потом уже что-то делать¹.

3. Разнообразные «бесплатные услуги», которые предлагают по телефону. Юридические, медицинские, косметологические услуги, поверка счетчиков и проверка пластиковых окон – список можно было бы продолжать до бесконечности.

При звонке никто не будет пытаться выманить деньги у абонента, а вместо этого могут предложить, например, бесплатно осмотреть ваши пластиковые окна. Если человек даст свое согласие, то к нему действительно придет мастер и проведет бесплатный осмотр окон. А дальше начнется самое интересное: окажется, что в ваших окнах есть множество «скрытых» неисправностей, которые не сегодня-завтра проявятся. Даже если у вас совершенно исправные окна, мошенник будет навязывать вам свои услуги. За дополнительный ремонт, естественно, с вас уже возьмут деньги, и немалые. И все это по-прежнему под эгидой «бесплатного обслуживания». Как это назвать, если не мошенничество?

¹ Колесникова Н. А. Разнообразие способов совершения мошенничеств в современных условиях // Евразийский юридический журнал. 2019. № 1. С. 275.

В этом случае, чтобы не стать жертвой, необходимо не соглашаться на «бесплатные» услуги и сервис. Если перед вами стоит задача сэкономить, лучше дождитесь скидок в компании, заслуживающей доверия. А когда слышите очередное: «У нас для вас очень выгодное бесплатное предложение», лучше сразу вешайте трубку.

4. «Странная активность» на карте.

Это достаточно новый вид мошенничества. Мошенник представляется сотрудником банка и сообщает, что на вашей карте замечена странная активность. При этом не спрашиваются реквизиты карты, этим мошенники пытаются усыпить бдительность жертвы.

Чаще всего такие разговоры заканчиваются тем, что жертве сообщают, будто на их телефоне установлено вредоносное ПО, и предлагают удаленно «посмотреть», есть ли какие-то проблемы.

Подключившись к мобильному телефону жертвы, мошенник может делать все, что угодно, в том числе, выводить любые средства на собственные счета. Доказать потом, что все это совершалось не самим держателем карты, будет очень сложно.

Для того чтобы не стать жертвой такой схемы обмана необходимо помнить, что если у банка появились сомнения в том, что операции по карте совершает не владелец, то он сразу блокирует карту, после чего начинает разбираться в случившемся¹.

5. Спасем щенков, погибающих на улице.

К сожалению, благотворительность – это та сфера, в которой часто встречаются мошенники. Как правило, они действуют через интернет, но могут пользоваться и телефонной связью. Потенциальной жертве приходит смс с предложением помочь «несчастливым домашним животным», отправив сообщение с указанием суммы пожертвования на определенный номер. Обман здесь может быть нескольких видов: либо сообщение окажется «золотым»,

¹ Мелихова Л. И. Мошенничество с использованием средств сотовой связи: характеристика и виды. Ростов-на-Дону, 2021. 673 с.

либо пожертвованные деньги попадут в карман мошенников, а не будут направлены на благое дело¹.

б. Розыгрыш призов.

На телефон поступает смс-сообщение, и злоумышленники представляются ведущими популярными радиостанций и сообщают, что абонент выиграл ценный приз, но при этом «победителю» необходимо заплатить налог, внести определенную сумму денег с обещанием непрямого возврата. После совершения необходимых действий злоумышленники скрываются.

Чтобы не попасться на уловки мошенников нельзя переводить деньги после сомнительных звонков с неизвестных номеров на телефон потерпевшего².

Можно сделать вывод, что в большинстве случаев обмана можно избежать, если воспринимать информацию критически, не торопиться, и не следовать указаниям людей, которых вы не знаете, даже если они назвали сотрудниками банка или специалистами в какой-либо сфере.

Особенностью современного состояния развития информационного общества является достаточно широкое использование информационно-телекоммуникационную сеть Интернет (далее – Интернет) во многих сферах жизни, в том числе и криминальной. Его важность не вызывает сомнений, что обусловлено современным информационным состоянием общества, когда информация выступает главным его ресурсом, а информационные технологии – основным средством ее получения.

Многие пользователи для облегчения и ускорения получения услуг устанавливают различные приложения, в том числе через мобильные маркетплейсы, обеспечивая тем самым возможность оперативного доступа к интересующей информации. Однако, необходимо помнить, что вместе с удобством и быстротой получения нужных услуг, пользователи могут быть подвержены активным действиям мошенников.

¹ Колесникова Н. А. Указ. соч. С. 276.

² Яковлева Л. В. Указ. соч. С. 78.

И. М. Парунов отмечает, что «одним из факторов, неблагоприятно влияющих на состояние национальной экономики, является развитие преступности и мошеннической деятельности, которая в условиях глобального распространения сети «Интернет» видоизменяется и интегрируется в сферы Интернет-торговли, Интернет-маркетинга и прочих товарно-денежных отношений в глобальной сети, подрывая постулаты экономической безопасности государства»¹.

Пандемия коронавирусной инфекции во всем мире обозначила проблемы в дистанционного мошенничества, поскольку вынужденное нахождение дома заставила многих обращаться к услугам Интернет-торговли.

В научной литературе предлагается следующую классификация способов Интернет-мошенничества:

1. Фиктивные Интернет-магазины - довольно распространенный вид мошенничества, представленный сайтами-одностраничниками с уникальным ценовым предложением на какой-либо товар. Как правило, «фиктивные Интернет-магазины работают по частичной либо по стопроцентной предоплате. Соответственно, жертва, осуществив перевод денежных средств, не получает требуемого товара. Далее сайт блокируется, и со временем «переезжает» на другой хостинг либо меняет доменное имя и продолжает свою противоправную деятельность. Такой сайт может быть наполнен большим количеством фальшивых отзывов с целью создания образа добропорядочного Интернет-магазина и введения в заблуждение потенциальных жертв»². Такой вид мошенничества является одним из самых простых методов осуществления преступной деятельности в сети Интернет и наносит большой урон по финансовой состоятельности слабозащищённых и не осведомленных граждан с учетом низкого уровня их информационной грамотности.

2. Фишинг – является чуть более продвинутым видом Интернет-мошенничества. Целью мошенника в таком случае становится возможность

¹ Парунов И. М. Указ. соч. С. 163.

² Батров Б. Б. Указ. соч. С. 22.

завладеть банковскими реквизитами, данными электронных платежных карт либо данными от электронных Интернет-кошельков пользователей. Фишинговый сайт сложно распознать ввиду того, что он полностью копирует оригинальный сайт, например, может быть полностью скопирован интерфейс какого-либо клиент-банка (в основном, актуально для физических лиц, так как клиент-банки у юридических лиц защищены средствами крипто шифрования и усиленных цифровых подписей), отличие будет составлять лишь адрес доменного имени, не привлекающий внимание неподготовленного гражданина. В такой ситуации жертва добровольно вводит свои учетные данные от кошелька либо банковской карты и в скором времени теряет денежные средства с данного носителя.

3. Черный инфобизнес – популярный вид Интернет-мошенничества, начиная с конца 2017 года. Стоит отметить, что «сам по себе инфобизнес не является мошенничеством, поскольку представляет собой продажу информации в форме книг, аудио и видео файлов, презентаций и т.п. Однако со стремительным развитием инфобизнеса в последние годы появился и его мошеннический аналог. Под видом вебинаров, курсов повышения квалификации либо онлайн школ, пользователю предполагают купить информацию либо менторство и наставничество на определенный срок в какой-либо сфере бизнеса или науки. Однако после перечисления средств, пользователь, в лучшем случае, получает информацию, которую можно найти в сети Интернет в свободном доступе, либо не получив блага или услуги, теряет свои денежные средства»¹.

4. Мошенничество с распространением контента – представляет собой вид мошенничества, при котором мошенниками создается архив с требуемой пользователю информацией. Как правило, срабатывает несложный скрипт, подменяющий название архива на запрашиваемую пользователем информацию в поисковой системе. Но при попытке распаковки либо загрузки данного

¹ Арсамерзаев И. С. Современные способы мошенничества, проблемы их выявления // Конкурс молодых ученых. 2020. С. 165.

архива, пользователю предлагается отправить сообщение для верификации его аккаунта, вследствие чего с его счета списывается крупная сумма денежных средств, а искомую информацию он так и не получает.

5. Финансовые пирамиды, которые законодательно запрещены на территории Российской Федерации, независимо от того, является ли она традиционной финансовой пирамидой либо Интернет-проектом. Как отмечает Н. А Колесников, «несмотря на то, что за организацию финансовых пирамид установлена уголовная ответственность, финансовые пирамиды являются весьма распространенным видом мошенничества в сети Интернет, а реклама подобных проектов широко распространена в социальных сетях. Стоит учесть, что помимо традиционных Интернет-пирамид вида МММ, довольно распространены компании, - это многоуровневый сетевой маркетинг. Концепцией является реализация товаров и услуг, которая основана на создании сети независимых дистрибьюторов (сбытовых агентов), каждый из которых, помимо сбыта продукции, также обладает правом на привлечение партнёров, имеющих аналогичные права. При этом доход каждого участника сети состоит из комиссионных за реализацию продукции и дополнительных вознаграждений (бонусов), зависящих от объёма продаж, совершённых привлечёнными ими сбытовыми агентами. Сама по себе концепция сетевого маркетинга не является мошенничеством, однако в сети Интернет работают компании, которые продают товар крайне сомнительного качества, который впоследствии дистрибьютор просто не может реализовать и оказывают фиктивные финансовые услуги»¹.

6. Интернет казино и нелегальные букмекеры – это противоправный вид Интернет-мошенничества, представляющий, на наш взгляд, наибольшую угрозу экономической безопасности государства. Законодательно онлайн-казино запрещены, что регулируется пунктом 3 Федерального закона от 29.12.2006 № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые

¹ Колесникова Н. А. Указ.соч. С. 276.

законодательные акты Российской Федерации», согласно которому деятельность по организации и проведению азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также средств связи, в том числе подвижной связи, запрещена.

Таким образом, можно сказать о том, что как правовое, так и техническое регулирование противоправных действий в телекоммуникационных сетях попадает в безвыходную ситуацию. Выходом из сложившейся ситуации может стать совершенствование законодательной базы, регулирующей подобные ресурсы и организация открытой дискуссии юристов, экономистов, технических специалистов и органов управления с целью нахождения вариантов решения данной проблемы.

ГЛАВА 2. РАСКРЫТИЕ И РАССЛЕДОВАНИЕ ОТДЕЛЬНЫХ ВИДОВ МОШЕННИЧЕСТВА

§ 1. Особенности раскрытия и расследования мошенничества в сфере кредитования

Активный переход граждан на удаленный режим деятельности привёл к повышению их активности в сети интернет. Организациями были динамично задействованы электронные платформы для оказания услуг. Данные факторы благотворно повлияли на последующий рост преступлений, совершаемых с использованием информационных систем.

Криминалистическое обеспечение – это деятельность ОВД в целом и система криминалистических знаний и основанных на них навыков и умений сотрудников использовать научные криминалистические рекомендации, применять криминалистические средства, методы и технологии в целях предотвращения, выявления, раскрытия и расследования преступлений в частности. Особое место в этой деятельности занимает точное установление механизма совершения дистанционного мошенничества¹.

Механизм отслеживания дистанционного мошенничества специфичен прежде всего из-за особенностей метода, который предполагает замену адреса пользователя в Интернете, использование подмены номера в IP-телефонии и т. д. При совершении киберпреступлений обнаруживаются цифровые следы, которые представляют собой незаконную деятельность по использованию компьютера, компьютерной сети или сетевого устройства. Данные преступления могут быть спланированы как организованными группами, так и отдельными лицами.

Одним из самых распространенных способов онлайн-мошенничества является фишинг. Мошенники предпринимают определенные действия, чтобы

¹ Потемкина М. О. Особенности раскрытия и расследования современных способов мошенничества в условиях крупного города. М., 2020. 222 с.

получить доступ к банковской карте потенциальной жертвы: используют списки рассылки от имени банка, содержащие веб-адреса нужных страниц, копии официальных сайтов, предлагающих ввести реквизиты банковской карты для дальнейшего ее использования. Довольно часто встречаются ситуации, когда жертве звонит мошенник, представляющийся сотрудником банка, и просит сообщить конфиденциальные сведения о карте или данные для входа в онлайн-банк, для того чтобы пресечь подозрительную транзакцию, совершаемую с использованием банковской карты или счета абонента. В таких случаях потерпевший, находясь в состоянии испуга, предоставляет необходимую злоумышленнику информацию¹.

Анализ совершенных дистанционным способом мошенничеств показывает, что одним из признаков запланированного или осуществляемого преступления с использованием сотового телефона является представление преступников сотрудниками службы безопасности банка и получение информации о банковской карте во время телефонного разговора.

Еще одним важным тактическим приемом, позволяющим мошенникам дистанционным способом добраться до денежных средств потерпевших, является получение одноразового пароля (в виде SMS-сообщения), который отправляется на номер абонента, привязанный к банковской карте. Владелец банковской карты предоставляет мошенникам одноразовый пароль, тем самым обеспечивая доступ к средствам, на ней хранящимся².

Следует отметить, что с 2020 г. в связи с массовым переходом на удаленную работу участились случаи рассылки писем якобы от служб техподдержки различных компаний, банков, государственных органов, содержащих уведомление о смене режима и предложение воспользоваться ссылками для дистанционного подключения к служебным ресурсам. Таким

¹ Струков А. Е. Понятие и способы мошенничества // Вестник магистратуры. 2022. № 1-2. С. 10.

² Явинский А. В., Соловьев А. А. Способы противодействия телефонному мошенничеству. Омск, 2021. 373 с.

способом мошенники воруют личные данные, а в дальнейшем могут атаковать информационные системы организаций.

Появились также новые способы мошенничества в связи с распространением коронавирусной инфекции. В частности, стали формироваться известные торговые площадки-клоны для продажи дорогого компьютерного оборудования. Неопределенность платежей, требования самоизоляции с информацией, которая не всегда является полной и доступной, позволили мошенникам по различным обманным причинам связываться с пенсионерами и получать доступ к их банковским реквизитам, а иногда и незаконно проникать в их дома.

Популярные сайты бесплатных объявлений способствовали появлению следующей схемы мошенничества: киберпреступники размещали лоты с заведомо заниженными ценами, и когда потенциальный покупатель проявлял интерес, они отправляли ему ссылку на фишинговую страницу предполагаемой курьерской службы с просьбой перевести деньги за товар и доставку.

Наблюдается заметное увеличение количества хищений с карт клиентов, осуществляемых с использованием методов психологического воздействия на потерпевшего, чаще всего отдаленно представляющего себе механизм защиты его денежных средств, которыми можно распоряжаться при помощи банковской карты. Используя формы общения банковских служащих с клиентами, злоумышленники окончательно вводят человека в заблуждение и принуждают сообщать коды и пароли от карты¹.

Следует отметить, что чаще всего признаки мошенничества с использованием средств связи выявляются по заявлению жертвы о совершении в отношении ее незаконных действий (около 87% случаев). Для определения персональных данных владельца абонентского номера, использованного при совершении такого способа дистанционного мошенничества, следователь (дознатель) может до возбуждения уголовного дела направить запрос

¹ Сорокун Н. С., Замалева С. В. Особенности современного мошенничества // Вестник Дальневосточного юридического института МВД России. 2021. № 2. С. 72.

оператору связи, обслуживающему регион, в котором зарегистрирована SIM-карта с номером абонента, имеющего отношение к расследованию, с целью предоставления необходимой информации. Преступники анонимно регистрируют телефонный номер и делают с него звонки. Такая же ситуация с сетью Интернет: преступники используют современные технические средства, чтобы скрыть свой IP и уйти от наказания.

Что касается механизма следообразования дистанционного мошенничества, то решающим в данном случае из-за своеобразности способа преступления, является наличие информационных или цифровых следов. Между тем, наблюдается очевидная сложность работы с такими следами и специальной подготовкой субъектов. Во-первых, временной промежуток получения нужной информации из компаний сотовой связи очень велик, во-вторых, мошенники все больше используют подставных лиц, на которых оформляют банковские карты, в третьих, мошенники часто меняют номера телефонов, с которых поступают звонки противоправного характера, в-четвертых, профессиональные возможности Интернет-мошенников находятся на достаточно высоком уровне и позволяют им использовать IP-адреса, сервера и ресурсы, находящиеся за пределами России.

Именно поэтому, как указывают А. В. Явинский и А. А. Соловьев, появилась «необходимость решения названных проблем требует выработку новых подходов в борьбе с преступностью, которая всё чаще взаимодействует с цифровой средой, а также активного формирования и совершенствования методических основ профилактики, расследования и выявления преступных деяний»¹. Именно из-за обозначенные выше проблем раскрываемость дистанционных мошенничеств остается на низком уровне.

В. Н. Фурман отмечает, что «положительная динамика расследования в этой сфере будет возможна, в случае разработки, внедрения и освоения

¹ Явинский А. В., Соловьев А. А. Указ. соч. С. 373.

методов, средств и рекомендаций профессиональными субъектами раскрытия и расследования преступлений в данной области»¹.

Достаточно актуальным остаётся вопрос уровня информационного и информационно-технического обеспечения раскрытия и расследования мошенничеств, совершаемых с использованием информационных средств. Видится неэффективность использования современных баз данных ввиду отсутствия достаточной вычислительной мощности, а также многочисленной штата профессиональных сотрудников.

В этих условиях речь можно вести о появлении информационных следов в виртуальном пространстве и о необходимости обнаружения, фиксации, изъятия и исследования информации, содержащейся на электронных носителях. Осуществить эту задачу самим следователем не всегда представляется возможным, так как требуется наличие специальных знаний в области информационных технологий, которыми следователи не обладают, требуется либо привлечение специалистов к участию в производстве следственных действий, либо назначение компьютерно-технических экспертиз.

В настоящее время по-прежнему является актуальным внедрение в следственную практику современной компьютерной техники, разработка, внедрение и использование следователями компьютерных программ, позволяющих анализировать исходные данные по уголовным делам об умышленных убийствах и предлагать следователям на основании этого рекомендации по определению наиболее оптимального пути расследования, алгоритмы разрешения складывающихся следственных ситуаций. По-прежнему также актуальным является создание автоматизированных рабочих мест для следователей, имеющих доступ к современным автоматизированным базам данных по уголовным делам и автоматизированным поисковым системам, а также базам данных не только правоохранительных органов, но и других организаций (например, многофункциональных центров). Это позволило бы

¹ Фурман В. Н. Современные виды мошенничества, способы совершения и их предупреждение. Великий Новгород, 2021. 311 с.

следователям оперативно получать необходимую поисковую, справочную информацию по делу, информацию о возможном местонахождении лиц и т. д. Актуальным является внедрение в следственную практику современной цифровой техники. Следователи фактически активно используют цифровую технику, в частности средства сотовой связи, которые следователи используют для фиксации хода и результатов следственных действий (чаще всего проверки показаний на месте).

В настоящее время в научной литературе много говорится о необходимости активного внедрения в практику борьбы с преступностью современных достижений науки и техники, достижений как естественных (математика, физика, химия, биология и др.), технических наук (например, материаловедение, нанотехнология, информатика и др.), так и гуманитарных (психология, социология, логика, этика, философия, история науки и др.)¹. Мы полагаем, что использование в практике всех средств, помогающих изучить причины совершенных преступлений включает в себя, во-первых, научный уровень, связанный с разработкой необходимых технических средств, во-вторых, практический уровень, связанный с внедрением в практическую деятельность разработанных технических средств. Также в структуру организационно-управленческого элемента входит решение вопросов об организации взаимодействия экспертных учреждений органами предварительного следствия, органами дознания и судами.

Вопросы противодействия преступлениям против дистанционного мошенничества являются достаточно актуальными, а задачи их предупреждения – основными и первоочередными в деятельности всех подразделений МВД России. Защита личности, общества и государства от противоправных посягательств основывается на положениях Конституции Российской Федерации и возлагается на систему субъектов профилактики правонарушений, главным образом на органы внутренних дел. Общая социальная профилактика правонарушений направлена на прогрессивное

¹ Парунов И. М. Указ. соч. С. 164.

развитие общества, улучшение жизнедеятельности населения во всех сферах. Ее объектом выступает все население страны. На недопущение правонарушений общая социальная профилактика влияет лишь косвенно. Специальное же предупреждение правонарушений заключается в непосредственном воздействии на причины и условия правонарушении, самих правонарушителей, на недопущение преступлений, административных правонарушений, антиобщественного поведения и негативных социальных явлений.

§ 2. Особенности раскрытия и расследования дистанционного мошенничества

Технологический прогресс, происходящий в обществе, влечет за собой возникновение новых форм мошенничества и способов его совершения. С сожалением приходится констатировать, что сегодня уже привычным явлением стало мошенничество с использованием электронных систем расчетов, под которыми понимается сложный механизм, включающий в себя и электронные средства платежа – банковские карты и электронные кошельки¹.

Раскрытие и расследование рассматриваемых преступлений сопряжено с рядом проблем. Безналичные деньги персонифицированы, т. е. их движение довольно легко отследить, поскольку каждое перемещение со счета на счет находит отражение в банковских документах. Такая «прозрачность» мешает преступникам, поэтому для вывода похищенных средств они используют различные схемы:

1. Перевод денег с карты на карту, а затем их снятие в банкоматах различных банков. Преимущественно карты регистрируются на подставных лиц (без определенного места жительства, страдающих какой-либо зависимостью и т. д.), приобретаются через посредников или в сети Интернет.

¹ Фурман В. Н. Указ. соч. С. 309.

В банкоматах деньги снимают специально нанятые люди. Кроме того, не все банкоматы оборудованы камерами видеонаблюдения, соответственно, идентифицировать граждан, снявших деньги, удастся далеко не всегда.

2. Переводы на QIWI-кошелек, в цифровую валюту, вывод денежных средств через букмекерские конторы и биржевые фонды, где при оформлении счетов не требуется подтверждения личности либо существует дистанционная регистрация (направляется копия паспорта гражданина).

3. Приобретение в интернет-магазинах различных товаров, которые затем забирают специально нанятые люди.

4. Мошеннические действия сотрудников банков с использованием системы электронных платежей путем внедрения в компьютерные программы.

5. Действия мошенников по хищению денежных средств с помощью создания разницы в процентной ставке при выделении краткосрочных кредитов.

Сегодня мошенничества, совершенные посредством информационно-телекоммуникационных технологий, получили широкое распространение по причине использования системы бесконтактных платежей – расчетов в специально оборудованных терминалах без введения подтверждающего транзакцию пин-кода. Средством таких платежей являются банковские карты, электронные кошельки, приложения для мобильных телефонов и т. д. Если они были утеряны, злоумышленники могут воспользоваться ими в своих целях. Отметим, что в случае отсутствия защиты в виде пароля или пин-кода реализации преступления, как правило, не предшествует подготовительный этап (если же средство оплаты защищено, то, прежде чем воспользоваться им, преступники устанавливают пин-код или подбирают пароль).

Обстановку совершения мошенничества образуют такие факторы, как:

1) пространственно-временной (место, время совершения мошенничества);

2) социально-экономический (состояние правового регулирования экономических отношений, эффективность деятельности государственных институтов и т. д.);

3) организационно-правовой (форма собственности предприятия, организации, учреждения, где совершено мошенничество, нормативные правовые акты, регулирующие порядок их деятельности, должностные инструкции сотрудников и пр.);

4) административно-управленческий (кадровая политика, система учета и отчетности, состояние дисциплины, наличие и состояние технических средств охраны и т. д.);

5) социально-психологический (взаимоотношения между сотрудниками, сотрудниками и руководством, уровень правового воспитания и т. д.)¹.

Мошенничества, совершенные посредством информационно-телекоммуникационных технологий наносят банкам огромный урон, однако не меньшие убытки они терпят и из-за недобросовестных заемщиков, взявших денежные средства с заранее имевшимся умыслом на невозврат и сознательно уклоняющихся от погашения кредиторской задолженности. Вина в сложившейся ситуации отчасти лежит и на самих банках, которые сделали процедуру получения кредита простой и доступной. Это привело к росту числа потребительских кредитов и спровоцировало активизацию действий злоумышленников.

При сборе материала проверки факта мошенничества в сфере кредитования нужно провести такие процессуальные и следственные действия, как:

- опросить заявителя о совершенных в отношении него действиях;
- направить запрос в банк для получения сведений о наличии банковской карты у пострадавшего, ее номере, дате открытия, наличии и сумме списанных денежных средств;

¹ Струков А. Е. Указ. соч. С. 11.

- установить возможность видеофиксации факта совершения действия с электронными средствами платежа и изъять соответствующие видеозаписи;

- опросить сотрудников банка;

- установить и приобщить к материалам проверки: документы, регулирующие отношения между держателем карты и банком; выписки по банковским (лицевым) счетам заявителя и подозреваемых лиц; сведения о владельце электронного кошелька; регистрационные данные доменных имен; IP-адрес владельца сайта; документы, отражающие факт получения кредита, и др.¹

Большое значение при расследовании мошенничеств, совершенных с использованием информационно-телекоммуникационных технологий, имеет оперативно-розыскная деятельность. Только ее средствами можно установить время, место совершения оплаты и т. д., что необходимо для выявления лиц, причастных к совершению преступления. Здесь следует сказать несколько слов об изъятии записей с камер видеонаблюдения, которое во многих случаях требует участия специалиста. В этой роли могут выступать представители службы технической поддержки торговых центров, павильонов, магазинов и иных объектов, где установлены средства видеофиксации; сотрудники центров автоматической фиксации административных правонарушений; операторы и специалисты, обеспечивающие работу системы «Безопасный город», и др.

Отметим, что мошенничества с использованием электронных средств платежа отличаются высокой латентностью. Потерпевшие часто не обращаются в правоохранительные органы, особенно если сумма причиненного ущерба незначительна.

Что касается личности преступника, совершающего «дистанционные» хищения, то нередко им является мужчина 18-35 лет, имеющий среднее или среднее специальное образование, трудоспособный, но без постоянного места работы или учебы, дееспособный, действующий в одиночку, не обладающий

¹ Филиппов А. Р. Указ. соч. С. 143.

специальными знаниями в области информационных технологий и навыками работы с электронно-вычислительными машинами¹.

Стоит сделать акцент и на механизме слеодообразования. Следы хищения можно обнаружить в фиктивных документах (банковских, регистрационных, бухгалтерских и т.д.): договорах о приеме на работу, аренду помещения, соглашениях о рекламе в средствах массовой информации, характеристиках и отзывах, – в компьютерной технике, счетных машинах, средствах печатного воспроизведения текста документов, которые могут использоваться для изготовления поддельных документов. Важную роль будут играть и идеальные следы, сохраняющиеся в памяти потерпевших, свидетелей и подозреваемых. Это могут быть показания об особенностях личности преступника, его поведении, семейном положении, месте проживания и т. д., поскольку встречаются случаи, когда злоумышленники используют реальные данные о своей личности.

Для эффективного расследования преступлений, в том числе мошенничеств, необходимы не отдельные, разрозненные данные, а совокупность сведений об основных элементах их криминалистической характеристики, что повышает информативность теоретической базы версии и результативность версионного процесса¹.

В области сохранности собственности принцип комплексного подхода к обеспечению защиты имущества физических и юридических лиц заключается в обеспечении ряда согласованных действий и действий различных подразделений полиции, занимающихся вопросами охраны общественного порядка, и направленных на по предупреждению и пресечению имущественных преступлений, а также по выявлению административных правонарушений в этой области, а также по выявлению причин и условий их совершения. Необходимость в этом принципе обусловлена, прежде всего, состоянием оперативной обстановки, которая влияет на безопасность владельцев

¹ Денисов А. А. Указ. соч. С. 32.

имущества и объектов, что влечет за собой обязанность координировать деятельность различных подразделений органа внутренних дел, работающих в одном месте.

Территориальный принцип означает соответствующее объединение территориального органа внутренних дел для определенной территории, как правило, совпадающей с территорией соответствующей административно-территориальной муниципальной единицы. Этот принцип позволяет обеспечить защиту имущества собственников с учетом местных социально-экономических условий, дает возможность повысить эффективность комплексного использования сил и средств.

Отраслевым принципом построения аппарата управления подразделениями является специализация структурных подразделений на определенных направлениях деятельности. Отраслевое построение позволяет сосредоточить силы и средства на управлении однородными подразделениями. Специализация позволяет сотрудникам в полной мере понять содержание поставленных задач, изучить и применить на практике формы и методы работы, разработать меры по повышению эффективности, что, в свою очередь, способствует принятию правильных управленческих решений и их реализации.

Одновременно с отраслевым принципом функционирования является основой для построения всех звеньев полицейских подразделений, что позволяет системе функционировать в целом. Таким образом, в состав территориального органа внутренних дел входят наряду с подразделениями, занимающимися вопросами охраны общественного порядка и обеспечения, такие подразделения, как кадровые, материально-технические, финансово-экономические, информационно-аналитические, юридические единицы. Эти подразделения проводят анализ эксплуатационной ситуации, занимаются подбором и расстановкой кадров, а также материально-техническим обеспечением подразделений, которые выявляют и пресекают правонарушения в сфере сохранности имущества.

¹ Коробов С. А. Указ. соч. С. 225.

Линейно-зональный принцип заключается в том, что отдельное подразделение или отдельный сотрудник руководит одним направлением работы, то есть специализируется на определенной деятельности. Например, участковый уполномоченный полиции может выявлять и расследовать административные правонарушения в области охраны собственности.

Принцип единоначалия и личной ответственности является обязательным условием деятельности подразделений полиции. Являясь продолжением отраслевого принципа, он обеспечивает единое централизованное руководство, единство технической и кадровой политики в системе МВД России. Этот принцип не исключает коллегиальность при принятии управленческого решения; однако руководитель принимает окончательное решение самостоятельно и несет личную ответственность за деятельность доверенного отдела.

За 12 месяцев 2021 года в Оренбургской области зарегистрировано 24989 преступлений (-9,1%). При этом можно отметить небольшое снижение числа зарегистрированных грабежей, краж, фактов мошенничества. Однако количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий, увеличилось на 73,4% (с использованием сети Интернет – на 91,3%, с использованием средств сотовой связи – на 88,3%). Данные статистики свидетельствуют о том, что раскрытие и расследование таких преступлений в МО МВД России «Ясненский» остается на низком уровне. Это обусловлено сложностью сбора доказательств причастности конкретных лиц к совершению преступлений, которая, в свою очередь, детерминирована:

- длительностью получения (от одного до трех месяцев) информации о соединениях между абонентами и (или) абонентскими устройствами, об их владельцах, о движении денежных средств по лицевым счетам абонентских номеров и др., имеющей доказательственное значение по уголовным делам, от операторов сотовой связи, банков;

- необходимостью командировочных выездов сотрудников следственных и оперативных подразделений в другие регионы России, что влечет за собой значительные затраты сил и средств;

- невозможностью во многих случаях использовать весь перечень оперативно-розыскных мероприятий, в том числе ограничивающих конституционные права и свободы граждан (снятие информации с технических каналов связи, прослушивание телефонных переговоров и т. д.);

- непродолжительным сроком хранения видеоматериалов с изображением лиц, осуществлявших обналичивание денежных средств в банкоматах;

- отсутствием систем электронного документооборота с кредитно-финансовыми организациями;

- невозможностью использовать в оперативно-служебной деятельности автоматизированные банковские системы обработки инцидентов «;

- проблемой получения информации о банковских реквизитах, используемых при перечислении денежных средств со счетов абонентских номеров (например, АО «НСК» предоставляет неполную информацию о номере карты (отсутствует полный номер: 4276*****5230), ссылаясь на защиту систем VISA и MasterCard);

- отсутствием эффективных механизмов блокировки банковских счетов и телефонных номеров, используемых при совершении преступлений указанной категории;

- недостаточным количеством сотрудников следственных подразделений, специализирующихся на расследовании киберпреступлений;

- стремлением кредитно-финансовых организаций быстро проводить денежные средства с одного банковского счета на другой.

Еще одной проблемой, с которой сталкиваются сотрудники МО МВД России «Ясненский», является длительность получения ответов из банковских организаций на поступившие им запросы. Часто сроки таковы, что когда удается установить счет, на который были переведены денежные средства, его владелец уже находится в другом городе или стране. Тогда

сотрудники МО МВД России «Ясненский» вынуждены отправлять запросы уже своим коллегам в другие субъекты Федерации или государства, что затягивает сроки проведения расследования.

Важно также отметить, что мошенничества, совершаемые с использованием информационно-телекоммуникационных технологий, имеют некоторые особенности, обуславливающие трудности их раскрытия и расследования:

- использование современных технологий изготовления и подделки платежных карт;
- высокий профессионализм преступников;
- обширная география;
- непрерывный процесс создания новых способов совершения преступлений и их сокрытия;
- высокая степень организованности участников преступной деятельности¹.

Комплекс различных оперативно-розыскных мероприятиям должны включать:

- направление в службу собственной безопасности банков, занимающихся всеми видами кредитования, соответствующих запросов, к которым должны быть приложены фотографии клиента, например, с копии паспорта или с записей веб-камеры, и список номеров мобильных телефонов «проблемных» заемщиков для организации анализа по имеющимся у этих банков базам данных, фиксирующих лица с отрицательной кредитной историей;
- истребование возможных сведений об утраченных паспортах и иных документах, которые были представлены заемщиками;
- получение информации по соответствующим номерам мобильных телефонов, которые были указаны заемщиком, обо всех осуществленных им соединениях с любыми абонентами или какими-либо абонентскими устройствами, зафиксированной за максимально возможный временной период,

¹ Едиджи Ф. А. Головин М. В. Указ. соч. С. 183.

с указанием конкретных адресов базовых станций либо используемых аппаратов, телефонных номеров этих абонентов и сведения об их анкетных данных;

- контроль и запись происходящих телефонных переговоров, ведущихся по интересующему телефонному аппарату, с дальнейшим определением и установлением номеров телефонов используемых сим-карт¹.

Кроме того, сложности раскрытия и расследования мошенничеств, совершенных посредством информационно-телекоммуникационных технологий в банковской сфере связаны с отсутствием методических рекомендаций по организации расследования и тактике производства следственных действий; недостаточной квалификацией следователей, работающих со специфическими источниками доказательственной информации; низкой мобильностью правоохранительных органов, что накладывает отпечаток на процесс доказывания, поскольку преступления совершаются в режиме реального времени с использованием технических средств и преступник сразу имеет возможность распорядиться похищенными деньгами.

Приведенный перечень проблем, с которыми сталкиваются сотрудники оперативных и следственных подразделений в ходе раскрытия и расследования мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий в банковско-кредитной сфере, не является исчерпывающим. Чтобы сократить их число, мы предлагаем реализовать некоторые организационно-управленческие меры:

1) закрепить в рамках уголовно-процессуального закона обязанность кредитных организаций и операторов сотовой связи предоставлять запрашиваемую органами предварительного следствия или дознания

¹ Мартынов А. Н. Особенности использования правовых категорий при разработке методики расследования мошенничества в сфере кредитования // Социум и власть. 2014. № 2. С. 83.

информацию, в том числе охраняемую законом, в течение трех суток с момента получения соответствующего запроса;

2) на законодательном уровне запретить использование незарегистрированных номеров сотовой связи, установить административную ответственность операторов сотовой связи за невыполнение указанного запрета;

3) создать базу данных номеров сотовой связи, использовавшихся для совершения мошеннических действий, обязать операторов сотовой связи уведомлять своих абонентов о том, что звонящий номер входит в эту базу.

Безусловно, перечень мер противодействия «дистанционным» мошенничествам можно расширить. Так, «при процедуре возбуждения дознавателем уголовного дела по выявленному факту мошенничества в сфере кредитования обязательно необходимо проводить тщательную предварительную проверку любого поступившего сообщения о событии преступления.

Дознаватель проводит следующие проверочные мероприятия.

Во-первых, необходимо получить все документы, либо копии этих документов, которые послужили выдачи кредита»¹. Такими документами, например, будут заявление о факте получения кредита; обязательная анкета заемщика; сам подписанный сторонами кредитный договор; расписаны график всех платежей по кредиту; необходимые ксерокопии определенного документа, удостоверяющего личность этого заемщика, предоставленные заемщиком справки с места его работы. Такое истребование дознавателем документов, как правило, осуществляется с помощью подачи запроса в соответствующее кредитное учреждение (ст. 21 и 144 УПК РФ).

Во-вторых, необходимо получить соответствующие объяснения у тех представителей кредитной организации, которые пострадали в результате мошеннических действий; также необходимо получить объяснения у всех лиц,

¹ Синенко Н. А. К вопросу о криминалистической характеристике мошенничества в сфере кредитования // Аллея науки. 2018. № 1. С. 697.

которые участвовали в процедуре оформлении этого кредита, и др. Дознавателем при процедуре опроса заявителя обязательно выясняются такие вопросы, как наличие особых должностных обязанностей того лица, кто выдал интересующий расследование кредит; следует выяснить также порядок, принятый при оформлении и выдачи соответствующего кредита в данной организации; выявить, какие документы обычно необходимо представить заемщику для получения в этой организации кредита; когда и при каких условиях был выдан кредит конкретному гражданину; какие именно документы были представлены заемщиком в данном случае; выяснить, какие цели были у заемщика при заявке на кредит; обязательно конкретная сумма, которую получил заемщик в результате выдачи ему кредита¹. Конечно же, данный перечень вопросов является примерным.

В-третьих, необходимо неведение необходимых справок. Также дознавателю следует получить консультацию у специалиста либо в устной, либо в письменной форме. Как правило, такие консультации обычно касаются особой кредитной политики банка, получению информации о тех документах, которые необходимы для получения у данного банка кредита. Обычно, в качестве таких консультантов выступают конкретные представители этой кредитной организации. Важным мероприятием будет исследование у эксперта всех документов с целью обнаружения на них следов интеллектуального или материального подлогов².

В завершение скажем несколько слов и о профилактике мошенничеств, совершаемых с использованием информационно-телекоммуникационных технологий. Всем известно, что хорошие результаты борьбы с противоправными деяниями достигаются непосредственно и проведением профилактических мероприятий, направленных на прекращение или

¹ Беняминов Ю. Д. Обстоятельства, подлежащие доказыванию при расследовании мошенничества в сфере кредитования // Образование. Наука. Научные кадры. 2016. № 5. С. 38.

² Кузьменко Е. С. Расследование мошенничества в сфере кредитования – нюансы доказывания и некоторые следственные ситуации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 2. С. 428.

частичного уменьшения отрицательного влияния причин, которые приводят к совершению преступных посягательств или совершения правонарушений. Но необходимо отметить что профилактика противоправных деяний в наше время не стоит на первом плане. Отсутствуют также методологические рекомендации по организационному обеспечению профилактической деятельности участкового уполномоченного, в частности по прогнозированию и предупреждению преступлений против собственности.

Взаимодействие является неотъемлемой частью деятельности полиции МО МВД России «Ясненский» по прогнозированию и предупреждению преступлений против собственности по выполнению возложенных на нее законодательством Российской Федерации, так как помогает обеспечить наиболее эффективную работу по направлению деятельности связанной с обеспечением общественной безопасности на территории Российской Федерации. Одним из направлений такого влияния является профилактика, целью которой является разработка теоретических указаний и методических рекомендаций по выявлению тех факторов, которые способствовали совершению определенного вида или группы преступлений.

Так, необходимо оповещать граждан о возможных способах совершения данных преступлений, об алгоритме действий, которые нужно предпринять, если преступление все-таки было совершено; организовать подготовку сотрудников органов внутренних дел, специализирующихся на расследовании рассматриваемых преступлений; разработать алгоритм действий для правоохранительных органов при поступлении сообщений, заявлений о «дистанционных» мошенничествах, методические рекомендации по их раскрытию и расследованию; заключить с банковскими организациями соглашения об обмене соответствующей информацией; создать базу данных «дистанционных» хищений, куда внести всю информацию, связанную с раскрытием и расследованием данных преступлений.

Безусловно, важное значение в процессе прогнозирования и

предупреждения преступлений против мошеннических действий будет иметь выработанная генеральная цель и миссия взаимодействия полиции и общества. Представляется наиболее понятной и доступной для большинства населения дифференциация стратегий (стратегических целей) по следующим направлениям взаимодействия: профилактика правонарушений; обеспечение охраны общественного порядка; борьба с преступностью¹.

Технологический фактор связан с внедрением новых форм взаимодействия полиции и населения на основе информационных технологий, развитием человеческих ресурсов и кадрового потенциала полиции, формированием морально-нравственного облика полицейского. «Нравственность», «духовность», «нравственное воспитание» целиком и полностью взаимосвязаны, имеют друг на друга свое влияние и дополняют друг друга. Несмотря на выделенную нами дискуссионность определения этих терминов в научной литературе, большинство ученых сходятся во мнении, что основным показателем эффективности нравственного воспитания молодого поколения будут внутренний самоконтроль, стремление к саморазвитию и самовоспитанию, формированию у себя таких важных в профессиональной деятельности личностных качеств, как дисциплинированность, чувство долга, преданность гуманистическим идеалам, умение сдерживать свои эмоции, неукоснительное соблюдение законов, чувство собственного достоинства, уважительное отношение к правам и свободам личности, толерантность, совесть, трудолюбие. Это далеко не все личностные и профессиональные качества, которые являются носителями нравственности и которыми должен обладать каждый гражданин, чтобы эффективно исполнять свою профессиональную деятельность в сложной атмосфере ежедневного столкновения с особой преступной средой, ее субкультурой, которая может изменить стиль поведения.

Социальные технологии, обеспечивающие процесс формирования партнерства и выступающие в качестве методов, форм и средств воздействия и

¹ Фурман В. Н. Указ. соч. С. 310.

регуляции человеческой деятельности, являются важнейшим элементом механизма партнерства между правоохранительными органами и гражданским обществом.

Институциональный фактор связан с управлением, регулированием отдельных сфер общественных отношений.

Повышение уровня вовлечения всех субъектов взаимодействия в решение данных проблем является основной предпосылкой партнерства между полицией и гражданским обществом, поскольку они не могут быть решены силами одной лишь полиции. Данная стратегическая задача решается в рамках социально-ориентированного подхода к управлению правоохранительной сферой, основными в котором являются различные социальные институты (экономические, политические, социокультурные, семейные и др.)¹.

Таким образом, с развитием общества трансформируются и способы, и формы мошенничества. Это достаточно ярко проявляется в области мошенничества в сфере кредитования. На сегодняшний день в России существует огромное количество организаций, специализирующихся на выдаче потребительских кредитов или занимающихся оказанием посреднических услуг в вопросе получения кредита в банке за определенный процент. Деятельность последних также вносит своей вклад в криминогенную обстановку в стране. Особенно это касается так называемой помощи будущему заемщику, имеющему негативную кредитную историю, в получении поддельных справок о доходах с места работы, подтверждении указанной в заявке на кредит заработной платы или должности, обеспечении поручителями, если по условиям банка необходимо их наличие. Зачастую мошенники уговаривают потенциального заемщика оформить кредит на свое имя с последующей передачей денежных средств третьим лицам. Арсенал методов убеждения весьма широк: от красноречивых аргументов о необходимости этого до обмана или введения в заблуждение и различных гарантий. Все это требует усиленной

¹ Полстовалов О. В. Указ. соч. С. 45-52.

работы полиции в части выявления подобных фактов деятельности указанных организаций, раскрытия и расследования уголовных дел, возбужденных по факту совершения мошенничеств в сфере кредитования.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволило сделать следующие выводы.

1. В соответствии с уголовным законом мошенничество понимается как хищение чужого имущества или приобретение права на чужое имущество путем обмана или же злоупотребления доверием.

2. Объектом мошенничества являются материальные и нематериальные ценности, подвергающиеся преступному воздействию. Предметом преступления являются вещи материальных или интеллектуальных ценностей, воздействуя на которые преступник нарушает общественные отношения, охраняемые уголовным законом. Основными признаками объективного характера мошенничества являются изъятие и (или) обращение имущества в пользу мошенника или иных лиц, противоправность, безвозмездность, ущерб собственнику имущества или иному владельцу, следствия и причинная связь. Субъективная часть рассматриваемого деяния характеризуется умыслом. Для основного состава мошенничества характерны общие субъекты, применяются общепринятые положения уголовного законодательства, то есть вменяемые физические лица, достигшие 16 лет.

3. Структурными элементами криминалистической характеристики мошенничества являются: обстановка мошенничества (типичные время, место и иные обстоятельства); способы подготовки, совершения и сокрытия мошенничества, а также присущие этой криминальной деятельности следы; характеристика мошенника и его соучастников, особенности их мотивации; характеристика потерпевших лиц; обстоятельства, способствовавшие мошенничеству.

4. Для обмана мошенники используют современные технологии, которые в современном мире постоянно развиваются. Сегодня каждое четвертое преступление совершается посредством сотовой связи или сети Интернет. Одним из признаков запланированного или осуществляемого преступления с использованием сотового телефона является представление преступников

сотрудниками службы безопасности банка и получение информации о банковской карте во время телефонного разговора. Еще одним важным тактическим приемом, позволяющим мошенникам дистанционным способом добраться до денежных средств потерпевших, является получение одноразового пароля (в виде SMS-сообщения), который отправляется на номер абонента, привязанный к банковской карте.

5. Сложности раскрытия и расследования современных видов мошенничеств связаны с отсутствием методических рекомендаций по организации расследования и тактике производства следственных действий; недостаточной квалификацией следователей, работающих со специфическими источниками доказательственной информации; низкой мобильностью правоохранительных органов, что накладывает отпечаток на процесс доказывания, поскольку преступления совершаются в режиме реального времени с использованием технических средств и преступник сразу имеет возможность распорядиться похищенными деньгами.

Приведенный нами перечень проблем, с которыми сталкиваются сотрудники оперативных и следственных подразделений в ходе раскрытия и расследования современных видов мошенничеств не является исчерпывающим. Чтобы сократить их число, мы предлагаем реализовать некоторые организационно-управленческие меры:

1) закрепить в рамках уголовно-процессуального закона обязанность кредитных организаций и операторов сотовой связи предоставлять запрашиваемую органами предварительного следствия или дознания информацию, в том числе охраняемую законом, в течение трех суток с момента получения соответствующего запроса;

2) на законодательном уровне запретить использование незарегистрированных номеров сотовой связи, установить административную ответственность операторов сотовой связи за невыполнение указанного запрета;

3) создать базу данных номеров сотовой связи, использовавшихся для

совершения мошеннических действий, обязать операторов сотовой связи уведомлять своих абонентов о том, что звонящий номер входит в эту базу.

Безусловно, важное значение в процессе прогнозирования и предупреждения преступлений против собственности будет иметь выработанная генеральная цель и миссия взаимодействия полиции и общества. Представляется наиболее понятной и доступной для большинства населения дифференциация стратегий (стратегических целей) по следующим направлениям взаимодействия: профилактика правонарушений; обеспечение охраны общественного порядка; борьба с преступностью.

В этих условиях речь можно вести о появлении информационных следов в виртуальном пространстве и о необходимости обнаружения, фиксации, изъятия и исследования информации, содержащейся на электронных носителях. Осуществить эту задачу самим следователем не всегда представляется возможным, так как требуется наличие специальных знаний в области информационных технологий, которыми следователи не обладают, требуется либо привлечение специалистов к участию в производстве следственных действий, либо назначение компьютерно-технических экспертиз.

Для эффективности борьбы с современными видами мошенничества необходимо повсеместное внедрение в следственную практику современной компьютерной техники, разработка, внедрение и использование следователями компьютерных программ, позволяющих анализировать исходные данные по уголовным делам об умышленных убийствах и предлагать следователям на основании этого рекомендации по определению наиболее оптимального пути расследования, алгоритмы разрешения складывающихся следственных ситуаций.

Важным остается создание автоматизированных рабочих мест для следователей, имеющих доступ к современным автоматизированным базам данных по уголовным делам и автоматизированным поисковым системам, а также базам данных не только правоохранительных органов, но и других организаций (например, многофункциональных центров). Это позволило бы

следователям оперативно получать необходимую поисковую, справочную информацию по делу, информацию о возможном местонахождении лиц и т. д.

Необходимым является внедрение в следственную практику современной цифровой техники. Следователи фактически активно используют цифровую технику, в частности средства сотовой связи, которые следователи используют для фиксации хода и результатов следственных действий (чаще всего проверки показаний на месте).

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:**I. Нормативные правовые акты и иные официальные документы**

1. Конституция Российской Федерации [Электронный ресурс] : (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 июня 1996 г. // Собр. законодательства Рос. Федерации. – 1996. – № 25, ст. 2954.

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 22 нояб. 2001 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 дек. 2001 г. // Собр. законодательства Рос. Федерации. – 2001. – № 52 (ч. 1), ст. 4921.

4. О полиции: Федеральный закон Рос. Федерации от 07.02.2011 № 3-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 28 янв. 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 2 фев. 2011 г. // Собр. законодательства Рос. Федерации. – 2011. – № 7, ст. 900.

II. Учебная, научная литература и иные материалы

1. Арсамерзаев И. С. Современные способы мошенничества, проблемы их выявления // Конкурс молодых ученых. 2020. С. 165-168.

2. Астапкина С. М. Методика расследования мошенничества: монография. Волгоград, 2004. 125 с.

3. Аюшина Д. В., Садыков Н. Б. Актуальные вопросы расследования мошенничества в сфере кредитования // Студенческий. 2017. № 15. С. 88-90.

4. Батров Б. Б. Криминалистическая профилактика интернет-мошенничеств: проблемы раскрытия и расследования // Вестник Бурятского

государственного университета. Юриспруденция. 2021. № 1. С. 21-28.

5. Беняминов Ю. Д. Обстоятельства, подлежащие доказыванию при расследовании мошенничества в сфере кредитования // Образование. Наука. Научные кадры. 2016. № 5. С. 37-39.

6. Денисов А. А. Криминалистическая характеристика мошенничества // Тенденции развития науки и образования. 2021. № 6. С. 31-33.

7. Евсеева Е. М. Методика расследования преступлений в сфере кредитования // Академическая публицистика. 2019. № 8. С. 40-43.

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

9. Зарипова Е. А. Некоторые проблемы квалификации мошенничества // Меридиан. 2021. № 3. С. 81-83.

10. Колесникова Н. А. Разнообразие способов совершения мошенничеств в современных условиях // Евразийский юридический журнал. 2019. № 1. С. 275-277.

11. Колескин Д. В. Теория развития мошенничества, современные виды мошенничества и способы борьбы с ними. Белгород, 2020. 42 с.

12. Коробов С. А. Специфика криминалистической характеристики мошенничества // Молодой ученый. 2021. № 6. С. 223-226.

13. Кузьменко Е. С. Расследование мошенничества в сфере кредитования – нюансы доказывания и некоторые следственные ситуации // Вестник Нижегородской академии МВД России. 2016. № 2. С. 427-431.

14. Мартынов А. Н. Особенности использования правовых категорий при разработке методики расследования мошенничества в сфере кредитования // Социум и власть. 2014. № 2. С. 80-83.

15. Мелихова Л. И. Мошенничество с использованием средств сотовой связи: характеристика и виды. Ростов-на-Дону, 2021. 673 с.

16. Парунов И. М. Мошенничества, совершаемые на современном этапе развития общества. Гатчина, 2021. 165 с.

17. Полстовалов О. В. К исследованию способов совершения организованных форм мошенничества в новой экономической реальности // Вестник Института права Башкирского государственного университета. 2020. № 3. С. 45-52.

18. Потемкина М. О. Особенности раскрытия и расследования современных способов мошенничества в условиях крупного города. М., 2020. 222 с.

19. Синенко Н. А. К вопросу о криминалистической характеристике мошенничества в сфере кредитования // Аллея науки. 2018. № 1. С. 696-699.

20. Сорокун Н. С., Замалева С. В. Особенности современного мошенничества // Вестник Дальневосточного юридического института МВД России. 2021. № 2. С. 69-74.

21. Струков А. Е. Понятие и способы мошенничества // Вестник магистратуры. 2022. № 1-2. С. 10-12.

22. Филиппов А. Р. Феномен мошенничества в России XXI века: уголовно-правовая, криминологическая и социально-психологическая характеристика // Юридическая наука: история и современность. 2021. № 6. С. 134-146.

23. Фурман В. Н. Современные виды мошенничества, способы совершения и их предупреждение. Великий Новгород, 2021. 311 с.

24. Хутуев В. А., Машекуашева М. Х. Некоторые вопросы квалификации мошенничества // Проблемы экономики и юридической практики. 2019. № 4. С. 123-125.

25. Чечель Г. И., Третьяк М. И. Мошенничество: вопросы квалификации // Общество и право. 2015. № 3. С. 63-65.

26. Шут О. А. Мошенничество в социальных сетях и способы его осуществления // Вестник Омского университета. Серия: Право. 2020. № 4. С. 97-106.

27. Яблоков Н. П. Криминалистика: учебник. М.: Юрайт, 2019. 489 с.

28. Явинский А. В., Соловьев А. А. Способы противодействия

телефонному мошенничеству. Омск, 2021. 373 с.

29. Яковлева Л. В. Современные способы совершения дистанционного мошенничества // Вестник Краснодарского университета МВД России. 2021. № 4. С. 77-80.

30. Яковлева Л. В., Яковлев В. В. Способы совершения мошенничеств и использованием современных технологий // Евразийский юридический журнал. 2020. № 12. С. 378-380.

III. Эмпирические материалы

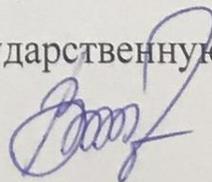
1. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда Российской Федерации. 2018. № 2.

2. Приговор № 1-10/2015 1-159/2014 от 14 января 2015 г. по делу № 1-10/2015. [Электронный ресурс]. Режим доступа: URL: //http://sudact.ru. (Дата обращения: 10.01.2022).

3. Приговор суда по ч. 1 ст. 159.1 УК РФ № 1-5/2017 (1-329/2016). [Электронный ресурс]. Режим доступа: URL: //http://sudact.ru (дата обращения: 10.01.2022).

Материал вычитан, цифры, факты, цитаты сверены с первоисточником.

Материал не содержит сведений, составляющих государственную и служебную тайну.



Власов И.С.

