

Министерство внутренних дел Российской Федерации

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

Кафедра криминалистики

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

**на тему «Особенности расследования мошенничеств с использованием
платежных карт»**

Выполнил: Козлов Н.М.

(фамилия, имя, отчество)

40.05.02. - Правоохранительная деятельность,

(специальность, год набора, № группы)

2012 год набора, 024 группа

Руководитель:

К.п.н., старший преподаватель кафедры

(ученая степень, ученое звание, должность)

криминалистики Хайруллова Э.Т.

(фамилия, имя, отчество)

Рецензент:

(ученая степень, ученое звание, должность)

(фамилия, имя, отчество)

К защите _____

(допущена, дата)

Начальник кафедры _____

Дата защиты: "___" _____ 20__ г.

Оценка _____

Казань 2017

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНЫХ КАРТ.....	7
§1. Платежные карты как средство совершения мошенничества.....	7
§2. Способы и обстоятельства совершения преступления.....	10
§3. Личность преступника.....	22
§4. Криминалистически значимые данные о механизме следообразования.....	27
ГЛАВА 2. АКТУАЛЬНЫЕ ПРОБЛЕМЫ (ВОПРОСЫ) РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНЫХ КАРТ.....	32
§1. Особенности первоначального этапа расследования.....	32
§2. Организационно-тактические особенности производства следственных действий (ОМП, допрос и др.).....	35
§3. Использование специальных познаний при расследовании мошенничеств с использованием платежных карт.....	53
ЗАКЛЮЧЕНИЕ.....	68
СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ.....	71

ВВЕДЕНИЕ

Актуальность темы исследования. По оценкам американской компании FICO, в 2015 году Россия заняла первое место в Европе по темпам роста убытков от мошеннических операций с банковскими картами. Объем этих потерь вырос на 27,6% по сравнению с показателем 2013 года и, следовательно, в 10 раз в сопоставлении с данными 2006 года и на 65% по отношению к 2008 году. По объему этих потерь, которые увеличились на 22,5 млн. евро и достигли 104,1 млн. евро, Россия находится на четвертом месте среди 19 европейских стран. Ее опережают Великобритания (534,9 млн. евро), Франция (428,9 млн. евро) и Германия (116,3 млн. евро). Таковы данные интерактивной карты "Эволюция карточного мошенничества в Европе - 2015".

Примечательно, что в России мошенничеств с картами Card Not Present (операции по карте без ее физического присутствия, в частности оплата виртуальными картами и т.д.) намного меньше, чем в странах Западной Европы (в России их доля лишь 3%). Одна треть российских убытков (1683,8 млн. руб.) приходится на Counterfeit Cards (фальшивые карты, на магнитных полосах которых содержится информация с легально выпущенной карты: имя держателя, номер карты, срок окончания срока ее действия, CVV- и CVC-код) и примерно столько же (1599,4 млн. руб.) - на Lost and Stolen (утраченная/украденная карта). Мошенничество ID Fraud (получение кредитной карты по поддельным (или украденным) документам) нанесло ущерб в размере 685,2 млн. руб. Как подсчитали в FICO, в 2013 году совокупные убытки от карточного мошенничества в 19 странах Европы составили 1,55 млрд. евро, немного превысив показатель 2008 года, когда наблюдалось последнее пиковое значение.

В феврале 2015 года Приволжский райсуд г. Казани вынес приговор по уголовному делу в отношении двух граждан Болгарии Цветомира и Митко Димитровых, которые за несколько месяцев с помощью поддельных банковских карт похитили у россиян свыше 4 млн. руб. Как установил суд, в

2013 году они установили на уличные банкоматы оборудование для незаконного копирования компьютерной информации, получив реквизиты более 1,8 тыс. банковских карт и пин-коды к ним. Затем с помощью изготовленных за рубежом дубликатов карт уже в российских городах они похитили деньги на общую сумму 4,6 млн. руб. По данным следствия, они снимали деньги в Туле, Рязани, Новомосковске, Калуге, Саратове, Балашове, Самаре и Пензе. Кроме того, находясь в Самаре, они аналогичным способом получили информацию о реквизитах почти 1,4 тыс. банковских карт и пин-коды к ним. В результате суд приговорил Ц. Димитрова к 5 годам лишения свободы, а М. Димитрова - к двум с половиной годам лишения свободы¹.

Банк обязан информировать клиента о каждой операции, совершенной с использованием банковской карты, путем направления клиенту соответствующего уведомления в порядке, установленном договором с клиентом (ч. 4 ст. 9 Закона от 27.06.2011 N 161-ФЗ²). Способы направления уведомлений, используемые банками, различны - это могут быть и смс-уведомления, и рассылка по электронной почте, и информирование через интернет-банк. При этом хотя бы один из способов информирования должен быть бесплатным для клиента.

Причин для возникновения вопросов по списанию денег с карты может быть много.

Например, при совершении покупки с использованием банковской карты деньги иногда сразу не списываются, а только блокируются на счете. Фактическое списание происходит в течение нескольких дней. Но бывают случаи, когда с даты покупки до даты списания проходит более длительное время, иногда до двух - трех недель. Соответственно, не всегда сразу можно вспомнить, что деньги списаны по ранее совершенной покупке.

Также бывают случаи, когда смс-сообщения о проведенных операциях по техническим причинам приходят с задержкой в несколько часов, что также

¹ Решение Приволжского районного суда города Казани от 23.02.2015 г. // Архив электронных решений суда

² Федеральный закон от 27.06.2011 N 161-ФЗ (ред. от 03.07.2016) "О национальной платежной системе" (с изм. и доп., вступ. в силу с 17.07.2016) // Российская газета. – 2011.- N 139.

может вызвать опасения неправомерного использования вашей карты третьими лицами.

Однако, часто встречаются случаи мошенничества с платежными картами. Соответственно, учитывая современное развитие общества у законодателя встала необходимость правового регулирования данного института нормами уголовного права, выявив в составе мошенничества отдельную норму по мошенничеству с платежными картами.

Современные информационные технологии сделали необычайно легким отчуждение произведения от его носителя. Копирование и передача объектов интеллектуальной собственности в цифровой форме имеют ничтожную себестоимость и доступны практически всем. Это способствует легкости нарушения прав и затрудняет борьбу с такими нарушениями. Без всякого сомнения в ближайшее время следует ожидать усиления борьбы с нарушениями именно прав интеллектуальной собственности.

Объектом исследования является комплекс общественных отношений, возникающих в связи с совершением мошенничества с использованием платежных карт.

Предметом исследования являются закономерности методики расследования мошенничества с использованием платежных карт.

Цель исследования – анализ теоретических положений по совершенствованию методики расследования мошенничества с использованием платежных карт.

Для достижения указанной цели необходимо решить следующие задачи:

- рассмотреть различные виды и основные характеристики платежных карт, выступающие, как средство совершения мошенничества.

- раскрыть способы и обстоятельства совершения мошенничества с использованием платежных карт.

- личность преступника, совершившего мошенничество с использованием платежных карт.

- проанализировать криминалистически значимые данные о механизме следообразования.

-изучить особенности первоначального этапа расследования.

-раскрыть организационно-тактические особенности производства следственных действий

-обосновать возможность использование специальных познаний при расследовании мошенничеств с использованием платежных карт.

Методология исследования складывается из общенаучных методов познания, таких как анализ, синтез, обобщение, а также частных научных методов исследования таких как: сравнительно-правовой, формально-юридический, системно-структурный, конкретно-логический, статистический.

Структура работы обусловлена целью и задачами исследования и включает в себя введение, две главы, семь параграфов, заключение и список использованной литературы.

ГЛАВА 1. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА МОШЕННИЧЕСТВ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНЫХ КАРТ

§1. Платежные карты как средство совершения мошенничества

В связи с динамичным ростом числа преступлений, совершаемых в целях хищения денежных средств с использованием высоких технологий в банковской сфере, был принят Федеральный закон от 08.06.2015 N 153, направленный на усиление уголовной ответственности за такие преступления. Ранее Федеральным законом от 27.06.2011 N 161-ФЗ "О национальной платежной системе" было введено определение электронного средства платежа, под которым понимаются средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверить и передавать распоряжения для осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

С 1 января 2014 года вступили в силу положения ст. 9 Закона N 161-ФЗ, согласно которым в случае совершения мошеннических операций с использованием электронных платежных средств ответственность за перевод денежных средств без согласия клиента несет оператор, если он не докажет нарушения правил использования электронного средства клиентом³.

Кроме того, с 16 марта 2015 года вступили в силу новые требования ЦБ России по борьбе с мошенничеством при дистанционном обслуживании граждан. Теперь банки обязаны блокировать рассылку служебных СМС (одноразовые пароли и пр.) при смене клиентом номера или сим-карты.

По заявлению клиента банк определяет параметры операций, которые могут осуществляться через интернет и мобильный банкинг. В частности, банк

³ Сухаренко А. Скимминг вне закона // ЭЖ-Юрист. 2015. N 37. С. 3.

устанавливает перечень устройств, с помощью которых может осуществляться доступ к системам дистанционного банковского обслуживания (ДБО) в целях перевода денег на основе идентификаторов данных устройств. Наряду с этим банк устанавливает максимальную сумму перевода клиента через ДБО за одну операцию и (или) за определенный период времени (один день/один месяц). Указанные требования изложены в указании ЦБ N 3361-У, которое изменяет Положение регулятора 382-П.

Новеллой в нашей стране является криминализация хищения чужого имущества с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации. При этом следует иметь в виду, что ст. 159.3 УК РФ <1> ("Мошенничество с использованием платежных карт") включена в уголовное законодательство сравнительно недавно, в ноябре 2012 года, ФЗ №207. В целом же незаконное обращение банковских карт регулируется руководящими разъяснениями Пленума Верховного Суда Российской Федерации⁴, согласно требованиям которого хищение чужих денежных средств, находящихся на счетах в банках, путем использования похищенной или поддельной кредитной либо расчетной карты следует квалифицировать как мошенничество только в тех случаях, когда лицо путем обмана или злоупотребления доверием ввело в заблуждение уполномоченного работника кредитной, торговой или сервисной организации (например, в случаях, когда, используя банковскую карту для оплаты товаров или услуг в торговом или сервисном центре, лицо ставит подпись в чеке на покупку вместо законного владельца карты либо предъявляет поддельный паспорт на его имя).

Особый интерес представляет то обстоятельство, что хищение чужих денежных средств путем использования заранее похищенной или поддельной кредитной (расчетной) карты не образует состава мошенничества, если выдача наличных денежных средств осуществляется посредством банкомата без

⁴П. 12 - 14 Постановления Пленума Верховного Суда Российской Федерации N 51 "О судебной практике по делам о мошенничестве, присвоении и растрате" от 27 декабря 2007 г. \СПС «Консультант Плюс». – URL: <http://www.consultant.ru> (дата обращения: 05.10.2016).

участия уполномоченного работника кредитной организации. При этом содеянное подлежит квалификации по соответствующей части ст. 158 УК РФ.

Банковское оборудование тоже совершенствуется: появляется все больше банкоматов с различными системами антискимминговой защиты. На сегодняшний день уже есть решения, которые позволяют исключить считывание информации с магнитной полосы карты всеми существующими сегодня типами скимминговых устройств. Также банкоматы обладают средствами защиты против такого вида мошенничества, как card-траппинг (захват карты мошенниками). К тому же считываемая с карты информация всегда передается в зашифрованном виде, чтобы исключить возможность перехвата данных.

Сейчас многие банки переходят на технологию выпуска чиповых карт, где предусмотрена функция ввода пин-кода. А на случай совершения операции по карте в местах массового скопления людей некоторые банки предоставляют возможность отказаться от ввода пин-кода, тогда операция подтверждается только подписью владельца карты на чеке. Также набирает популярность технология 3D-Secure, которая является дополнительным фактором защиты онлайн-транзакций. Для подтверждения покупки необходимо ввести одноразовый пароль, который направляется держателю карты посредством СМС-сообщения на номер телефона, указанный ранее в банке.⁵

Единственным документом, который разграничивает понятие между различными видами карт является Положение Центрального банка Российской Федерации (далее — ЦБ РФ) «Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт» от 24 декабря 2004г. №266-П[20], то его изучение позволило прийти к следующему выводу: что кредитные и расчетные карты являются платежными. То есть с их помощью осуществляются платежи между покупателем и продавцом или используются для получения наличных денежных средств. Платежные карты могут быть как банковскими (VISA, MasterCard), так и небанковскими (American Express, Diners Club, JCB и др.).

⁵ Сухаренко А. Скимминг вне закона // ЭЖ-Юрист. 2015. N 37. С. 3.

Деление карт на кредитные или расчетные зависит от характера договорных отношений между эмитентом карты и клиентом. В случае наличия кредитного договора операции с использованием карт осуществляются за счет заемных средств, следовательно, такие карты являются кредитными.

Кредитная карта предназначена для совершения ее держателем операций, расчеты по которым осуществляются за счет денежных средств, предоставленных кредитной организацией — эмитентом клиенту в пределах установленного лимита в соответствии с условиями кредитного договора. При осуществлении операций за счет собственных средств клиента или предоставленного кредита карты являются расчетными.

Расчетная (дебетовая) карта предназначена для совершения операций ее держателем в пределах установленной кредитной организацией — эмитентом суммы денежных средств (расходного лимита), расчеты по которым осуществляются за счет денежных средств клиента, находящихся на его банковском счете, или кредита, предоставляемого кредитной организацией — эмитентом клиенту в соответствии с договором банковского счета при недостаточности или отсутствии на банковском счете денежных средств (овердрафт).

На сегодняшний день, помимо банковских кредитных и расчетных карт, существуют еще и предоплаченные банковские карты. Предоплаченная карта предназначена для совершения ее держателем операций, расчеты по которым осуществляются кредитной организацией — эмитентом от своего имени, и удостоверяет право требования держателя предоплаченной карты к кредитной организации — эмитенту по оплате товаров (работ, услуг, результатов интеллектуальной деятельности) или выдаче наличных денежных средств.

§2. Способы и обстоятельства совершения преступления

Развитие современных технологий оказывает влияние и на криминальную сферу, особенно это касается хищений с использованием

платежных карт: если раньше на благосостояние граждан посягали лишь карманные и квартирные воры, то теперь с развитием онлайн-банкинга на охоту вышли такие "продвинутые" преступники, как фишеры, скиммеры и организаторы разнообразных мошеннических схем.

Мошеннические операции с пластиковыми картами уже не первый год являются проблемой как владельцев карточек, так и российской банковской сферы. Большая доля незаконных списаний происходит с помощью скимминга, т.е. считывания при помощи специального устройства данных с магнитной полосы карты. В России, по подсчетам компании Visa, доля скимминга в общем объеме мошеннических операций с картами этой системы достигает 49%. А еще 51% приходится на другие виды мошенничеств, имеющих целью завладеть данными банковских карт и паролями от кабинетов в системах интернет-банкинга⁶.

При совершении данного преступления существует личный контакт мошенника и уполномоченного работника кредитной, торговой и иной организацией, таким образом, необходимо отметить, что местом совершения преступления в большинстве случаев, является офисное здание кредитной, банковской или торговой организации, что при определенных ситуациях и условиях является плюсом при раскрытии и расследования данного преступления.

Временем совершения преступления является рабочее время, соответственно время функционирования кредитной, банковской или иной организацией.

Как известно, способ совершения преступления является основополагающим системообразующим элементом характеристики преступления. Его информационно-поисковое значение играет огромную роль при раскрытии и расследовании преступления. При владении информации о способе совершения мошенничества появляется возможность выдвигать

⁶ На златом крыльце сидели: скимминг, фишинг и аккаунт. Советы Центрального банка: как владельцам пластиковых карточек уберечься от финансовых мошенников // Юрист спешит на помощь. 2015. N 6. С. 30 - 32.

обоснованные версии о других элементах криминалистической характеристики конкретного преступления.

В криминалистическом смысле мошенничество с использованием платёжных карт можно определить как систему действий по подготовке, совершению и сокрытию хищения чужого имущества, основным содержанием которой является использование поддельной или принадлежащей другому лицу кредитной, расчётной или иной платёжной карты для осуществления обмана уполномоченного работника кредитной, торговой или иной организации. Фактически в этом случае, как и в других видах мошенничества, содержанием мошеннических действий остаётся в той или иной степени качественная или количественная замена предмета и средств совершения мошенничества. Классификации способов мошенничества с использованием платёжных карт по самым различным основаниям представлены в работах ряда авторов. Анализируя действующее законодательство с учётом произошедших изменений, вышеуказанные работы, а также сложившуюся практику расследования данной разновидности криминального обмана, можно выделить ряд классификаций, которые, на наш взгляд, имеют наибольшее значение в криминалистическом смысле.

В самой статье 159.3 УК РФ фактически представлен ряд оснований для классификации способов мошенничества с использованием платёжных карт. Так, их можно классифицировать в зависимости от того, какая разновидность платёжной карты была задействована мошенниками для совершения преступления. Соответственно, имеет смысл говорить о способах, в которых были использованы: а) кредитная карта; б) расчётная карта; в) иная платёжная карта (УК РФ).

Другим основанием для классификации способов является характеристика лица, на которое были направлены обманные действия при совершении преступления. По данному основанию способы мошенничества с использованием платёжных карт могут быть ранжированы на три категории: 1) криминальный обман уполномоченного работника кредитной

организации; 2) криминальный обман уполномоченного работника торговой организации; 3) криминальный обман работника иной организации (ст. 159.3 УК РФ)⁷

Криминалистическое значение имеет также разделение способов совершения мошенничества с использованием платежных карт в зависимости от количества лиц, участвующих в совершении данного преступления. Таким образом, можно выделить такие способы обмана как: совершенные в одиночку или в составе группы лиц. Наибольшую опасность составляет совершение мошенничества, в составе организованной группы.

Имеется мнение, что, как и другие киберпреступления с использованием платежных карт, нередко совершаются членами разветвленных хорошо организованных преступных групп, участники которых имеют свою криминальную специализацию. Специализация в группе может выглядеть так: одни члены группы осуществляют сбор информации по платежным картам, другие анализируют собранную информацию и передают их тем, кто занимается изготовлением поддельных карт. Подготовленное таким образом хищение осуществляют лица, которые специализируются на «вещевом кардинге» именно они используют платежную карту для обмана работников торговой организации.

Еще одним основанием для классификации способов мошенничества с использованием платежных карт, является использованием преступником поддельной карты, либо карты принадлежащей другому лицу. Примером последнего может служить уголовное дело, в ходе которого установлено что М. тайно похитил чужое имущество среди, которого находилась платежная карта потерпевшего. М. завладел данной картой и решил использовать её в противоправных целях. С целью реализации своего преступного умысла, М. неоднократно использовал данную карту для приобретения различных товаров. Данный способ совершения мошенничества не представляет

⁷Способы мошенничества с использованием платежных карт, как элемент криминалистической характеристики данного вида преступлений И.О Антнов, А.Н. Шалимов Учен. зап. Казан. ун-та. Сер. Гуманит. науки. - 2012. - Т. 155, кн. 4. - С. 196-202.

особых сложностей для предварительного расследования по уголовному делу, чего нельзя сказать о использовании мошенником поддельной карты.

Говоря о использовании поддельной карты при совершении мошенничества, необходимо отметить, что данный способ является наиболее квалифицированным, так как при совершении мошенничества данным способом, как правило действуют организованные группы, в которых четко распределены роли среди соучастников, что представляет сложность для выявления таких преступлений, а также в целом для предварительного расследования.

Для совершения мошенничества с использованием поддельных платежных карт, злоумышленникам необходимо получить информацию о держателях карты её реквизитах и иных данных, такой способ получения информации зачастую является самостоятельным преступлением такими как ст. 272, ст. 183, ст.327 УК РФ. Такую информацию злоумышленники получают с использованием различных методов и технических устройств.

1) Скимминг – вид мошенничества с банковскими картами, который предусматривает использование различных устройств типа – скиммер. С помощью таких устройств мошенники считывают информацию, содержащуюся на магнитной полосе карты. Скиммеры, как правило, прикрепляются к банкоматам, а именно – к принимающему слоту. PIN-код карты фиксируется с помощью дополнительно закрепленной рядом с банкоматом видеокамеры. Подобные устройства обычно оснащены передатчиками, дистанционно передающими полученную информацию. После получения информации с карты, мошенники изготавливают дубликат карты, и зная, PIN-код могут снять деньги со счета владельца подлинной карты.

Так, в ноябре в 2013 года жители г. Казани Л. И К. приобрели четыре скиммера. Устанавливали скиммеры в Казани. После установки запрещенного оборудования в ноябре 2013 года преступники получили данные нескольких десятков карт людей, которые воспользовались банкоматами. Дело было за изготовлением дубликатов, посредством которых можно снять деньги со счетов. Как выяснилось, Л. и К. не собирались заниматься этим сами, а хотели

продать полученные сведения неким неустановленным лицам, которые сделали бы за них дальнейшую работу.

2)Новейшие технологии, взятые на вооружение преступниками, позволили им модернизировать устройства, используемые для скимминга. В данном случае речь идет о шимминге. В шимминге вместо традиционных громоздких накладок на щель приемника пластиковых карт банкоматов (скиммеров) используется очень тонкая, гибкая плата, внедряющаяся через эту щель внутрь банкомата. "Шим" подсаживается при помощи специальной карты-носителя: ее просовывают в щель банкомата, где тонкий "шим" подсоединяется к контактам, считывающим данные с карт, после чего карта-носитель удаляется. Далее все работает, как и при традиционном скимминге — т.е. со вставляющихся в банкомат пластиковых карт считываются все важные данные, которые затем используются злоумышленниками для производства карт-дубликатов и снятия с их помощью денег. Единственное, но крайне важное отличие от скимминга состоит в отсутствии каких-либо внешних признаков того, что в банкомате сидит "жучок". Исходя из спецификаций, регулирующих размеры щели кардридера, толщина "шима" не должна превышать 0,1 мм, иначе он будет мешать пластиковым картам. Это примерно вдвое тоньше человеческого волоса. Кроме того, "шим" должен обладать определённой гибкостью, чтобы его можно было внедрить в банкомат. Поэтому производство такой платы — задача нетривиальная.

3)Помимо названных устройств, преступники могут также использовать более громоздкие технологии, например фальшивые банкоматы.

4)Методы социальной инженерии востребованы в процессе так называемого фишинга, Фишинг (от англ. phishing, от password — пароль и fishing — рыбная ловля, выуживание) – это вид интернет-мошенничества, основанный на незнании пользователями норм сетевой безопасности, целью которого является получение доступа к конфиденциальным данным - логинам и паролям.

Фишинг-атаки проводятся через электронную почту, всплывающие

сообщения и ссылки на фишинговые веб-сайты, с целью обманным путем выявить у получателя личную информацию, часто финансового характера. Фишинг распространяется через интернет-мошенников посредством электронных писем или всплывающих сообщений, часто от имени представителя известного финансового учреждения.

Большинство методов фишинга (известного также как бренд-спуфинг или кардинг) – сводится к тому, чтобы замаскировать поддельные ссылки на фишинговые сайты под ссылки настоящих организаций. Кроме рисков получения большого количества спама, атаки фишеров не вредят работе компьютера. Однако, при краже личных данных этот вид мошенничества может привести к значительному ущербу. Заполучив единожды чью-либо личную информацию, мошенник сможет воспользоваться кредитом или совершить преступление от этого имени.

5) Наиболее современным методом является вишинг, т.е. голосовой фишинг, реализуемый посредством мобильной телефонной связи.

6) Широкий общественный резонанс о ставших известных способах выведывания мошенниками конфиденциальной информации снизил эффективность фишинговых атак, что привело к изобретению «фарминга». Суть фарминга сводится к автоматическому перенаправлению пользователей на фальшивые сайты с целью хищения конфиденциальной информации, например, паролей и номеров банковских счетов. В отличие от фишинга, фарминг-атаки практически не требуют выполнения каких-либо действий потенциальной жертвой. При проведении фарминг-атак киберпреступники используют уязвимости в браузерах, операционных системах, а также программном обеспечении DNS-серверов.

Новый тип фарминг-атак получил название Drive-by Pharming. Суть его сводится к тому, что злоумышленники меняют настройки маршрутизаторов или беспроводных точек доступа в интернет, после чего пользователи, сами того не подозревая, перенаправляются на вредоносные сайты. Данный тип атак представляет угрозу, прежде всего, для тех пользователей, которые подключены к Сети посредством широкополосных линий. Сценарий

нападения, как правило, предполагает применение JavaScript-кода, который и вносит изменения в настройки оборудования потенциальной жертвы.

Согласно исследованию, проведенному специалистами Университета Индианы, порядка 50 процентов пользователей широкополосных каналов теоретически могут стать жертвами атак Drive-by Pharming. Специалисты настоятельно рекомендуют установить на маршрутизаторах пароль или сменить заводской пароль, угадать который для злоумышленников практически не составляет труда. Кроме того эксперты советуют не пренебрегать брандмауэрами, средствами обнаружения вторжений и стараться не переходить по ссылкам, полученным из неизвестных или ненадежных источников. После этого как владелец карты выполнит стандартную процедуру ввода платежных реквизитов, он перенаправляется на официальный сайт банка.

Далее необходимо отразить функции, которые выполняют различные участники преступных групп и весь механизм совершения преступления.

В настоящее время выявлено наличие криминальных сетевых групп и сообществ, к которым можно отнести, например, спамеров, кардеров, фишеров и.т.д.

1)Спамеры. Деятельность группы спамеров состоит в том, что первое лицо создает и совершенствует программное обеспечение для скрытого внедрения на компьютеры пользователей (тройные программы или трояны), второе лицо приобретает право на использование указанной программы, рассылает ее в массовом порядке, принимает сигналы и учитывает успешно внедрившиеся экземпляры троянцев, объединяет их в структурированную зомби-сеть, которую (полностью или частично, постоянно или на неопределенное время) приобретает третье лицо, осуществляющее с ее помощью рассылку спама, заказ на который приобретает четвертое лицо, в то время как пятая группа соучастников занимается сбором и верификацией адресов электронной почты для рассылок.

2)Деятельность кардеров заключается в том, что первый из сообщников занимается сбором атрибутов банковских карт, зачастую имея легальный доступ к ним. Второй из сообщников играет роль организатора криминального

бизнеса, аккумулируя у себя данные и передавая их исполнителям. Третье лицо исполняет по заказам второго верификацию реквизитов карт, т.е. проверяет их действительность, доступность для платежей. Четвертый - создает и поддерживает структуру с возможностью оплаты услуг карточками, обеспечивая механизм для отмыwania денег. Пятая группа сообщников (набивщики) получают от второго партии номеров банковских карт и вводят их через отмывочное предприятие под видом разных клиентов, при помощи технических средств, эмулируя доступ из разных стран и с разных компьютеров. Шестая группа, получая наиболее перспективные номера кредитных карт, осуществляет реальную закупку товаров, которые незначительны по размерам и легко перепродаются (телефоны, видеокамеры, запчасти к автомашинам). Указанные товары заказываются на адрес еще одной категории участников - дропов, которые проживают в преуспевающих странах, подвергаются проверке на состоятельность, получают товар и тут же перенаправляют его седьмой группе - реализаторам.

3) В деятельности фишеров первый сообщник занимается размещением подложных веб-сайтов банков или иных учреждений. В состав программ такого сайта входит система для моментальной отсылки предоставленных клиентом конфиденциальных данных злоумышленнику. Второй изготавливает указанные сайты, составляет подложные письма и рассылает их, пользуясь для этого услугами спамеров. Третий сообщник занимается реализацией полученных данных (номера карт с ПИН-кодами или пароли к платежным системам) кардерам или иным криминальным структурам.

Таким образом, формирующаяся преступность в сфере электронного бизнеса может иметь признаки международной, преступления могут совершаться как группой лиц по предварительному сговору, так и организованными преступными сообществами.

На первом этапе разнообразными способами преступники получают данные о банковских карточках, как правило, при соучастии лиц, имеющих возможность незаметно снимать данные с карточек клиентов как в силу своего служебного положения, так и с применением специальных вредоносных

программ-шпионов или посредством фишинга. Можно выделить следующие способы получения данных банковских карт:

- дистанционный неправомерный доступ к серверу, на котором такие данные хранятся или обрабатываются;
- доступ к указанным данным с применением служебного положения и недостатков в системе защиты информации предприятия;
- перехват трафика, когда данные карты передаются в открытом виде (по протоколу НТТР или по электронной почте);
- получение данных банковских карт или снятие дампа при обслуживании клиентов в предприятиях питания или торговли;
- выманивание данных карт и иногда ПИН-кодов у владельцев методами фишинга;
- получение дампов и ПИН-кодов при помощи фальшивых банкоматов или приставок к банкоматам (скиминг);
- получение самой карточки мошенническим способом ("ливанская петля" и др.);
- обычная кража карты у ее держателя (бывает, что ПИН-код записан на ней или на листке, лежащем в том же бумажнике).

Реализация данных с банковских карт, то есть обращение их в деньги, может производиться следующими способами:

- вещевой кардинг - приобретение в интернет-магазинах или в реальных магазинах (при наличии дампа карты) ликвидных товаров, чаще на продажу, реже на заказ, последующая их реализация;
- совершение фиктивных покупок в интернет-магазинах или приобретение услуг платных сайтов по сговору с их владельцами; при помощи данных чужой карты производится оплата, биллинговое предприятие (оно не участвует в сговоре) учитывает платеж и переводит магазину за вычетом своей комиссии, магазин переводит обусловленную долю кардеру;
- игра в интернет-казино, когда нанятые кардером игроки регистрируют в интернет-казино много аккаунтов на имя владельцев карт, вносят с карт депозит, играют, а затем для тех аккаунтов, где образовался выигрыш,

проводят процедуру вывода средств;

- использование иных интернет-сервисов, где возможно получение денег, например, организующих показ любительского видео;

- (редко) вымогательство у магазина, банка, иного предприятия, несущего ответственность за сохранность данных; за утрату и разглашение данных о картах клиентов предприятие может подвергнуться санкциям со стороны платежной системы, получить большой ущерб деловой репутации, может стать ответчиком по искам клиентов - за избавление от этих неприятностей многие готовы заплатить кардерам-вымогателям;

- обналичивание в банкоматах; когда есть дамп карты и ПИН-код, то изготавливается твердая копия карты (так называемый белый пластик, потому что внешнее оформление для банкомата не требуется), с которой в банкоматах снимается максимально возможная сумма за минимально возможное время.

Спецификой данной категории дел, в случае если мошенничество совершается участниками организованных групп является, то что при подготовке к преступлению, совершаются самостоятельные преступления, как правило это преступления которые охватываются, следующими составами Уголовного кодекса РФ: статья 187. Неправомерный оборот средств платежей. Статья 175. Приобретение или сбыт имущества, заведомо добытого преступным путем. Статья 272. Неправомерный доступ к компьютерной информации. Статья 273. Создание, использование и распространение вредоносных компьютерных программ, а в некоторых случаях и статья 274 нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Изготовление в целях сбыта или сбыт поддельных кредитных или расчетных банковских карт квалифицируется по статье 187 УК РФ. Изготовление лицом поддельных банковских расчетных либо кредитных карт для использования в целях совершения этим же лицом преступлений, предусмотренных частью 3 или частью 4 статьи 159 УК РФ, следует квалифицировать как приготовление к мошенничеству. В случаях, когда указанные деяния сопряжены с неправомерным внедрением в чужую

информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по статье 159 УК РФ, а также, в зависимости от обстоятельств дела, по статьям 272 или 273 УК РФ, если в результате неправомерного доступа к компьютерной информации произошло уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Представленные классификации способов мошенничества с использованием платежных карт позволяют более точно оценить возможные корреляционные связи между элементами криминалистической характеристики этого рода мошенничества. Большое значение необходимо уделить зависимости вида, способа и механизма преступного поведения от особенностей связи преступника с предметом преступного посягательства, обстановкой сложившейся на месте совершения преступления и вокруг него; следует также учитывать влияние на эту связь личностно-типологических свойств преступника, степени организованности, разветвленности и состава преступной группы, при её наличии.

Подводя итог вышесказанному, можно сказать, что исследовании мошенничеств с использованием платежных карт, анализ существующих способов совершения мошенничества и методов сбора информации, необходимой для совершения преступления, а также прогнозирование появления новых способов совершения данных преступлений способствует раскрытию данных преступлений и выводит на более качественный уровень предварительного расследования данной категории дел.

§3. Личность преступника

Важным элементом криминалистической характеристики компьютерных преступлений является личность преступника. Субъект преступления – это минимальная совокупность признаков, характеризующих лицо, совершившее преступление, необходимых для привлечения его к уголовной ответственности. Именно личностные качества человека и внешняя среда в своем взаимодействии последовательно определяют мотивацию принятия решения относительно преступной деятельности. Мотивация включает процесс возникновения, формирования мотива преступного поведения и его цели. Мотив преступного поведения следует рассматривать как понуждение, сформировавшееся под влиянием социальной среды и жизненного опыта личности, которое является внутренней непосредственной причиной деятельности, и выражает личностное отношение к тому, на что направлена преступная деятельность.

Для большинства мошенников характерен дар воображения и убеждения, позволяющий им чувствовать себя в любых ситуациях лидером. Для подавления воли потерпевшего нередко используют чисто внешние атрибуты, подтверждающие знакомство с влиятельными людьми, причастность к солидным предприятиям. Нередко с данной целью демонстрируют подложные документы, фотографии с элементами монтажа. Известны факты, когда для введения в заблуждение мошенники использовали свой природный дар убеждать людей под влиянием гипноза (таким методом часто пользуются цыгане при гадании).

Лица, которые занимаются мошенничеством с использованием платежных карт, достаточно четко отличаются от других преступников, так как им не свойственны такие черты характера, как импульсивность и агрессивность, как правило, они характеризуются стремлением к повышению социального статуса. Они имеют широкий кругозор, высокий интеллектуальный уровень, хорошую ориентацию в экономических и юридических вопросах. Анализ изучения уголовных дел показывает, что в

основном это мужчины. Среди лиц, совершивших преступление данной категории, $\frac{1}{2}$ часть - это люди в возрасте от 16 до 35 лет, $\frac{1}{4}$ часть составляют лица в возрасте от 35 лет до 50, и всего лишь $\frac{1}{8}$ часть – это возраст от 50 до 70 лет. Всего 10% составляют лица, имеющие высшее образование, остальная часть, т.е. 90% имеют среднее или средне специальное образование. Большинство из них – 90% нигде не работает. Следовательно, можно сделать вывод, что все они занимаются преступной деятельностью данного направления в качестве промысла.⁸

В правоприменительной практике встречаются следующие типы личности преступника исходя из способа совершения преступления:

1) обычная кража карты у ее держателя и дальнейшее ее использование в своих корыстных целях (покупка товаров, оплата услуг) или же находка платежной карты, которая принадлежит другому лицу, здесь необходимо отметить, что мошенничеством с использованием платежной карты будет в том случае, если при совершении преступления имел место обман уполномоченного работника кредитной, торговой и иной организации.

Таких преступников можно отнести к категории ситуативных, так как совершаемые ими преступления не являются квалифицированными, с точки зрения подготовки, оснащенности. Как правило, совершаются такие преступления, преступниками данной типологии, без соответствующей подготовки и использовании каких-либо сложных технических устройств. Чаще всего они делают это по внезапно возникшему умыслу или в силу стечения иных благоприятных для совершения хищения обстоятельств.

Так, например, в 2016 году Мурманский городской суд вынес приговор гражданину Н. который, имея умысел на хищение чужого имущества в свою пользу, достоверно зная, что на заднем сидении его автомобиля находится принадлежащая З. банковская карта на ее имя, воспользовавшись тем обстоятельством, что З. по невнимательности оставила вышеуказанную карту в его автомобиле, тайно похитил ее, с целью последующей покупки товара за

⁸ О.Г. Сумникова Криминалистическая характеристика мошенничества с использованием платежных карт// Журнал ОрЮИ МВД РФ «Наука и практика» №4(69) 2016г.

счет денежных средств находящихся на счету данной карты. продолжая свои преступные действия, направленные на хищение денежных средств со счета банковской карты, введя в заблуждение продавца-кассира, относительно правомерности нахождения у него банковской карты на имя З., выдав ее за свою, осознавая, что банковская карта и находящиеся на ней денежные средства ему не принадлежат, путем обмана похитил со счета вышеуказанной карты денежные средства в сумме 10 тысяч рублей, принадлежащие З. путем покупки товара, с которым скрылся с места преступления, распорядившись им впоследствии по своему усмотрению.⁹

2) Лица, которые в силу своего должностного положения, имеют доступ к информации, использование которой позволяет совершать мошенничества с использованием платежных карт.

Так в 2015 году районный суд города Новороссийска вынес приговор в отношении гражданки Ж., которая являясь сотрудником «ОАО Сбербанк России», воспользовалась своим служебным положением, и имея доступ анкетными данными гр. Ф незаконно заполнила заявление на получение кредитной карты и сопутствующие документы, выполнив подписи от имени Ф., после чего, незаконно получила кредитную карту, с кредитным лимитом в сумме 60 000 рублей. После чего, Ж., имея умысел на хищение денежных средств, обналичила в банкомате ОАО «Сбербанк России» с кредитной карты, оформленной на имя Ф денежные средства в сумме 50000 рублей, принадлежащие ОАО «Сбербанк России», которыми впоследствии распорядилась по своему усмотрению.¹⁰

3) Преступники, которые специализируются на совершении мошенничеств с использованием платежных карт и лица подготавливающие совершение таких преступлений, как правило такие преступники действуют в составе организованных групп. Такие лица являются квалифицированными

⁹Приговор Мурманского городского суда Мурманской области по делу № 2-378 от 15 апреля 2016 года\ \ Бюллетень Верховного суда РФ- 2016 № 7 -С. 351-354.

¹⁰Приговор Новороссийского городского суда Краснодарского края по делу № 4-765 от 20 февраля 2015 года\ \ Бюллетень Верховного суда РФ- 2016 № 6 -С. 454-457.

преступниками каждый из которых имеет «свою преступную специализацию», в таких группах четко распределены роли между соучастниками, сплоченность таких групп, как правила основана на корыстной направленности, финансовой составляющей. Совершенные преступления подобными группами, в большинстве случаев остаются не раскрытыми или же вообще остаются не известными правоохранительным органам, т.е являются латентными. Сюда же можно отнести и профессиональных специалистов, которые воспринимают меры безопасности, установленные на компьютере, в качестве вызова уровню своего профессионализма. Нередко они приобщаются к мошеннической деятельности, осознанно совмещая интеллектуальные и материальные стимулы своих преступных действий.

У организаторов подобных групп, как правило следующая характеристика: этот тип вероятного преступника не является квалифицированным ИТ специалистом и не имеет служебного положения, которым можно злоупотребить. С самого начала он планирует именно криминальное предприятие, отлично осознаёт его противозаконность. Решение совершить правонарушение именно в компьютерной (сетевой) среде, а не в «оффлайне» он принял не из-за своих особых знаний в этой области и не из-за внутренней тяги к компьютерам, а исключительно на основе рационального анализа. Он посчитал, что так будет выгоднее. «Выгода» компьютерного преступления обычно связана с его технической или организационной сложностью. На простые уловки попадаете мало жертв, от простых средств нападения большинство информационных систем давно защищены. Успешные компьютерные преступления отличаются технической сложностью, участием нескольких сообщников с «разделением труда», многоходовостью. Поэтому чертой личности таких преступников является наличие организаторских способностей и предпринимательской инициативы.

Указанному типу преступников отвечает большинство кардеров, спамеров и фишеров.

Применительно к мошенничеству с использованием платежных карт, личность преступника отличается следующими особыми характеристиками:

четко и профессионально формулирует задачу, однако отличается хаотическим бытовым поведением;

имеет весьма развитое формально-логическое мышление, однако именно оно нередко подводит его в реальной жизни;

старается говорить четко, точно и однозначно, регулярно переспрашивает, используя уточняющие вопросы и раздражая этим своего собеседника;

говорит преимущественно на компьютерном жаргоне, который малопонятен непрофессионалам.¹¹

Мошенничеством с использованием платежных карт может заниматься широкий круг лиц, среди которых встречаются специалисты высокой квалификации и просто дилетанты. Преступники могут отличаться разным уровнем образования и социальным статусом.

Таким образом, на основе материалов эмпирических исследований можно заключить, что возраст 33% злоумышленников на момент совершения преступления составляет от 14 до 20 лет; 54% – от 20 до 40 лет; 13% – старше 40 лет. Типовыми особенностями личности мошенников являются следующие: преимущественно мужской пол, возраст от 14 лет, при этом с каждым годом доля лиц от 20 до 40 лет возрастает. Как правило, это люди, имеющие профильное среднее и специальное образование и хорошие технические навыки, нередко ими движет в первую очередь азарт, а уже потом корыстный умысел, но чаще всего и то и другое одновременно. Они используют компьютерную терминологию, часто замкнуты, имеют малый круг общения, предпочитая виртуальный мир, считают себя гениями, пренебрежительно относятся к своим жертвам, ведут малоподвижный образ жизни, любят рисковать, обладают логическим мышлением, творческим подходом при решении поставленных задач, аналитическим складом ума, часто при наличии неопровержимых доказательств их вины начинают активно сотрудничать со следствием.

¹¹ Русаков И.М. Криминалистическая характеристика личности преступника, совершившего мошенничество в сфере предоставления интернет-услуг с. 206

§4. Криминалистически значимые данные о механизме следообразования

Основными источниками сведений о признаках мошенничества являются:

заявления физических лиц или представителей юридических лиц (например, банка или предприятия), потерпевших в результате мошеннических действий;

показания осведомленных лиц, круг которых изменяется в зависимости от конкретной следственной ситуации. К таковым, помимо потерпевших, можно отнести тех субъектов, которые вольно или невольно принимали участие в подготовке каких-либо документов, впоследствии использованных в мошенничестве;

В общей структуре преступности мошенничество не столь распространено, как кража, однако встречается достаточно часто. Так, в январе—декабре 2012 г. МВД РФ зарегистрировало 161 969 фактов мошенничества, из которых не раскрыто более 72 тысяч преступлений. При расследовании мошенничества, в зависимости от конкретной ситуации, следователь, а также сотрудники оперативно-розыскных подразделений, работающие в составе следственно-оперативной группы, обязаны установить и доказать следующие обстоятельства, которые отражены в ст. 159 УК РФ:

- факт хищения;
- факт, что противоправные действия осуществлялись по отношению к чужому имуществу или к правам на данное имущество;
- факт обмана;
- факт совершения мошенничества группой лиц по предварительному сговору;
- причинение потерпевшему значительного, крупного (более 300 тыс. руб.) ущерба или ущерба в особо крупном размере (более 1 млн. руб.);
- совершение данного деяния с использованием своего служебного положения;
- совершение мошенничества организованной группой.

Иными словами, следователь и оперативный работник, работающий в составе следственно-оперативной группы по расследованию факта конкретного мошенничества, обязаны знать, какие признаки элементного состава данного преступления они обязаны выявить, фиксировать, исследовать и доказать.

Следы мошенничества весьма разнообразны и зависят от конкретной ситуации. Для этого вида преступлений не характерны следы, оставляемые на месте происшествия. Нередко такого места просто не существует.

Так, при расследовании хищений, сопряженных с использованием реквизитов подлинных банковских карт, зарегистрированных на держателя карты с подключенной услугой «Мобильный банк», а также банковской карты с предоставлением ДБО к материальным следам, а также источникам получения информации по данным следам относятся:

- компьютер, с которого держатель карты постоянно или в последний раз— пользовался услугами Интернет-банкинга;

- компьютер (мобильный телефон), который использовался преступником— для использования ДБО с чужими паролями доступа;

- слипы с постоянным и разовыми паролями доступа к системе Интернет— банкинга;

- выписка по банковскому картсчету держателя карты, предоставленная банком; выписка по банковскому счету, который использовался для зачисления— похищенных с банковской карты денежных средств;

- анкета-заявление на получение банковских карт и договор банковского— обслуживания по счету, который использовался для зачисления денежных средств; выписка по банковскому счету, который использовался для дальнейшего— движения похищенных денежных средств;

- видеозапись с камеры наблюдения, установленной в месте обналичивания— денежных средств; следы пальцев рук на слипах, чеках, SIM-карте, мобильном телефоне;— банковская карта, используемая преступником для обналичивания— денежных средств;

- материальные ценности, приобретенные преступником с

использованием— банковской карты; схема, содержащая сведения о структурированной кабельной системе— здания (помещения) с указанием внешних подключений, выходящих за контролируемую зону; протоколы работы пользователей в сети Интернет с указанием— подключений, материалы проверки заявления держателя карты о несанкционированном списании денежных средств со счета банковской карты, проведенной службой безопасности банка;

-документы, подтверждающие использование лицензионного— программного обеспечения, а также использования лицензионных антивирусных программ; документ, регламентирующий политику информационной безопасности— юридического лица, содержащий сведения об ознакомлении конкретных сотрудников;

-к информационным системам, информации о входящем и исходящем— трафике конкретного IP-адреса, хранящиеся у интернет-провайдера или системного администратора;

-документы, содержащие сведения об IP-адресах, с которых происходила— авторизация с использованием похищенных учетных данных, хранящиеся в банках;

-видеозаписи с камер наблюдения, установленных в местах, где держатель— карты пользовался Интернет-банкингом (например, торговые центры, аэропорт и другие общественные места);

-черновые записи с паролями, используемые для доступа в ДБО;

-уставные и другие регистрационные документы юридического лица,

-реквизиты которого использовались для перевода похищенных денежных средств, документы могут быть предоставлены органами Федеральной налоговой службы;

-поддельные паспорта и иные документы, используемые преступником— для регистрации юридического лица и (или) открытия банковского счета на подставное лицо для последующего обналичивания похищенных денежных средств.

Следует иметь в виду, что важно быстро обнаружить и зафиксировать следы по данной категории дел, чтобы на первоначальном этапе расследования сразу выделить необходимые объекты-следоносители.¹²

При совершении мошенничеств с использованием платежных карт остаются идеальные следы, к носителям которых можно отнести:

- держателя карты,

- сотрудников банка, сотрудников службы безопасности банка или торгово-сервисной организации, так как при совершении данного преступления имеется визуальный контакт злоумышленника и работника кредитной, торговой и иной организации, а также возможен контакт с другими работниками таких организаций.

С учетом этого, к типичным идеальным следам указанного вида хищений можно отнести: сведения о внешнем виде, особенностях поведения лица, причастного к совершению хищения; сведения об общем количестве преступников; сведения о предмете хищения; сведения об обстоятельствах знакомства и взаимоотношений потерпевшего с преступником, отношениях после совершения преступления.

Подводя итог данному параграфу, мы можем сказать, что выявление следов преступления, как идеальных, так и материальных, и их качественное закрепление на первоначальном этапе расследования, ведет к успешному раскрытию и расследованию преступления.

Из всего вышесказанного в данной главе можно сделать вывод, о взаимообусловленной связи между обстановкой хищения и действиями субъекта преступления, поскольку место, время и другие факторы влияют на действия преступника и, в свою очередь, преступник отображает свои действия в обстановке в виде следов. Так, например, при совершении хищения в форме мошенничества с использованием поддельной банковской карты в торгово-сервисном предприятии преступник существенно ограничен в выборе

¹²Имаева Юлия Борисовна Особенности расследования хищений совершенных с использованием платежных карт Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность Диссертация на соискание ученой степени кандидата юридических наук. Уфа 2015 с. 3-229.

преступных действий порядком использования банковской карты при проведении банковских операций при оплате товаров, работ и услуг с использованием банковской карты. Анализируя указанные элементы криминалистической характеристики, мы можем резюмировать, что выбор способа хищения напрямую зависит от знаний преступниками правил банковских операций с использованием кредитных и расчетных карт, наличия специальных знаний в области изготовления банковских карт, занимаемой должности в кредитной организации. Нельзя не сказать о том, что лица, намеревающиеся длительное время совершать хищения в целях получения значительного дохода, тщательно готовятся к совершению преступления: изучают дополнительную литературу, компьютерные программы и т.д., и стараются оставить как можно меньше следов. И, напротив, более тривиальные способы совершения хищений выбирают преступники, не имеющие никакой профессиональной подготовки, а подготовка к совершению преступления занимает минимальное время непосредственно перед самим хищением, наличие судимости при совершении преступлений против собственности влияет лишь на выбор способов подготовки к хищению, а на выбор способа хищения влияния не оказывает.

ГЛАВА 2. АКТУАЛЬНЫЕ ПРОБЛЕМЫ (ВОПРОСЫ) РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ ПЛАТЕЖНЫХ КАРТ

§1. Особенности первоначального этапа расследования

В связи с динамичным ростом числа преступлений, совершаемых в целях хищения денежных средств с использованием высоких технологий в банковской сфере, был принят Федеральный закон от 08.06.2015 N 153, направленный на усиление уголовной ответственности за такие преступления. Ранее Федеральным законом от 27.06.2011 N 161-ФЗ "О национальной платежной системе" было введено определение электронного средства платежа, под которым понимаются средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверить и передавать распоряжения для осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств.

С 1 января 2014 года вступили в силу положения ст. 9 Закона N 161-ФЗ, согласно которым в случае совершения мошеннических операций с использованием электронных платежных средств ответственность за перевод денежных средств без согласия клиента несет оператор, если он не докажет нарушения правил использования электронного средства клиентом¹³.

Кроме того, с 16 марта 2015 года вступили в силу новые требования ЦБ России по борьбе с мошенничеством при дистанционном обслуживании граждан. Теперь банки обязаны блокировать рассылку служебных СМС (одноразовые пароли и пр.) при смене клиентом номера или сим-карты.

По заявлению клиента банк определяет параметры операций, которые могут осуществляться через интернет- и мобильный банкинг. В частности, банк устанавливает перечень устройств, с помощью которых может осуществляться

¹³ Сухаренко А. Скимминг вне закона // ЭЖ-Юрист. 2015. N 37. С. 3.

доступ к системам дистанционного банковского обслуживания (ДБО) в целях перевода денег на основе идентификаторов данных устройств. Наряду с этим банк устанавливает максимальную сумму перевода клиента через ДБО за одну операцию и (или) за определенный период времени (один день/один месяц). Указанные требования изложены в указании ЦБ N 3361-У, которое изменяет Положение регулятора 382-П.

О фактах совершения мошенничества с использованием банковских карт становится известно:

- 1) от держателей банковских карт
- 2) банков эмитентов
- 3) банков эквайеров
- 4) при задержании лица неправомерно использующего банковскую карту, которая ему не принадлежит или поддельная банковская карта
- 5) от представителей торгово-сервисных организаций
- 6) при расследовании других уголовных дел
- 7) в результате проведения оперативно-розыскных мероприятий или работы по делам оперативно учета.

При принятии заявления о совершении мошенничества, в рамках рассмотрения материала проверки сообщения о преступлении необходимо как можно быстрее произвести следующие процессуальные действия:

- детальное и подробное объяснение заявителя, держателя карты, задержанного лица (если таковое имеется), сотрудников банка, кредитных, торговых организаций, которые имели визуальный контакт со злоумышленником.

- изъятие записей с камер видеонаблюдения в местах использования злоумышленником карты, а также в местах подхода и отхода к данной точке (как правило необходимо производить немедленно при установлении места совершения преступления, так как запись в большинстве случаев хранится не более 60 дней)

- осмотр места где произошло незаконное использование банковской карты.

- запросы в банки, торгово-сервисные организации, с целью получения сведений о движении денежных средств.

Актуальной проблемой при расследовании таких видов мошенничеств, как правило, является значительный разрыв во времени между совершением уже оконченного преступления и обращением в правоохранительные органы пострадавшего лица, а это как правило ведет к утрате следов преступления, в информационной среде, а также материальных следов.

Это связано с тем, что многие мелкие случаи просто не доходят до правоохранительных органов. Наибольшее количество преступлений связаны со средним или незначительным ущербом для держателя карты. Банки в таких случаях стремятся самостоятельно разбираться в таких ситуациях. В некоторых случаях, банк в ходе собственного расследования может установить вину клиента в перечислении этих средств и они ему не возвращаются. Банку необходимо доказать, что клиент самостоятельно допустил ошибку при использовании карты, либо что клиент сам заведомо решил обмануть банк. Если же банком будет установлено, что вины клиента в несанкционированном списании средств нет, организуется поиск банка-получателя денег пострадавшего. Если банк не находит получателя, то возмещает утраченные средства.

В то же время и клиенты, столкнувшись с мошенничеством, предпочитают напрямую идти в банк и требовать возмещения убытка. Ведь согласно поправкам к закону «О национальной платежной системе» 2014 года у банка существует обязанность возвращать денежные средства клиенту, который заявил о несанкционированном списании средств с его личной платежной карты, а уже после проводить свое собственное расследование того, по чьей вине это произошло. Тем не менее, согласно закону, гражданин обязан уведомить банк «незамедлительно после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции». Банк же должен после транзакции уведомить клиента о совершенной операции «не

позднее дня, следующего за днем исполнения». После этого банк «обязан возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента – физического лица» (п. 15 ст. 9 закона). На рассмотрение заявления клиента о мошенническом списании банку дается 30 дней, но о сроках выплаты возмещения, к сожалению, ничего не сказано. Интересно также то, что, если банк не уведомил клиента о мошеннических действиях в отношении него, то он обязан возместить всю списанную сумму без каких либо разбирательств.

Данные условия закона «О национальной платежной системе» помогают регулировать конфликтные ситуации между банком и держателем платежной карты без вмешательства правоохранительных органов. Таким образом многие преступные по своей сути действия с использованием платежных карт могут остаться латентными.

Поводя итог данному параграфу, необходимо отметить, что на этапе возбуждения уголовного дела, при рассмотрении материала проверки сообщения о преступлении, необходимо как можно оперативно, полно, детально и качественно проводить все необходимые процессуальные, следственные действия, а также оперативно-розыскные мероприятия.

§2. Организационно-тактические особенности производства следственных действий (ОМП, допрос и др.)

На предварительной стадии расследования, при получении заявления о совершенном преступлении, и дальнейшем возбуждении уголовного дела, при допросе потерпевшего необходимо выяснить следующие обстоятельства: где в настоящее время находится карта, позволял ли он кому-либо ею пользоваться, если да, то кому именно и при каких обстоятельствах. Встречаются ситуации, когда заявитель и лицо, которое он подозревает, знакомы, следовательно уже на стадии возбуждения уголовного дела может предположить, что заподозренное заявителем лицо вряд ли будет отрицать факт получения денег по чужой

банковской карте, а факт присвоения денег объяснит другим способом.

В ходе допроса потерпевшего детально выяснить: обстоятельства знакомства с заподозренным им лицом; длительность знакомства; использовало ли ранее заподозренное лицо карту потерпевшего и при каких обстоятельствах; имеются ли у потерпевшего перед заподозренным им лицом какие-либо финансовые обязательства, как они оформлены, кто может подтвердить факт наличия или отсутствия финансовых обязательств; замечал ли ранее случаи хищения денежных средств; где обычно хранится карта; как узнал, что с банковской карты похищены денежные средства; кого сразу заподозрил и почему; разговаривал ли потерпевший с заподозренным лицом по поводу пропажи денежных средств и что последний при этом пояснил; кто присутствовал при этом разговоре; сколько денег похищено и каким образом, по мнению потерпевшего, лицо, которое он подозревает, мог ими распорядиться, не нуждался ли тот в деньгах. Здесь же можно выяснить, пользовался ли кто-либо банковской картой после хищения денег и в противном случае возможно изъятие карты для последующего дактилоскопического исследования. В некоторых случаях потерпевшие, еще до обращения с заявлением в правоохранительные органы самостоятельно обращаются в службу безопасности банка в целях просмотра результатов камер видеонаблюдения, установленных в банкомате, и имеют при себе фотографии с камер наблюдения. Данное обстоятельство также необходимо выяснить при допросе потерпевшего, при этом следует задать вопрос о том, узнал ли потерпевший кого-либо на данной фотографии и предъявлял ли ее как доказательство этому лицу.¹⁴

Также в ходе допроса необходимо получить ответы на следующие вопросы:

- как давно пользуется банковской картой; какая сумма находится на счету; где хранится; кто еще пользуется данной картой; кто имеет доступ к ней.
- как часто он рассчитывается данной картой при совершении покупок

¹⁴Филиппов А.Г. Особенности расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов: монография / М Филиппов М : Юрлитинформ, 2014.

или после оказания ему необходимых услуг этой картой; посещал ли он в последнее время какие-либо рестораны, кафе, совершал ли покупки в интернет магазинах.

- производился ли расчет в его присутствии, или сотрудники этих заведений уносили их в другое место. Было ли замечено что-либо подозрительное при расчете.

- когда у него со счета была списана определенная сумма денег, либо время обнаружения пропажи, подключена ли к его телефону услуга «Мобильный банк», приходили ли ему сообщения о снятии денежных средств.

- куда и когда обращался для блокирования счета и возврата списанных денег.

Действующее уголовно-процессуальное законодательство достаточно подробно регламентирует порядок проведения допроса потерпевшего и свидетеля. Данный результат мы можем объяснить только тем, что допрос, являясь самым распространенным следственным действием, определяет наличие стабильных практических навыков в его проведении, тогда как особенности сложившейся следственной ситуации следователями совершенно не учитываются, и меры к преодолению имеющегося или будущего противодействия не принимаются. Принять меры по противодействию расследованию, выразившемуся в уничтожении предметов и документов, а также предметов и ценностей, добытых преступным путем, возможно уже в ходе первоначального допроса подозреваемого. Однако, как опять показывает анализ судебно-следственной практики, допросы проводятся поверхностно, причем допросы подозреваемого и обвиняемого полностью дублируют друг друга, и указанное выше обстоятельство не устанавливается.

В протоколах допросов лишь указано, что «потратил на личные нужды», но как именно, в ходе следствия не установлено. Выяснение данного обстоятельства могло бы расширить круг свидетелей и помочь обнаружить товарно-материальные ценности, приобретенные с использованием похищенной банковской карты, и таким образом хотя бы частично решить вопрос о возмещении материального ущерба. Довольно распространено

противодействие расследованию в виде утаивания и дачи ложных показаний.

Отечественная наука многие десятилетия разрабатывает различные тактические приемы изобличения ложных показаний, однако следует отметить, что факты дачи ложных показаний не уменьшаются. Типичные мотивы ложных показаний довольно разнообразны, все зависит от категории преступления, личности преступника и сложившейся следственной ситуации. Исходя из судебно-следственной практики следует что, чаще всего подозреваемые (обвиняемые) в совершении хищений с использованием кредитных и расчетных карт дают ложные показания о следующих обстоятельствах совершенного преступления: о факте причастности к использованию карты или поддельной карты (приобретению каких-либо предметов), либо о мотивах получения денежных средств с использованием банковской карты другого лица. В первом случае подозреваемый (обвиняемый) отрицает саму причастность к получению каких-либо денег или материальных ценностей по чужой банковской картенередко в данном случае подозреваемый (обвиняемый), как уже отмечалось, привлекает для снятия денег в банкомате другое лицо или маскирует свою внешность, сознавая, что снятие денежных средств фиксируется с помощью средств фото или видеофиксации.¹⁵

В ряде случаев данная ситуация осложняется еще и тем, что подозреваемый (обвиняемый) после совершения хищения возвращает карту на место, т.е сама банковская карта к моменту обнаружения хищения и подачи заявления в правоохранительные органы находится у держателя карты. Так, Кулешов А. А., находясь в жилище бывшей жены, заведомо зная о местонахождении принадлежащей ей банковской карты, нашел ее, после чего в банкомате получил денежные средства. После совершенного преступления Кулешов А. А. вернулся в квартиру бывшей жены и положил карту на место. Будучи допрошенным в качестве подозреваемого Кулешов А. А. отрицал факт незаконного изъятия денежных средств, пояснив, что использовал банковскую карту с согласия бывшей супруги, т. к. та ранее занимала у него деньги и

¹⁵Протосевич А. А. , Зверьянская Л. П. Криминалистическая характеристика компьютерных преступлений // Российский следователь – 3 – № – С 45-47

решила таким образом рассчитаться. После получения «долга» банковская карта была им сразу возвращена К-вой З. Т. Данное противодействие было преодолено в результате успешно примененных тактических приемов при повторном допросе подозреваемого. Второй случай, по нашему мнению, более сложный в плане дальнейшего изобличения ложных показаний, т. к. подозреваемый (обвиняемый) не отрицает факта получения денег, например в банкомате, по чужой банковской карте, однако объясняет это тем, что потерпевший сам отдал карту для получения денежных средств, впоследствии полученные денежные средства не присваивались, а были возвращены держателю карты или оставлены себе с согласия потерпевшего в счет исполнения каких-либо обязательств, например возврата долга. Характерный пример. Козлова Л. В., зная что ее знакомая Ч-на Н. А. получает пособие на малолетнего ребенка, которое перечислялось на сберегательную книжку, посоветовала последней оформить банковскую карту, на которую перечислялись бы указанные выплаты. При этом Козлова Л. В. предложила Ч-ной Н. А. передать банковскую карту ей, чтобы родители потерпевшей, злоупотребляющие спиртными напитками, не смогли настаивать на передаче им находящихся на карте денежных средств для приобретения спиртного. В свою очередь, Козлова Л. В. обещала Ч-ной Н. А. покупать и привозить ей все необходимое по выгодным ценам. После получения от Ч-ной Н. А. банковской карты и PIN-кода Козлова Л. В., злоупотребляя доверием потерпевшей, ежемесячно получала принадлежащие Ч-ной Н. А. денежные средства, однако самой потерпевшей ничего не передавала, всего похитив, таким образом, денежные средства на общую сумму 55488 рублей. На неоднократные требования потерпевшей вернуть ей карту, Козлова Л. В. находила различные отговорки или отвечала отказом. В ходе следствия Козлова Л. В. виновной себя в предъявленном обвинении не признала и пояснила, что потерпевшая сама передала ей банковскую карту, потому что ее родители злоупотребляют спиртными напитками. При этом разрешила пользоваться денежными средствами, а также привозить ей продукты и вещи для детей, что она и делала. Следователем был допрошен ряд свидетелей, в т. ч. сестра и отец потерпевшей,

которые пояснили, что неоднократно были свидетелями того как Ч-на Н. А. разговаривала по телефону с Козловой Л. В. и требовала вернуть карту. Сестра потерпевшей пояснила, что как только Козлова Л. В. узнала о том, что Ч-на Н. А. обратилась в правоохранительные органы, то сразу пообещала вернуть все денежные средства. В дальнейшем данные показания были положены в основу обвинения.

В обоих случаях следователю необходимо тщательно готовиться к допросу, а именно: изучить материалы уголовного дела, в частности заявление и показания– потерпевшего об обстоятельствах обнаружения пропажи карты и (или) денежных средств с банковской карты; изучить личность лица, которого потерпевший или правоохранительные органы подозревают в совершении хищения.

Как показывает судебно-следственная практика, в половине случаев потерпевший и подозреваемый (обвиняемый) были знакомы или даже являются родственниками. В данном случае необходимо до допроса установить характер отношений между этими лицами, выявить факты неприязненных отношений, наличие денежных обязательств и.т.д ; к моменту первого допроса подозреваемого иметь в материалах– уголовного дела фотографии лица, запечатленного в момент снятия денежных средств в банкомате или покупки в магазине; иметь другие доказательства (допросы свидетелей, результаты осмотра, выемки и т д), которые можно будет предъявить при допросе; составить плана допроса.

К сожалению, имеющиеся методические рекомендации по подготовке к допросу следователями выполняются крайне редко, а при расследовании это выражается в низкой результативности допроса как следственного действия, т.к следователь в связи с игнорированием подготовительного этапа допроса не может использовать какие-либо тактические приемы для изобличения ложных показаний. В данном случае мы не говорим о таком тактическом приеме, как «допущение легенды», когда допрашиваемому предоставляется возможность беспрепятственно излагать придуманные им объяснения фактов, а у следателя нет возможности противостоять ложным показаниям

допрашиваемого, в практике это ведет к дополнительным допросам потерпевших, неоднократным дополнительным допросам самих подозреваемых (обвиняемых) и, как следствие, продлению сроков предварительного следствия.

Таким образом сотрудникам следственных и оперативных подразделений(в случае производства допроса по поручению следователя), необходимо всегда быть готовым к противодействию со стороны подозреваемых (обвиняемых), а также придерживаться имеющихся криминалистических рекомендаций в части подготовки к допросу. В ходе самого допроса, если следователь столкнулся с конфликтной ситуацией, противодействием со стороны допрашиваемого (подозреваемого, обвиняемого) и его защитника, применительно к рассматриваемой категории уголовных дел, рекомендуется использовать следующие тактические приемы:

«Допущение легенды». Данный прием рекомендуем использовать при расследовании мошенничеств, совершенных с участием сотрудников банковских учреждений, а также мошенничества с использованием поддельных карт. Это обусловлено тем, что расследование данных видов хищений, как правило, длительное, связано с изъятием большого количества материальных объектов-носителей следов преступлений, которые можно будет использовать при последующих допросах, чтобы подчеркнуть противоречие показаний по материалам уголовного дела.

«Проговорка» рекомендуется использовать при расследовании хищений— в случаях знакомства подозреваемого и потерпевшего, а также мошенничеств с использованием поддельных банковских карт в составе группы лиц. В данном случае, применяя увеличение темпа допроса и плавный переход к выяснению других обстоятельств, можно добиться от допрашиваемого «проговора» об обстоятельствах преступления, известных только лицу, его совершившему.

«Создание заполненности» выражается в выделении следователем невыясненных мест для того, чтобы у допрашиваемого самого возникло желание заполнить эти пробелы информацией;создание условий, при которых у

допрашиваемого создается мнение, что следствие располагает всем объемом доказательств по данному делу, чего можно достичь постепенным предъявлением проверенных доказательств, предъявлением главного доказательства, постановкой вопросов о второстепенных деталях и т.д.; предъявление материалов дела, в частности распечатанных фотографий, записи с камер видеонаблюдения. В данном случае необходимо быть крайне осторожным и предъявлять фотографии только хорошего качества, будучи полностью уверенным, что на фото изображен именно подозреваемый (обвиняемый). Последнее обстоятельство должно быть подтверждено другими материалами дела, которые также должны быть готовы для предъявления допрашиваемому лицу. В противном случае может возникнуть ситуация, когда подозреваемый (обвиняемый) в ходе допроса может заявить, что на фото изображено другое лицо, лишь некоторым образом на него похожее, а следователь не сможет опровергнуть данное высказывание. Впоследствии у подозреваемого возникнет убежденность в отсутствии у следователя доказательств, что еще больше укрепит его уверенность в дальнейшем отрицании вины и даче ложных показаний; Демонстрация допрашиваемому научно-технических возможностей следствия, в частности, возможностей судебной экспертизы, также можно использовать при определенных условиях, что может дать желаемый результат.

Указанные тактические приемы одинаково подойдут как к первому случаю дачи ложных показаний, так и ко второму, когда подозреваемый не отрицает факта получения денег по чужой банковской карте. Однако в последнем случае следователю необходимо быть более подготовленным и еще до допроса провести ряд мероприятий, которые помогут преодолеть противодействие при допросе.

Также не менее распространенное, в следственной практике это производство осмотра. Осмотр места происшествия позволяет решить следователю ряд задач: кто принимал участие в совершении преступления, как долго лица находились на месте преступления, какие технические средства и документы использовали преступники, где могли находиться возможные

очевидцы хищения, что могло способствовать совершению преступления (например, халатные действия кассира) и т.д. Как и любое следственное действие, осмотр места происшествия осуществляется в три этапа: подготовительный, рабочий и заключительный, из которых, на подготовительном этапе осмотра необходимо вызвать соответствующего специалиста, который может решить вопросы о необходимости изъятия того или иного оборудования, сообщить следователю о том, какие именно технические средства могут нести значимую для расследования информацию, целесообразности использования соответствующей техники и особенностях упаковки изъятых. В качестве специалистов, в зависимости от ситуации, рекомендуется приглашать сотрудников технического отдела банка, установившего банкомат и осуществляющего его обслуживание; специалиста-криминалиста, который будет работать с традиционными следами преступления (следами рук и ног); специалиста, который будет осуществлять фото- и видеосъемку.¹⁶

При расследовании мошенничеств с использованием кредитных и расчетных карт во всех случаях необходимо производить осмотр места происшествия, в случае если имеются сведения о месте получения денежных средств. При этом осмотр места хищения денежных средств должен носить поисковую направленность, а не носить лишь информативный характер о месте расположения окружающих объектов. При производстве осмотра необходимо осмотреть пути подхода и отхода злоумышленника к месту и от места совершения преступления. Также при производстве осмотра необходимо обращать внимание на изъятие видеозаписи с камер наружного видеонаблюдения так, как при совершении мошенничества с использованием платежных карт, так как совершение таких мошенничеств, как правило совершается на каких-либо торговых точках, а также в банковских и кредитных учреждениях, где в большинстве случаев вышеуказанные помещения

¹⁶Имаева Юлия Борисовна Особенности расследования хищений совершенных с использованием платежных карт Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность Диссертация на соискание ученой степени кандидата юридических наук. Уфа 2015 с. 3-229.

оснащены камерами видеонаблюдения. В дальнейшем данная видеозапись, изъятая в ходе ОМП, должна быть осмотрена в соответствующем уголовно-процессуальном порядке. Как правило, осмотр видеозаписи происходит по месту проведения следственного действия, т.к. при обнаружении и изъятии это сделать затруднительно, а порой и невозможно в связи с отсутствием на месте необходимого оборудования. Однако, как и любой следственный осмотр, осмотр видеофонограммы необходимо проводить незамедлительно, как только появилась возможность. Просмотр и прослушивание видеофонограммы производится следователем в присутствии понятых и с привлечением специалиста, который будет использовать для просмотра необходимую аппаратуру. В протоколе осмотра видеофонограммы необходимо указать: условия освещения, наличие изоляции посторонних шумов;— технические средства, которые использовались при просмотре видеозаписи— (в т.ч. марка монитора и наименование программы); результаты внешнего осмотра упаковки: вид упаковки, наличие подписей понятых и пояснительной записи, с указанием времени и места изъятия (например, видеозапись камер наблюдения, установленных в торговом зале магазина «...», расположенного по адресу: ...); наличие видимых повреждений упаковки; объекты, обнаруженные в упаковке, их внешний вид, наименование,— серийный номер диска, наличие видимых повреждений; результаты осмотра с использованием технических средств информации,— хранящийся на диске: наличие файлов, их количество, наименование, формат, даты создания, даты изменения, объем хранящейся информации; результаты осмотра каждого файла: что запечатлено, наличие в кадре каких-либо людей, их действия, какие действия проводятся, с каких слов начинается и заканчивается речь, как заканчивается видеозапись, общее время записи каждого файла; каким образом материальный носитель видеоинформации был упакован— и опечатан в присутствии понятых; производилась ли по ходу просмотра распечатка стоп-кадров, на какой— секунде просмотра и что запечатлено, с использованием какого печатающего устройства производилась распечатка; содержание

видеозаписи или фонограммы в той части, которая относится— к делу. Содержание видеофонограммы также может быть записано (по возможности дословно) в протоколе осмотра. Результаты внешнего осмотра, просмотра и прослушивания видеофонограмм необходимо фиксировать в едином процессуальном документе-протоколе, к которому прилагаются распечатанные стоп-кадры, также заверенные подписями понятых и следователя. Как показало изучение уголовных дел, осмотр видеозаписи проводится весьма поверхностно, и зачастую уже после установления личности преступника; содержание осмотра не несет никакой криминалистически значимой информации и нередко изобилует сделанными следователем выводами и предположениями, «выгодными» следствию, что нарушает объективность расследования.

Производство осмотра также необходимо, когда подозреваемый в совершении мошенничества, дает показания о месте и способе уничтожения карты, в данном случае необходимо установить местонахождение карты, с последующим её изъятием.

Зачастую к осмотру места происшествия даже не прилагается таблица фотоиллюстраций или схема места происшествия, что впоследствии при допросе и проверке показаний на месте могло бы иметь существенное значение.

«При производстве осмотра места происшествия целесообразно использовать тактический прием «От центра – к периферии».

Одним из основополагающих условий качественного расследования хищений с использованием кредитных и расчетных карт является своевременный выезд СОГ на место происшествия. В случае промедления данное следственное действие может быть малоинформативным или даже совсем бесполезным с точки зрения криминалистики, и, как следствие, безуспешным для дальнейшего преодоления противодействия расследованию.

После решения задач общего осмотра следователю предстоит наиболее сложная стадия – детальный осмотр, вызывающий большие затруднения на практике. Зачастую, в случае отсутствия явных следов преступления, данная стадия сводится только к описанию вида терминала, какие-либо поисковые

действия проводятся нединамично или не проводятся вообще, а следовательно ограничивается фразой: «В ходе осмотра ничего не обнаружено и не изъято». Однако следователь вправе проводить любые манипуляции с корпусом терминала, в том числе с участием специалиста вскрывать корпус терминала а данной стадии необходимо предпринять наиболее активные поисковые мероприятия в целях обнаружения следов преступления: следы рук, ног преступника (преступников); следы орудий и материалов; следы проникновения в корпус терминала; следы крепления сторонних технических устройств или наличия сторонних прикрепленных предметов; машинограммы – документы, подтверждающие проведение операции (например, слип, контрольная лента); документы, которые преступник использовал для совершения хищения (документы, удостоверяющие личность, сама банковская карта); вещи, оброненные преступником.

Как правило, при первичном осмотре следователь не принимает меры к своевременному изъятию документов из автоматизированных охранных систем наблюдения. Зачастую это обусловлено отсутствием необходимого специалиста при осмотре или отсутствием представителя банка, которому принадлежит терминал. Впоследствии изъятие системы наблюдения проводится по прошествии времени в ходе выемки, что может привести к утрате записи, затягиванию следствия и другим негативным последствиям. Осмотр предметов и документов зафиксирован в материалах 97,5 %1 изученных нами дел, а каждый четвертый респондент отметил, что проведение данного следственного действия вызывает затруднение (чаще других трудности вызывает осмотр документов на машинном носителе, электронного терминала и видеозаписи). При этом мы можем отметить, что в 34,76 % уголовных дел после изъятия записи с камер наружного или скрытого внутреннего видеонаблюдения банкомата ее осмотр вообще не производился. При первоначальном осмотре карты необходимо иметь в виду, что на ней могут сохраниться следы преступника, поэтому необходимо соблюдать традиционные криминалистические правила обращения со следами. При обнаружении и изъятии документа на машинном носителе или машинограммы

необходимо помнить, что в распоряжении следствия должен оказаться подлинник документа, т.к именно он впоследствии будет являться объектом криминалистических исследований «Поэтому в случае нежелания Подлинником документа на машинном носителе является первая по времени запись документа на машинном носителе и содержащая указание, что этот документ является подлинником (руководителя организации, участвующей в операционной работе, выдать подлинник документа, следовательно необходимо проявить настойчивость и добиться предоставления подлинников, а взамен – оставить копии осмотренных и изъятых машинограмм с копией протокола следственного действия». При осмотре документов необходимо учитывать их назначение, состояние, объем содержащейся в ней информации, взаимосвязь с иными доказательствами, собранными по делу невзирая на довольно широкое освещение в криминалистической литературе общих положений осмотра документов как вида следственного осмотра, документы по данной категории дел остаются недостаточно исследованы. Разработка данного вопроса необходима, по нашему мнению, еще и потому, что после изучения уголовных дел можно констатировать недооценку следователем документов, которые могут нести доказательственную информацию, что также обусловлено недостаточным знанием следователем признаков, содержащихся в документе, и могущих иметь информационное значение для раскрытия и расследования преступлений и преодоления возможного противодействия. Среди трудностей, которые следователи испытывают при осмотре документов, согласно анкетированию, названы: невладение методикой анализа содержания документов, недостаточное знание документооборота, незнание признаков, которые могут указать на факты возможных хищений. Исследование указанного вопроса необходимо потому, что при изучении уголовных дел было нами отмечено, что следователи недооценивают документы, которые могут указать на преступление. К основным целям осмотра документа, которые необходимо знать следователю при проведении осмотра, относятся: проверка действительности документа, выявление признаков подделки документа, выявление признаков интеллектуального подлога, обнаружение следов,

оставленных преступником на документе. В связи с изложенным, а также в целях сохранения следов на документе, документ при осмотре рекомендуется хранить в прозрачной упаковке (пакете) для проведения дальнейших криминалистических исследований, также нельзя делать пометки, скреплять клеем к подложке, делать дополнительные перегибы. В случае необходимости для ежедневной работы рекомендуется осматриваемый объект сфотографировать или сделать электрографическую копию, которую можно приобщить к материалам уголовного дела без боязни испортить документ. При осмотре уже изъятых и приобщенных к уголовному делу слипов нами установлено, что часть из них непригодна для восприятия, т е по причине выцветания (перегибания, загрязнения) является нечитаемой. Чтобы предотвратить это, необходимо соблюдать соответствующие криминалистические рекомендации по хранению документов.¹⁷

Осмотр электронного терминала. «Электронный терминал является, во-первых, техническим устройством, в котором находятся электронные документы и их бумажные копии – машинограммы (на контрольной ленте), имеющие значение для уголовного дела, во-вторых, средством (орудием) совершения преступления». Применительно к рассматриваемому преступлению электронным терминалом являются контрольно-кассовые машины, банкомат, мобильный телефон. Если первоначальный осмотр электронного терминала производится в ходе осмотра места происшествия, то рекомендуется обратиться за помощью к специалисту, знакомому с правилами работы с данным следоносителем, а именно: оператору терминала, инженеру-программисту. Как показали результаты изучения уголовных дел, осмотр электронного терминала проводился в ,4 % случаев в рамках осмотра места происшествия. Однако даже этот осмотр содержит лишь описание принадлежности терминала к тому или иному банку и его номер. Данная информация нам представляется недостаточной. При осмотре самого терминала следует обращать внимание и фиксировать в протоколе осмотра:

¹⁷Коновалов С.И Соболев А.В К вопросу о совершенствовании процессуального положения специалиста как участник уголовного судопроизводства // Известия Тульского государственного университета Экономические и юридические науки Выпуск Ч.II С.6-33

местонахождение объекта осмотра (если терминал находится в здании, то также указать адрес помещения); направления подхода и отхода к объекту осмотра, в т ч наличие дорог, парковок, автостоянок и т д ; внешнее состояние объекта осмотра; расположение объекта относительно средств видеонаблюдения; тип, марку, конфигурацию, цвет, заводской и (или) инвентарный номер терминала, состояние терминала и его периферийных устройств на момент проведения осмотра; вид изображения на дисплее (мониторе) на момент осмотра; наличие на путях отхода, подхода или самом объекте следов преступления и преступника; внешний вид, наличие и работоспособность отдельных узлов, наличие не присущих данному терминалу деталей (проверку необходимо поручить специалисту); «Стоит обратить особое внимание на то, что перед началом производства любых следственных действий, непосредственно связанных со средствами электронно-вычислительной техники, средствами системами их защиты, необходимо в обязательном порядке получать и анализировать с участием специалистов информацию о технологических особенностях функционирования вышеприведенных технических устройств, уровня их соподчиненности и используемых средств связи и телекоммуникации. Это позволит избежать их разрушения, нарушения заданного технологического ритма и режима функционирования, причинения крупного материального ущерба собственникам, владельцам или пользователям, а также уничтожения вещественных доказательств».

Далее обратим внимание на производство такого следственного действия как обыск. Чаще всего при обыске по делам о мошенничестве, совершенных с использованием кредитных и расчетных карт, в зависимости от способа хищения, искомым объектом могут быть: банковские карты, заготовки банковских карт, оборудование для их изготовления, товары, приобретенные с использованием банковской карты, товарные и кассовые чеки на приобретенные товары, средства электронно-вычислительной техники, черновые записи, слипы, квитанции из банкоматов, поддельные и чужие документы, удостоверяющие личность, мобильные телефоны, SIM-карты,

компьютерная техника, различные устройства типа «скиммеры», микрокамеры, кард-ридеры, а также различные информационные носители и технические устройства. Необходимо обращать внимание на средства маскировки внешности, которые использовались при совершении мошенничеств, например, накладные усы или борода, головные уборы и т. д. Тактике обыска в помещениях в криминалистической литературе уделено достаточно внимания. Следует остановиться на основных тактических особенностях проведения обыска по данной категории дел, которые, на наш взгляд, имеют важное значение для успешного расследования рассматриваемого вида хищений. Так, еще на подготовительном этапе обыска следователю необходимо взаимодействовать с сотрудниками оперативных подразделений, которые должны к этому моменту обладать максимальной информацией о местах возможного нахождения и сокрытия искомых предметов. Как правило, ввиду небольшого размера банковской пластиковой карты или SIM-карты, их легко спрятать, поэтому детальная стадия обыска представляется наиболее трудоемкой. При обнаружении каких-либо банковских карт или заготовок к банковским картам в протоколе необходимо отразить некоторые индивидуальные признаки: цвет, номер, фамилию и имя держателя карты. При обнаружении оборудования для изготовления пластиковых карт необходимо обратиться за помощью к специалисту, чтобы изъять оборудование полностью, принять меры к недостающим составляющим и т. д. С обнаруженными документами (слипами, чеками, поддельными документами, удостоверяющими личность) необходимо обращаться бережно, принимать меры к сохранности имеющихся следов пальцев рук на документах. При обнаружении предметов, похожих на приобретенные в торговых организациях по поддельной или похищенной карте, необходимо принять меры к обнаружению ярлыков, товарных и кассовых чеков к этим предметам. Стоит отметить о процессе фиксации и изъятии, вышеуказанных предметов и документов, так как на данных объектах носителях остается важная доказательственная информация, которую необходимо сохранить, с целью проведения дальнейших экспертиз по данным объектам, таким образом, цифровые объекты, там где содержится

электронная (цифровая) информация, необходимо изымать с участием специалиста, в данной области, в случае обнаружения традиционных следов, например, следов пальцев рук, и т.д., данные объекты изымаются специалистом-криминалистом.

Крайне отрицательную результативность обыска можно объяснить только несвоевременностью его проведения, обыск не является первоначальным следственным действием, а проводится уже ближе к окончанию расследования после неоднократных допросов подозреваемых и обвиняемых, находящихся под подпиской о невыезде. Таким образом, сотрудники следственных подразделений вопреки теоретическим положениям и существующим практическим рекомендациям по планированию расследования, не принимают соответствующих мер по поиску орудий и предметов преступления, а также предметов и ценностей, добытых преступным путем а наш взгляд, это не только не противостоит имеющемуся противодействию, но и противоречит полноте расследования.

Зачастую, особенно при задержании преступника с поличным, времени для подготовки обыска недостаточно и он может проводиться в порядке статьи 165 УПК РФ в рамках тактической комбинации. Однако следователи указанным положением уголовно-процессуального закона не пользуются, чем предоставляют подозреваемому (обвиняемому) и (или) его близким реальную возможность для уничтожения орудий преступления, предметов, добытых преступным путем. Совершенно справедлива рекомендация В.Б Вехова: «Если из исходной криминалистически значимой информации усматривается, что преступление было совершено группой лиц, целесообразней всего разработать тактическую операцию по одновременному проведению ряда обысков и выемок в нескольких заранее определенных местах. При этом следователь должен проводить следственное действие на наиболее сложном и перспективном в информативном отношении месте, а сотрудники органов дознания – в иных местах». На подготовительном этапе обыска следователю, помимо всего прочего, необходимо наиболее достоверно установить способ хищения и предмет хищения, чтобы обыск был наиболее эффективным.

Таким образом, обыск, наряду со следственным осмотром, является довольно результативным и наиболее продуктивным следственным действием, которое необходимо для успешного расследования уголовного дела.

Предъявление подозреваемого для опознания мы также можем отнести к первоначальным следственным действиям, которые способствуют нейтрализации противодействия. Следователь еще при планировании расследования может выявить лиц, которые впоследствии смогут опознать лицо, совершившее хищение. Как правило, это кассиры или продавцы, которые общались с предъявителем чужой карты, а также лица. В таком случае опознание должно проводиться сразу после допроса подозреваемого, независимо от того, признал он вину или нет, т.к, последний впоследствии может отказаться от своих показаний, заявив, что хищения не совершал. Так же мы рекомендуем при наличии нескольких свидетелей, которые могут опознать подозреваемого, проводить ряд опознаний без какого-либо разрыва во времени. Таким образом будет достигнуто необходимое воздействие на подозреваемого. Также производство опознание возможно в тех случаях, когда мошенничество было совершено в соучастии и при расследовании один из соучастников отрицает факт знакомства, а также совместную преступной деятельности, проведение такого следственного действия может снизить противодействие расследованию.¹⁸

Также необходимо в данной главе уделить внимание взаимодействию органов предварительного следствия и оперативных подразделений.

При расследовании каждого уголовного дела, возбужденного по факту мошенничества использованием кредитных и расчетных карт, следователи сталкиваются с противодействием расследованию, противостоять которому не готовы и, как следствие, не принимают достаточных мер к его преодолению. Знание типичных следственных ситуаций может помочь следователю прогнозировать характерные способы противодействия расследованию.

¹⁸Имаева Юлия Борисовна Особенности расследования хищений совершенных с использованием платежных карт Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность Диссертация на соискание ученой степени кандидата юридических наук. Уфа 2015 с. 3-229.

Основной причиной, по которой следователи не принимают мер к преодолению противодействия, является неиспользование криминалистических рекомендаций по проведению следственных действий, а также уголовно-процессуального закона и других нормативно-правовых актов, регламентирующих деятельность правоохранительных органов.

§3. Использование специальных познаний при расследовании мошенничеств с использованием платежных карт

Сфера использования кредитных и расчетных карт, с точки зрения технических решений, пожалуй, одна из самых сложных и наукоемких сфер расследования. Как свидетельствует практика, в ходе расследования мошенничеств с использованием кредитных и расчетных карт многие вопросы невозможно разрешить без использования специалистов, обладающих специальными знаниями. Специальные знания могут относиться к области банковской деятельности, технологических особенностей конкретного процесса и т.д. Круг сведущих лиц, обладающих специальными знаниями, достаточно велик, как и круг вопросов, по которым их можно привлечь для выявления и расследования хищений. Впервые термин «специальные знания» законодатель употребил в Федеральном законе № 73-ФЗ от 3 мая г «О государственной судебно-экспертной деятельности в Российской Федерации», и вслед за этим УПК РФ нормативно определил специалиста и эксперта как лиц, обладающих «специальными знаниями» (ст.57, 58 УПК РФ). В рамках данного параграфа необходимо отграничить эксперта и специалиста.

Эксперт — это лицо, назначаемое судом, следователем, дознавателем для производства судебной экспертизы и дачи по ее итогам заключения по вопросам, требующим привлечения для этого специальных познаний в области науки, техники, искусства, ремесла. УПК установлены специальный порядок назначения и производства экспертизы в стадиях предварительного расследования и судебного разбирательства (ст. 195, 207, 269, 283), а также случаи обязательного назначения экспертизы (ст. 196).

Специалист — это лицо, обладающее специальными знаниями, привлекаемое к участию в процессуальных действиях в установленном порядке для содействия в обнаружении, закреплении и изъятии предметов и документов, применении технических средств в исследовании материалов уголовного дела, постановки вопросов эксперту, а также разъяснения сторонам и суду вопросов, входящих в его профессиональную компетенцию (ч. 1 ст. 58 УПК). Специалист, как и эксперт, — это лицо, обладающее специальными познаниями в различных областях знаний, не заинтересованное в исходе дела. Поэтому до начала следственного или иного процессуального действия следователь (дознатель) должен не только удостовериться в его компетенции, но и выяснить его отношение к подозреваемому, обвиняемому, потерпевшему. Специалисту может быть заявлен отвод по тем же основаниям, что и эксперту (ст. 70 УПК).

Основное различие между экспертом и специалистом состоит в их процессуальном предназначении. Эксперт, используя специальные познания, проводит экспертное исследование, на основании которого формирует свое заключение, признаваемое законом в качестве одного из видов доказательств (ст. 74, 80 УПК). Специалист же исследования не проводит, а его заключение (ч. 3 ст. 80 УПК) — это суждение по поставленным перед ним вопросам, которое является самостоятельным видом доказательства (п. 31 ч. 2 ст. 74 УПК).

Сфера использования кредитных и расчетных карт, с точки зрения технических решений, пожалуй, одна из самых сложных и наукоемких сфер расследования. Как свидетельствует практика, в ходе расследования мошенничеств с использованием кредитных и расчетных карт многие вопросы невозможно разрешить без использования специалистов, обладающих специальными знаниями. Специальные знания могут относиться к области банковской деятельности, технологических особенностей конкретного процесса и т. д. Круг сведущих лиц, обладающих специальными знаниями, достаточно велик, как и круг вопросов, по которым их можно привлечь для выявления и расследования хищений. Во многом от того, насколько грамотно

следователь сможет организовать необходимые процессуальные и следственные действия, связанные с установлением обстоятельств дела, настолько и будет зависеть успех расследования в целом и один следователь, даже имея достаточный опыт расследования данной категории дел, не будет настаивать на том, что в совершенстве владеет всеми необходимыми навыками для успешной работы в данной сфере.¹⁹

В большинстве случаев, способы совершения мошенничеств столь разнообразны, что в большинстве случаев следователю просто не обойтись без привлечения к работе соответствующих специалистов. Также очевидно, что и сам следователь должен достаточно хорошо представлять специфику процессов, возникающих при использовании банковской карты, иначе, даже с привлечением специалиста, он не сможет организовать не только свою деятельность, но и деятельность специалиста. Следует сказать, что необходимость привлечения специалиста (ст. 68 УПК РФ) должна быть обусловлена не отсутствием определенной компетенции у лица, ведущего расследование, а последовательной организацией процесса расследования. Важную роль в расследовании преступлений, связанных с мошенничествами с использованием кредитных и расчетных карт, повышении их качества и эффективности играет применение специальных знаний, активное внедрение в деятельность правоохранительных органов современных достижений науки и техники, расширение возможностей использования специальных познаний в деятельности правоохранительных органов. Специфика применения специальных знаний по данной категории дел обусловлена следующим обстоятельством: обнаружение многих документов на электронных носителях возможно только с использованием компьютерной техники, а неквалифицированное ее использование может привести к уничтожению информации, имеющей доказательственное значение.

По мере накопления знаний об использовании банковских карт в целях хищения денежных средств стала разрабатываться проблема необходимости и формы использования специальных знаний при раскрытии и расследовании

¹⁹ Федотов Н.Н. Форензика компьютерная криминалистика 2007 г. С 26-84.

таких преступлений. При этом назрела необходимость в рекомендациях по привлечению отдельных технических специалистов в помощь следователю и оперативным сотрудникам. Часть способов хищений с использованием кредитных и расчетных карт невозможна без использования компьютерной техники преступниками, что до настоящего времени, несмотря на большое количество методических рекомендаций, вызывает проблемы в производстве проверочных и следственных действий сотрудниками правоохранительных органов.

Стоит отметить, что помимо процессуальной формы, участие специалиста в предварительном расследовании мошенничеств, существует консультационно-справочная деятельность сведущих лиц; участие специалистов в подготовке и проведении оперативно-розыскных мероприятий. Консультационная деятельность имеет важное значение в процессе оказания помощи в преодолении противодействия расследованию рассматриваемого вида хищений Консультации представляют собой сообщения специалистами необходимых сведений следователю (оперативному сотруднику), позволяющих правильно оценивать те или иные обстоятельства, подлежащие установлению и последующему доказыванию Консультации могут иметь отношение к методике применения научно-технических средств при проведении ОРМ, особенностям специфики работы какого-либо технического средства, участвующего в использовании кредитной или расчетной карты В то же время консультации не должны касаться правовых вопросов, однако могут помочь получить предварительную информацию, важную для раскрытия и расследования преступления Круг лиц, а также вопросов, по которым можно использовать консультационную деятельность, законом не ограничен, и применять специальные знания могут в данном случае: эксперты, специалисты, представители Банка России, а также сотрудники правоохранительных органов, имеющие опыт расследования данной категории дел.

Для оказания консультационной деятельности к специалистам, как правило, обращаются в случаях:

выяснения особенностей процесса использования банковских карт;
сообщения следователю сведений в области изготовления банковских карт;

выяснения особенностей функционирования технических средств (банкоматов);

при необходимости изъятия технических средств, используемых для хищений, а также средств компьютерной техники и электронных носителей информации;

оказания помощи в подборе материала и составлении вопросов для допроса подозреваемого (обвиняемого);

оказания помощи в подготовке к назначению судебной экспертизы (определении объектов, необходимых для ее проведения, а также круга вопросов, которые необходимо поставить перед экспертом).

Кроме того, по нашему мнению, исходя из специфики расследования данной категории уголовных дел, следует обозначить следующие непроцессуальные формы использования специальных знаний:

привлечение внимания следователя к обстоятельствам, существенным для расследования дела, к которым можно отнести сведения, основанные на изучении выявленных в ходе расследования фактов наиболее результативно данная форма использования специальных знаний может проявляться как при производстве самих следственных действий, так и при осуществлении взаимодействия следственно-оперативной группы при корректировке плана расследования;

организационно-техническое содействие, к которому можно отнести оказание помощи в обработке фотовидеоматериалов, расшифровке компьютерных кодов, а также подготовке технико-криминалистических средств к проведению следственных действий.

В то же время, как показывает практика, следователи далеко не всегда эффективно обращаются к непроцессуальным формам использования специальных знаний.

Одним из видов процессуального использования специальных знаний в

процессе расследования уголовного дела является привлечение специалиста к производству следственных действий, где он использует свои специальные знания и навыки для оказания содействия правоохранительным органам в обнаружении, фиксации и изъятии доказательств; обращения их внимания на обстоятельства, связанные с обнаружением и закреплением доказательств; пояснения специальных вопросов, возникающих при производстве следственных и судебных действий.

Участие специалиста при производстве следственных действий является довольно эффективным, а порой участие специалиста при производстве осмотра или обыска бывает просто незаменимым апример, при производстве обыска в жилище подозреваемого специалист в целях предотвращения возможного противодействия, может подсказать следователю объекты, имеющие значение для дела, оказать помощь в их обнаружении, фиксации среди других объектов, предупредить их уничтожение заинтересованными лицами ч.9.1 статьи182 и ч. 3.1 статьи 183 УПК РФ в настоящее время закрепили обязательное участие специалиста при производстве выемки электронных носителей информации.

Как справедливо отмечает А.А Топорков, «... сейчас методически обязательным участие специалистов считается тогда, когда в ходе следственного действия могут встретиться объекты, осмотр, исследование или фиксация, которых требуют специальных познаний, отсутствующих у следователя»²⁰, однако в практической деятельности следователи расценивают существующие рекомендации только как совет, не являющийся обязательным к исполнению.

Если факт преступного использования кредитной или расчетной карты имел место, то перед правоохранительными органами возникает задача определения лица, осуществившего данные действия, повлекшие криминальные последствия. Опыт показывает, что такую задачу невозможно решить каким-либо одним способом следственные действия в этом случае

1 Топорков А.А Криминалистика М : «Юридическая фирма «КО ТРАКТ»-И ФРА-М», [Электронный ресурс] 2012 Гарант-аэро (дата обращения: 10.04.2014).

прочно пересекаются с применением специальных знаний специалиста, и взаимодействие этих двух направлений приобретает в данном случае решающее значение. Проведение комплекса исследований на предварительном этапе расследования всех обнаруженных на месте происшествия материальных объектов должно способствовать решению главной задачи расследования преступления установлению личности преступника и обстоятельств совершенного деяния.

Как правило, в качестве специалистов для участия в следственных действиях привлекаются сотрудники экспертно-криминалистических подразделений органов внутренних дел, а также сотрудники соответствующих служб банков. Требования, предъявляемые к специалисту в этом случае, должны несколько отличаться от общепринятых: специалист должен знать несколько операционных систем, особенности функционирования банкоматов, импринтеров и др. Незнание специалистом специфики использования пластиковых банковских карт может привести к некомпетентной оценке выявленных криминалистических признаков или даже к полной утрате информации, например записанной на жестких дисках. Любое следственное или процессуальное действие должно быть тщательно подготовлено, а определить круг специалистов необходимо на подготовительном этапе. Так, при проведении осмотра без специалиста следственное действие зачастую сводится к описанию окружающей обстановки и, как следствие низкой эффективности закрепления криминалистических значимых следов, а порой результаты осмотра не несут никакой доказательственной информации. Кроме того, несогласованность со следователем может привести к возможности изъятия всех имеющихся доказательств, фиксации изъятых с игнорированием факта существования между ними какой-либо связи, имеющей отношение к расследуемому событию.

Необходимо привлечение специалиста при проведении таких процессуальных действий, как получение образцов для сравнительного исследования, а именно получение фотоизображений подозреваемого (обвиняемого) в различных ракурсах, а также получение образцов голоса для

предоставления их впоследствии для проведения соответствующих экспертиз.

Среди процессуальных форм использования специальных знаний следует особо выделить назначение и производство судебных экспертиз. Установить все обстоятельства, подлежащие доказыванию при совершении хищений с использованием кредитных и расчетных карт, в т.ч. установить лиц, их совершивших, зачастую невозможно без проведения соответствующей экспертизы. С помощью экспертов имеется возможность установить важные факты, которые подчас без их участия установить чрезвычайно сложно. Экспертом может быть лицо, обладающее специальными знаниями и назначенное в порядке, установленном Уголовно-процессуальным кодексом РФ для производства экспертизы и дачи заключения. Эксперт должен быть не только специалистом в той или иной области человеческой деятельности, обладать специальными знаниями, но и должен понимать сущность методов, используемых в экспертном исследовании.

Основными видами назначаемых экспертиз являются: почерковедческая, технико-криминалистическая экспертиза документов, дактилоскопическая, портретная, компьютерная, фоноскопическая.

Своевременность назначения экспертиз и последовательность их проведения, а также правильная постановка вопросов эксперту являются существенными условиями, обеспечивающими полноту и оперативность расследования, а также эффективным средством преодоления противодействия расследованию. Выбор времени назначения судебной экспертизы может зависеть от целого ряда условий, таких как достаточность имеющихся материалов для будущего экспертного исследования, возможность планирования производства дальнейших следственных действий без заключения эксперта, возможность обеспечения сохранности подлежащих исследованию объектов.

В процессе расследования хищений с использованием кредитных и расчетных карт могут быть назначены традиционные судебные экспертизы: Почерковедческая назначается для установления личности исполнителя рукописного текста и подписи, выполненной путем подражания. Объектами

данной экспертизы могут быть: платежная карта (оборотная сторона с подписью владельца); заявление об открытии счета в банке; генеральное соглашение между банком и клиентом; анкета или расписка в получении карты и т.п.

Основными вопросами, выносимыми на разрешение почерковедческой экспертизы, являются: Исполнен ли рукописный текст (подпись) в слипе (карте) конкретным лицом (держателем карты Ф И О) или другим лицом? Выполнена ли подпись от имени клиента на слипе (кредитной карте, документе) конкретным лицом? Одним или разными лицами выполнены подписи на слипах (кредитных, расчетных картах, документах)?

Особых сложностей при назначении почерковедческих экспертиз у следователя не возникает, однако в правоприменительной практике существуют некоторые вопросы, на которые необходимо обращать внимание лицу, ведущему расследование. Так, в качестве объектов на исследование предоставляются не первый, а второй или третий экземпляры слипов банковских карт, которые оформляются через копировальную бумагу; не применяются меры к обнаружению такого объекта экспертизы, как сама банковская карта некачественные образцы для сравнительного исследования; невозможность проведения экспертизы по изъятым слипам ввиду отсутствия подписи держателя (клиента).

Судебная технико-криминалистическая экспертиза документов назначается при хищениях, совершенных с поддельной банковской картой или банковскими сотрудниками. Объектами данной экспертизы являются сами банковские пластиковые карты, вызывающие сомнения в их подлинности, слипы, прокатанные с них, банковские документы с оттиском печати; изделия из материалов, предназначенных для изготовления документов; пишущие приборы; вещества, использованные для изменения содержания документов (паста-штрих, средства для смывания, травления и пр.). Целью технико-криминалистической экспертизы документов является установление способа изготовления или подделки документов и использованных для этого технических средств, восстановления поврежденных документов, исследования

материалов документов.

При производстве технико-криминалистической экспертизы документов, для установления подлинности банковских карт, исследования слипов могут быть поставлены следующие вопросы: Выполнены ли оттиск клише импринтера торгового предприятия в слипе при помощи клише импринтера, представленного на исследование? На одном или разных импринтерах выполнены оттиски клише импринтера торгового предприятия в слипе? Выполнены ли оттиски эмбоossedованных реквизитов (клише) с карты покупателя в слипе при помощи эмбоossedованных реквизитов (клише) карты, представленной на исследование? С эмбоossedованных реквизитов одной или разных карт выполнены оттиски эмбоossedованных реквизитов с карты покупателя в слипе, представленном на исследование? С использованием какого красящего вещества, инструментов, приспособлений, технических (программно-технических) средств и материалов выполнены оттиски на слипе, представленном на исследование?

Дактилоскопическая экспертиза назначается для установления личности подозреваемого (подозреваемых) по обнаруженным следам пальцев рук. Объектом исследования дактилоскопической экспертизы являются следы рук, обнаруженные на поддельных банковских картах; на оборудовании, инструментах, приспособлениях и материалах, использованных при изготовлении поддельных банковских карт; на товарах, приобретенных с использованием банковских карт. При производстве дактилоскопической экспертизы можно поставить вопросы:

На разрешение судебной компьютерной (компьютерно-технической) экспертизы могут быть поставлены следующие вопросы:

1. Какая информация содержится на магнитной полосе (в памяти микропроцессора) пластиковой карты, представленной на исследование, и как она может быть интерпретирована в соответствии с правилами платежных систем? Например, экспертиза может установить фамилию держателя карты, номер счета, PIN-код, наименование платежной системы, наименование карточного продукта, наименование организации-эмитента, дату окончания

действия карты и т д

2. Производилась ли перезапись (модификация, блокирование) компьютерной информации, содержащейся на магнитной полосе (в памяти микропроцессора)?

3. Какие данные (файлы) были стерты (уничтожены), скопированы, изменены (модифицированы), как изменялось их содержание, дата создания (уничтожения, изменения)?

4. Соответствует ли информация, записанная на магнитной полосе пластиковой карты, информации, имеющейся в элементах внешнего оформления данной карты?

5. Какими специальными знаниями, умениями, навыками должно обладать лицо для проведения вышеуказанных действий с картой?

6. Производилось ли зачисление денежных средств на пластиковую карту (пластиковые карты) в определенный период времени? Если да, то каков был алгоритм действий по зачислению денежных средств и какого числа и в какое время произведены зачисления?

7. При использовании какого компьютера и с использованием какого пароля произведены зачисления денежных средств на пластиковую карту?

8. Когда, с использованием какого банкомата и на какую сумму происходили транзакции по снятию денежных средств с пластиковой карты?

Принимая во внимание, что ответы на часть указанных выше вопросов требуют от эксперта получения доступа к охраняемой федеральным законом тайне, содержащей информацию о вкладах и счетах граждан в банках и иных кредитных организациях, следовательно необходимо получить соответствующее судебное решение. По нашему мнению, учитывая рост хищений, сопряженных с проведением транзакции с использованием третьими лицами SIM-карты мобильного оператора связи, зарегистрированной на держателя карты с подключенной услугой «Мобильный банк», и положительные возможности использования СССПС для установления других обстоятельств, подлежащих доказыванию, в рамках полноты расследования, а также преодоления противодействия расследованию заинтересованных лиц, в случае обнаружения

и изъятия мобильного телефона следовательно необходимо назначать судебную компьютерную (компьютерно- техническую) экспертизу, объектом которой будет информация, хранящаяся в телефоне и SIM-карте «В сотовом телефоне это: продолжительность и оставшиеся без ответа запросы; SMS и MMS информация, данные с SIM-карты, информация на диктофоне и в видеопамяти; данные о WAP-браузере (протокол беспроводного доступа в Интернет), сообщение E-mail и другая специализированная информация. При этом тактически правильно зафиксировать имеющиеся на них отпечатки пальцев рук и микрочастиц. Для систем GPRS/3G в случаях работы с системами мобильных платежей и проведенными транзакциями может быть установлен MSISDN- (международный ISDN номер подвижного абонента), его PIN-код, проведенные транзакции и т д.

Мы поддерживаем мнение юристов, которые относят мобильные телефоны к иным компьютерным средствам или иным программируемым устройствам, в связи с чем мобильный телефон также является объектом компьютерной экспертизы. В данном случае удачными, на наш взгляд, следует признать вопросы, предложенные В.А Козинкиным:²¹

1. На какие телефонные номера осуществлялись звонки, а также с каких телефонных номеров звонили на данный телефон, если возможно, то с установлением даты и времени разговора?

2. Каково содержание телефонной книги представленного телефона?

3. Каково содержание телефонной книги представленной SIM-карты?

4. а какие номера телефонов осуществлялись SMS-сообщения и с каких телефонных номеров поступали SMS-сообщения, их содержание и по возможности даты и время данных сообщений?

5. Имеются ли в памяти представленного телефона изображения, если да, то какие?»

При назначении фоноскопической экспертизы эксперту могут быть поставлены вопросы:

²¹Протосевич А А, Зверьянская Л П Криминалистическая характеристика компьютерных преступлений / Российский следователь 3 № С 45–47; Быков В М , Черкасов В Понятие компьютерной информации как объекта преступлений // Законность 3 № С 37–4 ;

Фоноскопическая экспертиза также назначается в случае возбуждения уголовного дела по материалам дел оперативного учета, когда в ходе оперативно-разыскных мероприятий проводилась запись переговоров субъектов преступлений.

В этом случае на фоноскопическую экспертизу ставятся следующие вопросы:

1. Каково дословное содержание разговора, записанного на предоставленной фоно- или видеограмме?
2. Сколько лиц участвовало в разговоре, записанном на фоно- или видеофонограмме?
3. Произнесена ли устная речь (или ее фрагменты), начинающаяся словами (приводится дословное содержание слов или фразы), гражданину, образцы речи которого представлены на исследование?

Также нельзя не сказать о использовании возможностей портретной экспертизы. Так как, совершение мошенничеств с использованием платежных карт, совершается в местах, которые оснащены камерами видеонаблюдения. Поэтому использование данной возможности может явиться одним из доказательств по уголовному делу.

Диагностическими вопросами могут являться следующие: Какова половая принадлежность лица, изображенного на фотоснимке? К какому типу телосложения (конституциональному типу) относится лицо, изображенное на фотоснимке? К какой возрастной группе относится человек, изображенный на фотографии? Постановка диагностических вопросов возможна при изъятии органами предварительного следствия фотоснимков лица, совершающего (или только что совершившего) преступление, в полный рост.

Проведенный анализ позволяет выделить следующие негативные обстоятельства, влияющие на назначение и производство портретной экспертизы:

- нежелание следователя получать образцы для сравнительного
- исследования; боязнь следователя получить заключение с отрицательным выводом

- заключение о невозможности провести исследование в результате некачественных фотоснимков;

- низкое качество объектов портретной экспертизы в результате:

- фотосъемки с близкого расстояния (часто в банкомате), когда искажаются пропорции, положение и контуры частей лица; съемка с ракурса, затрудняющего распознавание и дальнейшее исследование элементов внешности (например «снизу-вверх» с банкомате и «сверху-вниз» в торговых организациях); низкие технические характеристики систем видеонаблюдения, тогда как «доброкачественными и полными считаются образцы, всесторонне и достоверно отображающие признаки внешности человека».

Объектами портретной экспертизы при расследовании рассматриваемого вида хищений являются фотоснимки или видеокадры, полученные с помощью аппаратуры для видеонаблюдения.

Подводя итог вышеизложенному, мы считаем неприемлемой с позиции уголовно-процессуального закона и имеющихся криминалистических рекомендаций замещение следователями назначения фотопортретной экспертизы другими следственными действиями, результаты которых в соответствии со статьей 88 УПК РФ «Правила оценки доказательств» не могут являться допустимыми и достоверными. Полученные таким образом доказательства, в случае их признания недопустимыми в соответствии со статьей 75 УПК РФ недопустимые доказательства, не могут быть положены в основу обвинения.

В настоящее время использование специальных знаний, как в процессуальной, так и непроцессуальной форме при расследовании хищений с использованием кредитных и расчетных карт, остается на низком уровне. Следователи в целях экономии времени пренебрегают имеющимися криминалистическими рекомендациями по взаимодействию со специалистом по проведению следственных и процессуальных действий, хотя сами не обладают необходимым уровнем специальных знаний, что, в свою очередь, отражается на качестве расследования. Мы полагаем, что пренебрегать имеющимися достижениями науки в области судебной экспертизы, когда в них

имеется необходимость, недопустимо.

ЗАКЛЮЧЕНИЕ

Подводя итог данной работы, необходимо отметить что, актуальные проблемы и особенности расследования мошенничества с использованием платежных карт, исследованы и раскрыты полностью. При проведении данного исследования были выявлены основные проблемы, решение которых позволит успешно решать задачи, стоящие перед правоохранительными органами. А именно к таким особенностям и проблемам в правоприменительной практикенеобходимо отнести:

1)Разработанную методику расследования мошенничества с использованием кредитных и расчетных карт мы рассматриваем в виде теоретической основы.С учетом результатов изучения судебно-следственной нами конкретизированы основные наиболее распространенные способы совершения мошенничеств с использованием платежных карт, обосновано значение в структуре криминалистической характеристики таких элементов, как личность потерпевшего и обстоятельства, способствующие совершению хищения.Практическое значение указанных элементов криминалистической характеристики состоит в наличии информации, способной оказать помощь правоохранительным органам в выдвижении версий, оценке типичных следственных ситуаций и прогнозировании тактики дальнейших действий. Выявлены и изучены типичные следы мошенничеств с использованием реквизитов подлинных кредитных и расчетных карт и SIM-карты мобильного оператора связи, зарегистрированной на держателя карты с подключенной услугой «Мобильный банк», а также банковской карты с предоставлением ДБО.

2) Каждый субъект расследования сталкивается с противодействием расследованию, которое до настоящего времени изучено не достаточно полно. Данное явление мы определяем как противодействие расследованию мошенничеств, совершенных с использованием кредитных и расчетных карт,это умышленная противоправная и иная деятельность заинтересованных в результатах расследования лиц, выражающаяся в действии и (или) бездействии,

направленная на воспрепятствование реализации органами предварительного расследования и суда своих полномочий по установлению истины по уголовному делу. На основе проведенного анализа выявлены приемы противодействия расследованию мошенничеств с использованием кредитных и расчетных карт, определены причины и условия, детерминирующие противодействие. Выявлена взаимосвязь приемов противодействия расследованию мошенничеств с использованием кредитных и расчетных карт с типичными следственными ситуациями, что позволит правоохранительным органам своевременно прогнозировать возможное проявление противодействия еще до проведения следственных действия и выбирать наиболее результативную тактику их проведения. Предложены приемы по противодействию расследованию с использованием кредитных и расчетных карт, даны конкретные методические рекомендации по проведению следственных действий: следственного осмотра, обыска, предъявление для опознания, допроса потерпевшего и подозреваемого (обвиняемого), использование которых позволит нейтрализовать уже возникшее противодействие или устранить факторы, благоприятствующие его проявлению, а именно приемы обнаружения скрываемых предметов, документов; приемы нейтрализации противодействия преступника в ходе допроса; рекомендации по фиксации хода и результатов следственных действий в условиях оказываемого противодействия и др. Одним из эффективных процессуальных приемов может выступить правоприменение статьи 118 УПК РФ «Если соответствующее нарушение допущено в ходе досудебного производства, то дознаватель, следователь составляет протокол о нарушении, который направляется в районный суд и подлежит рассмотрению судьей в течение 5 суток с момента его поступления в суд.»

3) Одной из причин низкого уровня расследования уголовных дел данной категорией, обусловлен отсутствием методических рекомендаций по расследованию данных видов преступлений или же их уровень не соответствует объективной действительности, а также низкий уровень взаимодействия следственных и оперативных подразделений. Проведенное

исследование выявило основные причины, по которым правоохранительные органы в установленный законом срок не могут установить личность лица, подлежащего привлечению в качестве обвиняемого: нарушение криминалистических рекомендаций по производству первоначальных следственных действий, отсутствие соответствующего взаимодействия между службами, занимающимися раскрытием и расследованием преступлений, игнорирование использования специальных знаний, нарушение принципов планирования расследования, несвоевременное возбуждение уголовных дел, отсутствие преодоления противодействия расследованию.

4) Также целесообразно создать федеральный централизованный учет поддельных пластиковых платежных карт в целях создания базы данных для установления общности происхождения пластиковых платежных карт по способу и технологии изготовления, а также выявления лиц, занимающихся их изготовлением.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. Конституция Российской Федерации [принята всенародным голосованием 12 декабря 1993 г.: по состоянию на 21 июля 2014 г.] – Собрание законодательства РФ. – 2014. - № 31. – Ст. 4398.

2. Уголовный кодекс Российской Федерации [федер. закон: принят Гос.Думой 24 мая 1996 г.: по состоянию на 25 июля 2016 г.] – Собрание законодательства РФ. – 2015. - N 30. - Ст. 4659.

3. Уголовно-процессуальный кодекс Российской Федерации: [федер. закон: принят Гос.Думой 18 декабря 2001 г.: по состоянию на 13 июня 2016 г.] – Собрание законодательства РФ. – 2015. - № 27. - Ст. 3981.

4. Об оперативно-розыскной деятельности: [федер. закон: принят Гос.Думой 12 августа 1995 г.: №144-ФЗ по состоянию на 6 июля 2016 г.] – Собрание законодательства РФ. – 2015. - N 30. - Ст. 4659.

5. О банках и банковской деятельности: [федер. закон: принят Гос.Думой 02 декабря 1990 г. № 395-1 ФЗ по состоянию на 6 июля 2016 г.] – Собрание законодательства РФ. – 2015. - N 30. - Ст. 2835.

6. О национальной платежной системе [федер. закон: принят Гос. от 27.06.2011 N 161-ФЗ по состоянию на 5 мая 2017 года] – Собрание законодательства РФ. – 2015. - N 30. - Ст. 4162.

7. Приказ МВД России N 776, Минобороны России N 703, ФСБ России N 509, ФСО России N 507, ФТС России N 1820, СВР России N 42, ФСИН России N 535, ФСКН России N 398, СК России N 68 от 27.09.2013 "Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд" (Зарегистрировано в Минюсте России 05.12.2013 N 30544) // СПС КонсультантПлюс.

8. Приказ Генпрокуратуры России N 39, МВД России N 1070, МЧС России N 1021, Минюста России N 253, ФСБ России N 780, Минэкономразвития России N 353, ФСКН России N 399 от 29.12.2005 (ред. от

20.02.2014) "О едином учете преступлений" (вместе с "Типовым положением о едином порядке организации приема, регистрации и проверки сообщений о преступлениях", "Положением о едином порядке регистрации уголовных дел и учета преступлений", "Инструкцией о порядке заполнения и представления учетных документов") (Зарегистрировано в Минюсте России 30.12.2005 N 7339) // СПС КонсультантПлюс.

9. Приказ МВД России от 31 августа 1993 г № 400 «О формировании и ведении оперативно-справочных, розыскных, криминалистических учетов, экспертно-криминалистических коллекций и картотек органов внутренних дел Российской Федерации» // СПС КонсультантПлюс

10. Приказ МВД России от 29.08.2014 N 736 "Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях" (Зарегистрировано Минюсте России 06.11.2014 N 34570) // "Российская газета", N 260, дата обращения 14.11.2014

Монографии, учебники, учебные пособия.

11. Аннеков С.И. Расследование мошенничества [Текст]: / под.ред. А.А.Леви – Саратов, 2012. – С.20

12. Анненков, С. И. О криминалистической характеристике мошенничества / С. И. Анненков // Актуальные вопросы советской юридической науки. – Саратов 2011. – Ч. 2. – С. 126–128.

13. Алескеров В.И., Максименко И.А. Особенности отдельных следственных действий при расследовании преступлений в сфере компьютерной информации // Вестник Всероссийского института повышения квалификации сотрудников МВД России. 2004 N4(16).

14. Бакрадзе А.А. Теоретические основы уголовно-правовой собственности, совершаемых путем обмана или злоупотребления доверием [Текст] : ...д-ра юрид.наук. М., 2011. С.538

15. Башкатов Л.Н., Безлепкин Б.Т., Бородин С.В. и др. Комментарий к

Уголовно-процессуальному кодексу РФ (постатейный). Под ред. И.П. Петрухина. Изд. шестое, перераб. и дополн. М.: Юрайт, 2008. - 754 с

16. Безлипки́н Б.Т. Комментарий к Уголовно-процессуальному кодексу Российской Федерации (постатейный), 11 –е издание переработ. и доп. М: Проспект, 2014. Ст.140

17. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. Общая и частная теории. М.: Издательство Московского университета, 1987. - 193с

18. Бембеева Г.В. Тактические и психологические особенности расследования мошенничества [Текст] : Дис. ...канд. юрид. наук. Волгоград, 2011. С.188.

19. Берданикова Ф.В. Некоторые проблемы работы с криминалистической информацией на месте происшествия // Российский следователь 2009. №13. С.2.

20. Валеев А.Т. Тактика обыска и выемки при производстве расследования преступлений: Монография. Вологда. 2009.С. 49-159

21. Виноградова, К. А. Особенности методики расследования отдельных видов мошенничеств на первоначальном этапе / К. А. Виноградова // Расследование преступлений: проблемы и пути их решения. 2015. № 1 (7). С. 106-110

22. Гилязов Р.Р. некоторым особенностям способов совершения мошенничеств с использованием средств сотовой связи [Текст]: материалы международной научно-практической конференции 2 «Балтийский юридический форум «Закон и правопорядок в третьем тысячелетии» /Калининградский филиал СПб Университет МВД России, 13 декабря 2013 года. – С.207-209.

23. Герасимов И.Ф., Драпки́н Л.Я., Ищенко Е.П. и др. Криминалистика: Учебник для вузов / Под ред. И.Ф.Герасимов, Л. Я. Драпкина. - 2-е изд., перераб. и доп. - М.: Высшая школа, 2015. - 520 с.

24. Гуев А.Н. Постатейный комментарий к Уголовно-процессуальному кодексу РФ [Электронный ресурс] //Консультант Плюс / ЗАО «Консультант

Плюс». – Версия 40000.00.03 – Электрон. текстовые данные – Режим доступа: клиент-сервер.- загл. с экрана (дата обращения 20.01.2017).

25. Доля Е.А. Формирование доказательств на основе результатов оперативно-розыскной деятельности: Монография, М.: Проспект 2009.

26. Дмитриев Е.Г., Котенков А.В. О некоторых особенностях использования информации систем видеонаблюдения в ходе расследования преступлений // Российский следователь. 2013. N.С.5.

27. Зинин А.М. Руководство по портретной экспертизе. – М.: Эксмо, 2006. – 208 с.; Криминалистика: Учебн. /Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. 3-е изд., перераб. и доп. – М.: Норма, 2008. – С. 322-349.

28. Комментарий к Уголовно-процессуальному кодексу Российской Федерации под общ. ред. А.В. Смирнова. М., 2013. С.230.

29. Криминалистика [Текст]: учебник /под ред. А.Ф. Волынского, В.П.Лаврова.- изд.,доп.и перераб. – М, ЮНИТИ-ДАНА : Закон и право. 2012 С.29.

30. Комментарий к Уголовному кодексу Российской Федерации: постатейный 7-е издание, переработанное и дополненное / отв. ред. В.М. Лебедев. М.: Юрайт- Издат, 2012.

31. Комментарий к Федеральному закону от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» / под ред. А.И. Алексеева, В.С. Овчинского. - М.: Проспект, 2012. - 415 с.

32. Лазарева И.В. Расследование преступлений, связанных с несанкционированным доступом к сети сотовой радиотелефонной связи: автореф. дис. ... канд. юрид. наук. Хабаровск, 2010.

33. Леонова О.В. Особенности проведения некоторых следственных действий по уголовно - процессуальному законодательству // Актуальные проблемы современности уголовного процесса России: Сборник научных статей. - Самара: Самарский университет, 2012. - 234с

34. Лузгин И.М. Методологические проблемы расследования. М., 2013. С 110-115.

35. Мамонов В.С. Уголовно- процессуальные и криминалистические

аспекты осмотра места происшествия в современных условиях. дис. канд.юрид.наук. Краснодар. 2011. С. 42-43.

36. Матвеев, А. Н. Особенности расследования преступлений о мошенничестве с использованием сети «Интернет» / А. Н. Матвеев // Судебная реформа и эффективность деятельности органов суда, прокуратуры и следствия: 7-я науч.-практ. конф. молодых ученых. 24 апреля 2004 г.: тезисы выступлений. –СПб., 2004. – С. 105–107

37. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы: Монография. Омск: Омская академия МВД России, 2011.

38. Основы оперативно-розыскной деятельности ОВД: Учебник / под ред. Ю.А. Агафонова, Ю. Ф. Кваши. - М.: Юрист, 2009. - 376 с

39. Осмотр место происшествия: Практическое пособие / Под ред. А. И. Доворкина. - М.: Норма,2009. - 336 с

40. Рыжаков А.Н. Комментарий к статье 186.1 УПК РФ «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». Консультант Плюс / ЗАО «Консультант Плюс». – Версия 40000.00.03 – Электрон. текстовые данные – Режим доступа: клиент-сервер.- загл. с экрана (дата обращения 20.01.2017).

41. Семенов, Г. В. Криминалистическая классификация способов совершения мошенничества в системе сотовой связи / Г. В. Семенов // Следователь. – 2007. – № 2 (106). – С. 45–49

42. Семенов, Г. В. Классификация способов совершения мошенничества в системе сотовой связи / Г. В. Семенов // Известия Тульс. гос. ун-та. Сер.: Современные проблемы законодательства России, юридических наук и правоохранительной деятельности. – Вып. 4. – С. 193–201

43. Соловьев И.Н. ОВД проводят оперативно-розыскные мероприятия / И.Н. Соловьев // Законы России: опыт, анализ, практика. - 2013. - № 2. - С. 16-21.

44. В.В. Степанов Тактика следственного осмотра и освидетельствования // Тактика следственных действий: учебное пособие / под ред. Комиссарова В.И., Саратов: Издательство СГАП, 2013. С27.

45. Филипов, М. Н. Особенности расследования краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов / М. Н. Филипов. – М.:«Юрлитинформ», 2014. – 160 с

46. Цветкова А.С. К вопросу о правовой регламентации осуществления некоторых оперативно-розыскных мероприятий / А.С. Цветкова // Законы России: опыт, анализ, практика. - 2012. - № 10. - С. 44-49

47. Центров Е.Е. криминалистическое учение о потерпевшем. [Текст] : - М., 2014. С17-20.

48. Яблоков, Н. П. Криминалистика: учебник / Н. П. Яблоков. – Москва: Юрайт: ИД Юрайт, 2013. – с.279

49.Якимович Е.Я. Способы мошенничества с использованием платежных банковских карт // Юридический консультант. 2005. - № 10. - с.10-14

Материалы судебной практики

50. Постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. N 51 “О судебной практике по делам о мошенничестве, присвоении и растрате”

51.Решение Приволжского районного суда города Казани от 23.02.2015 г. // Архив электронных решений суда (дата обращения 12.03.2017 год)

52. Решение Приморского районного суда города Хабаровска от 18.05.2016 г.// Архив электронных решений суда(дата обращения 12.03.2017 год)

53. Решение Ленинского районного суда города Калининград от 25.01. 2016 г.// Архив электронных решений суда(дата обращения 12.03.2017 год)