Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно – Уральский государственный университет
(Национальный исследовательский университет)»
Институт открытого и дистанционного образования
Кафедра «Современные образовательные технологии»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой
/А.В. Прохоров/
28 мая 2019 г.

Методика расследования мошенничества, совершенного с использованием средств сотовой связи и сети Интернет

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
ЮУрГУ – 40.03.01.2019.169.ВКР

Консультанты, (должность)

Руководитель работы
к.ю.н., доцент
/В.А. Морозков/
24 мая 2019 г.

Консультанты, (должность)

Автор работы
обучающийся группы ДО-592
/В.А. Шевчук/
23 мая 2019 г.

Консультанты, (должность)

Нормоконтролер
/Н.В.Назарова/
24 мая 2019 г.

Челябинск 2019

АННОТАЦИЯ

Шевчук В.А. Методика расследования мошенничества, совершенного с использованием средств сотовой связи и сети Интернет. – Челябинск: ЮУрГУ, ДО-592 , 85 с., ил. нет, таб. нет, библиогр. список – 57 наим., прил. нет, слайдов нет

Целью выпускной квалификационной работы является анализ методики расследования мошенничества, совершенных с использованием средств сотовой связи и сети Интернет.

Для достижения поставленной цели исследования были определены следующие **задачи**:

- изучить уголовно-правовую характеристику мошенничества, совершенного с использованием средств сотовой связи и сети интернет,

- рассмотреть криминалистическую характеристику мошенничества, совершенного с использованием средств сотовой связи и сети интернет,

- провести анализ основных положений организации расследования мошенничества, совершенного с использованием средств сотовой связи и сети интернет,

- изучить типичные следственные ситуации первоначального этапа расследования мошенничества, совершенного с использованием средств сотовой связи и сети интернет,

- изучить особенности рассмотрения заявления (сообщения) о преступлении по факту мошенничества с использованием мобильных средств связи,

- рассмотреть тактику отдельных следственных действий при расследовании мошенничества, совершенного с использованием средств сотовой связи и сети интернет.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность выпускной квалификационной работы выражается в развитии информационных технологий современного общества, это повлекло за собой увеличение мошенничества, совершенного с использованием средств сотовой связи и сети интернет. Согласно информации ГИАЦ МВД России, в 2015 г. зарегистрировано 200 598 преступлений, предусмотренных ст. 159.6 УК РФ (что на 24,6 % больше, чем в 2014 г.); в 2016 г. - уже 208 926; в 2017 г. - 222 772 (рост количества на 4,2 % и 6,6 % соответственно); при этом в общей структуре преступности различные виды мошенничества составляют 10,8 %[1].

Объектом исследования является мошенничество с использованием средств сотовой связи и сети Интернет.

Предметом исследования является методика расследования мошенничества с использованием средств сотовой связи и сети Интернет.

Целью выпускной квалификационной работы является анализ методики расследования мошенничества, совершенных с использованием средств сотовой связи и сети Интернет.

Для достижения поставленной цели исследования были определены следующие **задачи**:

- изучить уголовно-правовую характеристику мошенничества, совершенного с использованием средств сотовой связи и сети интернет,
- рассмотреть криминалистическую характеристику мошенничества, совершенного с использованием средств сотовой связи и сети интернет,
- провести анализ основных положений организации расследования мошенничества, совершенного с использованием средств сотовой связи и сети интернет,

[1] МВД России [Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации (https://xn--b1aew.xn--p1ai/). – Режим доступа: https://xn--b1aew.xn--p1ai/

- изучить типичные следственные ситуации первоначального этапа расследования мошенничества, совершенного с использованием средств сотовой связи и сети интернет,

- изучить особенности рассмотрения заявления (сообщения) о преступлении по факту мошенничества с использованием мобильных средств связи,

- рассмотреть тактику отдельных следственных действий при расследовании мошенничества, совершенного с использованием средств сотовой связи и сети интернет.

Методологическую основу исследования составили, во-первых, формально-юридический метод, с помощью которого вычленялись понятия, выяснялась их сущность, признаки, а также отличие одних суждений от других. Во-вторых, структурно-функциональный метод, с помощью которого определялась структура работы, а также излагались результаты исследования в рамках используемых методов. Также были использованы такие методы как: наблюдение, анализ, дедукция, сравнительно-правовой.

Теоретическая и практическая значимость работы. Выводы и практические рекомендации исследования позволяют продолжить дальнейшее научное и практическое изучение заявленной темы. Материалы и отдельные положения работы могут быть использованы для преподавания учебного курса в вузах по дисциплине «Криминалистика».

Структура работы: Выпускная квалификационная работа выполнена в соответствие с предъявляемыми требованиями, и состоит из введения, 3 глав, включающих в себя 6 параграфов, заключения и библиографического списка, общий объем работы 85 страниц.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ И СЕТИ ИНТЕРНЕТ

1.1 Уголовно-правовая характеристика мошенничества, совершенного с использованием средств сотовой связи и сети интернет

Под мошенничеством принято понимать завладение чужим имуществом путем обмана или злоупотребления доверием. Лиц, которые занимаются совершением данного вида преступления называют мошенниками. Особенность данного преступления заключается в том, что жертва мошенничества, ввиду целенаправленного искажения истины, сама передает что-либо из своего имущества мошеннику [1].

В статье 35 Конституции РФ указано, что защита любого имущества, которое находится в собственности у граждан является обязанностью государства. Также в основном Законе государства указано, что никого нельзя лишать имущества без решения суда [2].

В соответствии с ч. 1 ст. 159 «Уголовного кодекса Российской Федерации» (далее – УК РФ) «1. Мошенничество, то есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием, - наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо

[1] Алпатов, А.С. Мошенничество и причинение имущественного ущерба путем обмана или злоупотребления доверием [Текст] / А.С. Алпатов // Трибуна молодого ученого. – 2016. – № 2. – С. 16-37.

[2] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.) [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа:www.pravo.gov.ru.

арестом на срок до четырех месяцев, либо лишением свободы на срок до двух лет.»[1].

Мошенничества, связанные с неправомерным доступом к компьютерной информации с последующим неправомерным списанием денежных средств с расчетных счетов граждан, являются одним из способов совершения преступлений, предусмотренных ст. 159.6 УК РФ.

Объектами преступлений выступают общественные отношения, обеспечивающие законный доступ к денежным средствам, находящимся на счетах физических (юридических) лиц. Основным объектом преступления, предусмотренного ст. 159.6 УК РФ, признаются отношения собственности, дополнительным - отношения в сфере охраны компьютерной информации.

Предметами преступных посягательств являются собственно денежные средства, находящиеся на счетах клиентов банка. В качестве предмета также следует выделить компьютерную информацию, которая умышленно подвергается негативному воздействию. Однако компьютерная информация, которую используют при совершении преступления, предусмотренного ст. 159.6 УК РФ, выступает не предметом, а средством совершения преступления. Так, в ч. 1 ст. 159.6 УК РФ говорится о хищении чужого имущества или приобретении права на чужое имущество «путем ввода, удаления, блокирования, модификации компьютерной информации…». Выполнение указанных действий возможно только с использованием компьютерной информации, заключенной в компьютерные программы, чаще всего, вредоносные. Компьютерная информация в данном случае – это тот инструмент, с использованием которого похищается чужое имущество[1].

В примечании 1 к ст. 272 УК РФ указывается, что под компьютерной информацией понимаются сведения (сообщения, данные), представленные в

[1] Уголовный кодекс Российской Федерации (принят Государственной Думой 24.05.1996 г.) [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа:www.pravo.gov.ru.

форме электрических сигналов, независимо от средств их хранения, обработки и передачи. У информации нет собственника, но имеется обладатель, поэтому информация, имея стоимость, не является имуществом, понимаемым как совокупность вещей[2].

В соответствии с диспозицией ч. 1 рассматриваемой статьи, данное преступление представляет собой хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационнотелекоммуникационных сетей.

Однако следует отметить, что рассматриваемый вид хищения является мошенничеством, который вне зависимости от разновидности (ст. 159 – 159.6 УК РФ) должен предусматривать два альтернативных способа, а именно:

1) Обман, который определяется как ложное утверждение о том, что не соответствует действительности.

2) Злоупотребление доверием, при котором виновный использует определенные отношения, основанные на доверии сторон для получения от потерпевшего денег или иного имущества под условием выполнения заведомо не выполнимых или впоследствии не выполненных обязательств.

Злоупотребление доверием взаимосвязано с обманом. Виновный использует особые доверительные отношения, установившиеся между ним и собственником или иным законным владельцем, чтобы обман был более убедительным, либо прибегает к обману, чтобы заручиться доверием потерпевшего.

При совершении преступления, предусмотренного ст. 159.6 УК РФ виновный используя один (или несколько) способов, указанных в диспозиции

---

[1] Российское уголовное право. Особенная часть [Текст] / под ред. В. П. Коняхина, М. Л. Прохоровой. – М.: Проспект, 2015. С. 638.

[2] Елин, В.М. Мошенничество в сфере компьютерной информации как новый состав преступления [Текст] / В.М. Елин // Бизнес-информатика. 2013. № 2. С. 74.

рассматриваемой статьи, фактически выдает себя за собственника денежных средств, находящихся на счету потерпевшего, и без его ведома и, соответственно, согласия, обращает данные средства в свою пользу. Следует отметить, что при совершении данного мошенничества непосредственного контакта потерпевшего с обвиняемым не происходит.

Следовательно, при совершении преступления, предусмотренного ст. 159.6 УК РФ, фактически отсутствует обман, обязательным признаком которого является введение другого лица в заблуждение путем воздействия на сознание этого лица. Воздействие осуществляется не на психическую сферу человека, а на компьютерную информацию (субъект манипулирует такой информацией посредством технических средств). Потерпевший в это время ничего не знает о передаче имущества или права на имущество и не желает его передавать, а значит, отсутствует такой признак мошенничества, как внешняя добровольность передачи имущества (права на имущество).

Совершение рассматриваемого преступления, условно, можно разделить на несколько этапов.

Первый этап совершения преступления, предусмотренного ст. 159.6 УК РФ, заключается в неправомерном доступе к компьютерной информации, что представляет собой незаконное либо не разрешенное собственником или иным законным владельцем информации несанкционированное обращение к данной компьютерной информации. При этом обязательным элементом, характеризующим данный этап, является то, что виновный стремится использовать эту компьютерную информацию с корыстной целью.

С точки зрения стадий совершения преступления (ст. 30 УК РФ) данный этап можно охарактеризовать как приготовление к совершению преступления по признаку «иного умышленного создания условий для совершения преступления». Следовательно, если действия виновного были пресечены в момент неправомерного доступа к компьютерной информации, то при наличии умысла на совершение мошенничества данное деяние следует квалифицировать по ч. 1 ст. 30

и ст. 159.6 УК РФ, как не доведенные до конца по независящим от лица обстоятельствам.

Так же к первому этапу могут относиться такие действия как удаление, блокирование, модификация, копирование компьютерной информации.

Однако указанные действия, согласно содержания ст. 159.6 УК РФ, фактически являются различными способами совершения преступления.

Удаление компьютерной информации по аналогии с уничтожением компьютерной информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Следует отметить, что удаление и уничтожение (ст. 274 УК РФ) это понятия, наполненные разным содержанием.

Удаление компьютерной информации по смыслу ст. 159.6 УК РФ это, прежде всего один из способов совершения преступления, из реализации которого образуются негативные для информации последствия. При этом, по нашему мнению, удаленная информация может быть восстановлена по инициативе ее законного владельца (потерпевшего) или лицом который собственно ее удалил.

Уничтожение информации, по смыслу ст. 274 УК РФ – это последствия, которые явились результатом совершения данного преступления. Кроме того, по нашему мнению, уничтожение – это процесс необратимый. Восстановление информации в этом случае невозможно.

Блокирование компьютерной информации это результат воздействия на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, то есть совершение действий, приводящих к ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением.

Модификация компьютерной информации – это внесение изменений в компьютерную информацию (или ее параметры).

Под иным вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационнотелекоммуникационных сетей можно понимать любые другие способы воздействия на компьютерную информацию с целью совершения мошенничества.

Например, копирование компьютерной информации, а именно создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации[1].

В теории уголовного права выделяют и другие способы (приемы) мошенничества в сфере компьютерной информации: незаконное завладение регистрационными данными учетных записей; использование платежных сервисов интернет-ресурсов; взлом электронных кошельков; организация благотворительных акций через Интернет, где на банковский счет предлагается перечислять денежные средства[2], внесение грубой подделки банкноты в банкомат[3].

Хищение может совершаться как со счетов граждан, привязанных к банковским картам, так и не привязанных к ним. Одним из наиболее распространенных видов криминального использования компьютерной техники

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» (утв. Генпрокуратурой России) [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа:www.pravo.gov.ru.
[2] Коломинов, В.В. О способе совершения мошенничества в сфере компьютерной информации [Текст] / В.В. Коломинов // Человек: преступление и наказание. 2015. № 3. С. 145-149.
[3] Прозументов, Л.М. Квалификация сбыта поддельных банкнот посредством банкоматов [Текст] / Л.М. Прозументов Л.М., А.В. Архипов // Уголовное право. 2016. № 2. С. 18.

является создание и распространение вредоносных программ, которые используются для хищения денежных средств со счетов клиентов банков.

Объективную сторону хищений с использованием вредоносных компьютерных программ условно можно разделить на несколько этапов:

1) использование вредоносной компьютерной программы (при необходимости – ее создание или модификация);

2) списание денежных средств со счетов потерпевших;

3) обналичивание похищенных денежных средств.

Для совершения хищений со счетов физических (юридических) лиц, указанным способом, виновными лицами, как правило, выполняются подготовительные действия в виде создания (приобретения) и использования вредоносных программ для банковских ЭВМ с целью незаконного получения информации о ключах и паролях банковских систем управления счетами или доступа к системе дистанционного обслуживания счета.

Если при совершении мошенничества создавались, использовались или распространялись вредоносные компьютерные программы, заведомо предназначенные для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, то, помимо квалификации по ст. 159.6 УК РФ, действия виновного лица могут быть квалифицированы по совокупности преступлений, предусмотренных ст. ст. 272, 273 УК РФ.

Так, согласно разъяснениям Постановления Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» (абзац 4 пункт 12) «в случаях, когда указанные деяния (мошенничество авт.) 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»[1].

Квалификация по ст. 273 УК РФ необходима всегда, если с целью совершения мошенничества лицом создана или распространена вредоносная компьютерная программа, так как действия, предусмотренные ч. 1 ст. 273 УК РФ, не предусмотрены объективной стороной рассматриваемого преступления[2].

Разграничение составов преступлений, предусмотренных ст. 159.6 и ст. 272 УК РФ, должно проводиться по следующим элементам и признакам: объекту, предмету, объективной стороне, субъективной стороне. Основным объектом преступления, предусмотренного ст. 272 УК РФ, выступают общественные отношения в сфере обеспечения безопасности компьютерной информации.

Основным **объектом преступления**, предусмотренного ст. 159.6 УК РФ признаются отношения собственности, дополнительным - отношения в сфере охраны компьютерной информации.

Предметом мошенничества в сфере компьютерной информации выступает имущество или право на имущество. Предметом преступления, предусмотренного ст. 272 УК РФ, является компьютерная информация, которая умышленно подвергается негативному воздействию.

Объективная сторона преступления, предусмотренного ст. 159.6 УК РФ, состоит в хищении чужого имущества или приобретении права на чужое имущество, совершенном следующими способами: ввод, удаление, блокирование,

[1] Постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа: www.pravo.gov.ru.

[2] Справка Камчатского краевого суда [Электронный ресурс] // Официальный сайт Камчатского краевого суда (oblsud.kam.sudrf.ru). – Режим доступа: oblsud.kam.sudrf.ru

модификация компьютерной информации либо иное вмешательство в информационную или информационнотелекоммуникационную сеть. Данные способы мошенничества направлены на обращение в пользу виновного чужого имущества, обращение его в свою пользу и влекут причинение имущественного ущерба. В составе неправомерного доступа к компьютерной информации (ч. 1 ст. 272 УК РФ) общественно опасным последствия ограничиваются уничтожением, блокированием, модификацией либо копированием компьютерной информации.

Умысел виновного при совершении преступления, предусмотренного ст. 159.6 УК РФ, в итоге направлен на хищение имущества либо приобретение прав на него; умысел при неправомерном доступе к компьютерной информации – на получение определенных сведений

Хищение денежных средств посредством неправомерного доступа к компьютерной информации, чаще всего, совершается в сети «Интернет» путем удаленного доступа к счетам потерпевших. В ходе выполнения объективной стороны мошенничества виновный, как правило, использует компьютер и модем. Нередко это мобильное компьютерное устройство, наиболее удобное для входа и работы в сети «Интернет», применяется с wi-fi роутером. В отличие от модема, посредством роутера доступ в сеть «Интернет» можно осуществить более чем с одного компьютера.

Состав преступления, предусмотренного ст. 159.6 УК РФ, по конструкции относиться к материальным, то есть предусматривает в качестве обязательных признаков, помимо собственно деяния, также причинноследственную связь и наличие общественно опасных последствий.

Общественно опасные последствия рассматриваемого мошенничества выражаются в виде прямого имущественного ущерба собственнику или иному владельцу имущества (обладателю права на чужое имущество).

Субъективная сторона преступления характеризуется прямым умыслом. Для квалификации содеянного по ст. 159.6 УК РФ должно быть доказано, что

виновный имел целью использование компьютерной информации в корыстных целях.

Субъект преступления – общий (физическое лицо, вменяемое, достигшее 16-летнего возраста).

Состав преступления также будет иметь место в случае, если лицо, к которому поступило СМС-сообщение с указанной выше информацией, позвонит по обозначенному номеру телефона и ему будет предложено сообщить номер банковской карты и пин-код для ее активации (разблокировки). Если же потерпевший перечислил денежные средства, действия лица подлежат квалификации как оконченное преступление по соответствующей части ст. 159 УК РФ. Если потерпевший в процессе разговора осознает, что в отношении его совершается мошенничество, и откажется переводить (передавать) обозначенную сумму, то деяние надо квалифицировать как покушение на совершение преступления, предусмотренного ст. 159 УК РФ.

Подводя итог уголовно-правовой характеристики такого вида мошенничества следует выделить что основным объектом преступления, предусмотренного ст. 159.6 УК РФ признаются отношения собственности. Объективной стороной является хищение чужого имущества или приобретение права на чужое имущество, совершенным вводом, удалением, блокированием, модификацией компьютерной информации либо иное вмешательство в информационную или телекоммуникационную сеть. Субъект преступления – общий, а субъективная сторона – корыстный умысел.

Следует отметить, что на 2018 год существует множество самых разнообразных способов мошенничества с использованием сотовой связи и сети Интернет, что при краже имущество тайно похищается помимо и вопреки воле потерпевшего, при мошенничестве присутствует "добровольная" передача имущества собственником или владельцем преступнику.

1.2 Криминалистическая характеристика мошенничества, совершенного с использованием средств сотовой связи и сети интернет

Криминалистическая характеристика представляет собой совокупность сведений о преступлении, которые способствуют его раскрытию. Она включает данные об особенностях подготовки, совершения и сокрытия следов преступления. Если следователь располагает информацией о наиболее часто используемых виновным лицом способах совершения преступления, приемах маскировки, к которым могут прибегнуть преступники, ему намного легче раскрыть такое преступление. Действия следователя по обнаружению вещественных доказательств и самого виновного в данном случае будут целенаправленными и успешными.

Криминалистическая характеристика преступлений, связанных с хищением денежных средств, совершаемых с использованием компьютерных технологий, имеет ряд особенностей, свойственных для данной категории.

Для расследования данного вида преступления важное значение имеет форма предмета, которая выступает в виде безналичных денежных средств.

Выделем следующие элементы криминалистической характеристики по преступлениям данной категории:

- способ совершения преступлений: подготовка, совершение, сокрытие;
- время, место совершения преступления;
- механизм следообразования;
- сведения о личности преступника (преступников);
- сведения о личности потерпевшего (потерпевших);
- сведения о связи с другими преступлениями.

Особенность хищения денежных средств, совершаемых с использованием компьютерных технологий, обуславливается подготовкой, совершением и сокрытием следов, указывающих на совершение данного преступления. Целью данных преступлений является незаконное завладение денежными средствами,

принадлежащими и хранящимися на банковских и иных платежных счетах клиентов, мотив является только корыстным.

Способы хищения денежных средств с использованием компьютерных технологий достаточно разнообразны и зависят от изобретательности и интеллектуальных способностей преступника. Из них наиболее часто встречаются такие как рассылка SMS-сообщений о выигрыше автомобиля, о блокировке банковской карты, создание Интернет-сайтов по продаже авиабилетов, а также Интернет магазинов, которые предлагают товары по заниженным ценам, требуя при этом перечисления предоплаты. Распространены такие виды услуг, как изготовление, распространение и использование вредоносных программ, которые позволяют дистанционно подменять платежные распоряжения с компьютерных устройств потерпевших либо дают возможность управлять операциями выдачи денежных средств из банкоматов. Одним из способов совершения хищения денежных средств является дистанционное проникновение в компьютерные системы банков, организаций, используя сбои или недостатки в обеспечении безопасности в их работе, что позволяет незаконно списывать денежные средства с банковских счетов.

Способ совершения подобных хищений напрямую связан с созданием и использованием вредоносных компьютерных программ. Заметим, что само место, где было совершено противоправное деяние и место, где наступили общественно-опасные последствия, не совпадают, если хищение денежных средств не совершены сотрудниками коммерческих банков. Механизм совершения хищений денежных средств с использованием вредоносных компьютерных программ условно можно разделить на несколько этапов: использование вредоносной компьютерной программы (при необходимости – ее создание или модификация); списание денежных средств со счетов потерпевших; обналичивание похищенных денежных средств. Рассмотрим первый этап. Места подготовки хищений денежных средств с использованием компьютерных технологий могут находиться по месту жительства либо работы преступника. Они оборудованы

соответствующей компьютерной и иной техникой, используемой для приобретения, разработки, модификации и распространения вредоносных программ. Также техника может быть использована для сбора компрометирующей информации, создания и направления в коммерческие банки поддельных электронных расчетных документов, скиммингового (миниатюрное считывающее устройство, которое может крепиться к банкомату) оборудования для совершения хищения и осуществления иных подготовительных мероприятий. Подготовительные действия могут реализовываться в разных местах. Иногда эти объекты могут быть удалены на достаточно большое расстояние друг от друга, располагаясь в различных регионах страны, а также за рубежом.

В настоящее время существует несколько операционных платформ, которые предназначены для различных компьютерных устройств. Самой распространенной в России и наиболее подверженной деятельности вредоносных программ для ЭВМ, является OS «Android», на основе которой функционирует более половины всех мобильных устройств в России (смартфонов, планшетных компьютеров).

При хищении денежных средств с банковских и иных платежных счетов используются вредоносные программы «троянского» типа. Данные программы распространяются людьми. В задачу «троянцев» входит сбор информации и её передача (копирование) преступнику, уничтожение или модификация, нарушение работоспособности компьютерного устройства, использование ресурсов компьютерного устройства в противоправных целях.

Для операционной платформы «Android» злоумышленниками используются такие вредоносные программы как «Android.bankbot», «TrojanSMS.AndroidOS.Svpeng», «TrojanSMS.AndroidOS.FakeInst».

Например, после установки на мобильное устройство, «Android.BankBot.34.origin» размещает на главном экране операционной системы ярлык, имеющий значок одного из популярных приложений. Если вредоносная программа запускается непосредственно владельцем зараженного мобильного

устройства, то данный ярлык в дальнейшем удаляется. Если же пользователем не запущена вредоносная программа самостоятельно, этот ярлык сохраняется. Вредоносная программа способна автоматически начать свою работу, загрузившись вместе с операционной системой. После того как программа запущена, она запрашивает у пользователя доступ к функциям администратора мобильного устройства. После чего программа начинает отслеживать активность пользователя, ожидая запуска последним ряда популярных приложений таких как «WhatsApp», «Viber», «Instagram», «Facebook», «Twitter».

После запуска одной из указанных программ, «Android.BankBot.34.origin» отображает поверх ее интерфейса собственное окно, которое имитирует запрос ввода конфиденциальной информации (логин и пароль, номер телефона или сведения о кредитной карте). Полученные таким образом данные передаются на управляющий сервер

Чтобы передать похищенную информацию злоумышленникам, а также получить от них команды, ««Android.BankBot.34.origin» соединяется с управляющим сервером, расположенным в анонимной сети «Tor». При первом сеансе связи с удаленным центром вредоносной программой выполняется регистрация зараженного мобильного устройства и передаются основные сведения о нем (IMEI-идентификатор, название модели).

«Android.BankBot.34.origin» получает от сервера необходимую команду, после чего может выполнить следующее действия:

- начать или остановить перехват входящих и исходящих SMS;
- выполнить USSD запрос;
- внести в черный список определенный номер, сообщения с которого будут скрываться от пользователя (по умолчанию в списке содержатся сервисные номера ряда телефонных операторов, системы мобильного банкинга известного российского банка, а также популярной платежной платформы);
- очистить список блокируемых номеров;

- передать на сервер информацию об установленных на устройстве приложениях;
- выполнить отправку SMS сообщения;
- передать на сервер идентификатор вредоносной программы;
- отобразить на экране диалоговое окно или сообщение в соответствии с полученными с управляющего сервера параметрами (например, в команде может задаваться текст, предназначенный для демонстрации на экране, количество полей для ввода данных и т. п.)»[1].

Таким образом, вышеописанная вредоносная троянская программа, «прописавшись» на мобильном устройстве пользователя, дает возможность правонарушителям считывать полную информацию о данном устройстве и установленном на него программном обеспечении, а самое главное – перехватывать, блокировать доступ законного пользователя, и отправлять SMS--сообщения от его имени, при этом пользователь не знает о таких действиях. Приведенные возможности программы по несанкционированной блокировки, копированию и модификации информации наглядно характеризуют ее вредоносность.

Наиболее опасным и сложным в расследовании способом совершения данной категории преступлений является хищение денежных средств в системе дистанционного банковского обслуживания (далее – ДБО), установленной на компьютерном устройстве потерпевшего.

Для примера, в ПАО (публичное акционерное общество) «Сбербанк России» имеется два основных вида программного обеспечения ДБО: «Мобильный банк» и «Сбербанк-Онлайн».

«Мобильный банк» это программное приложение, которое функционирует на терминалах сотовой связи (мобильных телефонах, планшетах) и позволяет путем отправки SMS-сообщения и USSD-команд на определенный номер,

[1] Dr.Web Android.BankBot.34.origin [Электронный ресурс] // официальный сайт ООО «Доктор Веб» (https://vms.drweb.ru/). – Режим доступа: https://vms.drweb.ru/

принадлежащий банку (по линии ПАО «Сбербанк России» по всей территории РФ данный номер определен как «900»), управлять своим банковским счетом. Пользователь получает информацию о состоянии счета банковской карты, осуществляет различные платежи, перевод денежных средств со счета банковской карты на счета других банковских карт. Провайдером при этом является организация, предоставляющая услуги сотовой связи (голосовые данные, SMS-сообщения, MMS-сообщения и др.). Пользование услугой «Мобильный банк» возможно при наличии подключенного к оператору сотовой связи мобильного устройства и сети Интернет для работы данного приложения не требуется.

Схема проведения операции по банковской карте через услугу «Мобильный Банк» давно известна: на своем мобильном устройстве гражданин (являющийся клиентом банка и абонентом оператора сотовой связи одновременно) формирует SMS-сообщение определенного содержания на номер «900» (который показывает все движения денежные средств по банковской карте клиента) или USSD-команду и передает на сервер оператора сотовой связи. Далее сервер оператора сотовой связи передает SMS-сообщение или USSD-команду в процессинговый центр банка ПАО «Сбербанк России», который расположен в г. Москве, тот, в свою очередь, обрабатывает команду/сообщение и проводит соответствующую операцию со счетом карты. Используя возможности вредоносной программы по доступу ко всем SMS-сообщениям, поступающим на мобильный телефон потерпевшего, а также отправки с его номера SMS--сообщений и USSD-команд, злоумышленники, используя сервисы приложения «Мобильный банк», осуществляют хищение денежных средств с банковской карты потерпевшего.

В ПАО «Сбербанк России» также имеется компьютерная система дистанционного банковского обслуживания под названием «Сбербанк-Онлайн». Для доступа к ней необходима авторизация путем введения реквизитов – «логина» и «пароля». Получить данные реквизиты можно у оператора в любом отделении ПАО «Сбербанк России», написав соответствующее заявление, а также

в любом банкомате и терминале банка, предъявив банковскую карту (банкомату, терминалу) в результате чего банкомат/терминал выдаст кассовый чек, где будут указаны «логин» и «пароль». Для функционирования данной услуги обязательно использование сети Интернет, этим она и отличается от услуги «Мобильный банк». В услуге «Сбербанк-Онлайн», видны все счета, принадлежащие клиенту и операции по ним

Для совершения хищения с использованием системы ДБО «Сбербанк-Онлайн» правонарушителям необходим доступ к «логину» и «паролю», который он может получить, используя вредоносные компьютерные программы «троянского» типа

Последующие этапы механизма совершения хищений – вывод денежных средств со счетов потерпевших и их последующее обналичивание, рассмотрены далее при описании функций участников преступной группы.

Особое место в криминалистической характеристике занимает субъект, совершающий хищений денежных средств с использованием компьютерных технологий, т.е. личность преступника.

Лица, создающие вредоносные программы, могут быть специалистами в области программирования, системного администрирования, автоматизированных систем, которые используются в деятельности определенных отраслей, в частности, банковской, обладать определенным уровнем образования в данных сферах. Кроме того, они владеют определенными навыками и умениями, которые ими используются при работе с компьютерами

Сложность механизма совершения таких преступлений говорит о том, что осуществить их в одиночку практически невозможно, и совершаются они, как правило, в составе преступных групп. Данные преступные группы характеризуются организованностью, устойчивостью, сплоченностью, у них четко выработанное, неизменное внутреннее строение, есть лидер и соподчинение между членами группы. Существование группы рассчитано на длительное время с целью осуществления преступной деятельности, направленной на совершение

неопределенного количества преступлений, и масштаб ее может охватывать территорию различных субъектов Российской Федерации. В группе существует четкая специализация участников: в зависимости от распределения преступных ролей каждым выполняются строго свои обязанности. Они объединены между собой единой преступной целью, с четко отработанной системой конспирации и защитой от разоблачения правоохранительными органами. Каждому участнику преступной группы определена обязанность со строгим подчинением руководителю. Отличительной особенностью таких преступных групп является то, что их члены, выполняя конкретные функции, могут быть незнакомы друг с другом, или знакомы только с кем-то из других участников

Механизм совершения хищений определяется распределением ролей участников в преступной группе, которых можно разделить на виды:

1. Организатор.

2. Лица, занимающиеся распространением вредоносных программ.

3. Лица, занимающиеся выводом денег с взломанных счетов, так называемые «заливщики».

4. Участники «дроппроекта», предназначенного для обналичивания похищенных денежных средств. Это псевдокомпания, которая может заниматься чем угодно: продажами, перевозками и т.д. В его состав входят руководитель дроппроекта, «дроповоды», «дропы». «Дроповоды» – это члены группы, создающие юридическое лицо и нанимающие на исполнительную должность (генерального или финансового директора, например) сотрудника. «Дропы» держатели платежных средств.

5. При возникновении необходимости создания вредоносной программы в состав преступной группы также может входить их разработчик или разработчики.

Изучив и поняв, кто является субъектом данной категории преступлений, можно рассмотреть следующие этапы механизма совершения хищений процесс вывода и обналичивания похищенных денежных средств.

Способов вывода денег, применяемых дроппроектами, много. В зависимости от суммы похищаемых денег, могут быть использованы либо частные владельцы платежных карт, готовые за небольшую плату обналичить поступления и передать их представителю «дроповода», либо специально созданные юридические лица, представители которых оформляют «зарплатные проекты» (множество платежных карт для сотрудников фирмы для перечисления зарплаты) в банке, обслуживающем это юридическое лицо.

Конечным звеном обналичивания являются «дропы», которые по команде «дроповода» обналичивают деньги, поступившие на счет, либо переводят их на другой счет, указанный «дроповодом». «Дропы», в свою очередь, делятся на два вида: «разводных» и «неразводных». «Разводные дропы» – это люди, которые, по крайней мере, на первых порах своего сотрудничества с «дроповодом», не осознают, что они участвуют в преступлении. Как правило, задача получения и перевода денег преподносится «разводным дропам» под какимнибудь благовидным предлогом. В отличие от них «неразводные дропы» прекрасно осведомлены о том, для чего они выполняют задания «дроповодов». К лицам, причастным к совершению хищений в системе ДБО, следует отнести «денежных мулов» либо «финансовых агентов», т.е. те, кто соглашается выступить финансовым посредником для использования своего банковского счета с целью перевода похищенных денег на счета злоумышленников. Обналичивание похищенных денежных средств может осуществляться через системы расчетов, электронные кошельки и платежные системы, типа WebMoney, Яндекс деньги, QIWI, PayPal. Вывод денежных средств из платежной системы WebMoney осуществляется с помощью банковской карты, карты, заказанной через сервис WebMoney, виртуальную карту, Интернетбанкинг (услуги, предоставляемой банком по доступу к счетам и операциям в любое время и с любого компьютера, имеющего доступ в Интернет), почтового либо денежного переводов, банковского перевода. Для того чтобы обналичить похищенные денежные средства и при этом не быть разоблаченными, преступники перечисляют эти средства с одного

банковского счета на несколько банковских счетов, как правило, счетов иных платежных систем.

Время совершения хищения напрямую зависит от момента поступления крупной денежной суммы на счет потерпевшего (например, заработной платы). Имея доступ к состоянию счета, преступники дожидаются данного момента, после чего осуществляют вывод денег. В ряде случаев, если это крупная сумма, операции по выводу денежных средств преступники стараются проводить под конец рабочего дня банка, лишая возможности потерпевшего и банк оперативно заблокировать транзакцию.

Потерпевшими при совершении рассматриваемых хищений являются клиенты банков, использующих программное обеспечение дистанционного банковского обслуживания, чьи компьютерные устройства подверглись заражению вредоносными программами «троянского типа». Основными источниками информации о следах преступных действий являются компьютерное устройство потерпевшего со следами наличия и использования компьютерных вредоносных программ, детализация телефонных и иных соединений потерпевшего (сведения об отправленных и полученных SMS-сообщениях и USSD-команд). При подключении компьютера преступника к сети, компьютер сам становиться ее частью, так называемой рабочей станцией, а поэтому следы остаются на серверах, через которые осуществлялось подключение и работа в сети, интернет-сервера, используемые преступниками для размещения электронных почтовых ящиков, а также вредоносной информации. Источником информации о следах является банковский процессинговый сервер, где имеются сведения о незаконных банковских транзакциях со счета потерпевшего.

Таким образом, можно сделать вывод, что подготовкой является сбор данных о жертвах, их банковских счетах, социальном положении и т.д. Наиболее опасным и сложным в расследовании способом совершения преступлений является хищение денежных средств в системе дистанционного банковского обслуживания.

Еще одной особенностью являются место совершения преступления, оно может быть хоть по месту жительства или месту работы, хоть в станции метро, это может быть обычный с виду банкомат или вообще другая страна по средствам сети Интернет. Временем совершения преступления чаще всего является день зарплаты либо крупной сделки потерпевшего.

Личность преступника представляет собой специально обученного человека в области программирования, системного администрирования, автоматизированных систем, которые используются в деятельности определенных отраслей, в частности, банковской, обладать определенным уровнем образования в данных сферах. Кроме того, они владеют определенными навыками и умениями, которые ими используются при работе с компьютерами.

Мошенничество в сети Интернет обладает рядом отличий по сравнению с традиционным мошенничеством. Эти отличия обусловливают особенности расследования данного преступления. В частности, такие особенности проявляются при производстве оперативно-розыскных мероприятий и следственных действий.

2 ОСОБЕННОСТИ ОРГАНИЗАЦИИ И РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ И СЕТИ ИНТЕРНЕТ

2.1 Основные положения организации расследования мошенничества, совершенного с использованием средств сотовой связи и сети интернет

В последние годы в Российской Федерации наблюдается устойчивая тенденция роста количества преступлений, совершаемых путем хищения чужого имущества, приобретения права на чужое имущество путем обмана или злоупотребления доверием, что подтверждается объективными данными.

Согласно информации ГИАЦ МВД России, в 2015 г. зарегистрировано 200 598 преступлений, предусмотренных ст. 159.6 УК РФ (что на 24,6 % больше, чем в 2014 г.); в 2016 г. - уже 208 926; в 2017 г. - 222 772 (рост количества на 4,2 % и 6,6 % соответственно); при этом в общей структуре преступности различные виды мошенничества составляют 10,8 %[1].

Однако если ранее преобладало мошенничество, выражавшееся в обмане о потребительских свойствах товара, доставке товаров, производстве работ, то в настоящее время получило распространение «высокотехнологичное» мошенничество, осуществляемое с использованием современных средств мобильной связи.

По оценкам различных экспертов, ущерб, причиняемый такими преступлениями, исчисляется миллиардами долларов (от 10 до 40 млрд долларов). При этом подсчитать его точную сумму невозможно, поскольку операторы сотовой связи для сохранения репутации о своих потерях не сообщают, а абоненты, обманутые мошенниками на суммы до 1000 рублей, в большинстве случаев не заявляют о подобных фактах в правоохранительные органы, так как не

[1] МВД России [Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации (https://xn--b1aew.xn--p1ai/). – Режим доступа: https://xn--b1aew.xn--p1ai/

верят в возможность последних установить и привлечь к ответственности преступника и вернуть похищенные денежные средства, и по этой причине не желают тратить время на общение с ними.

Такой подход оправдан, поскольку существуют сложности в расследовании подобных преступлений, обусловленные недостаточной профессиональной подготовленностью сотрудников, а также методико-криминалистическим обеспечением расследования. Кроме того, расследование затрудняется спецификой способа их совершения, которая заключается:

1) в возможности донести необходимую информацию до потенциальной жертвы (как в виде звонка, так и СМС-сообщения) с учетом своей анонимности и безопасности;

2) получении от жертвы денег без вступления с ней в непосредственный контакт, что снижает объем и качество доказательственной базы по делу;

3) возможности нахождения как потерпевшего, так и преступника в любом уголке земного шара (с этим связаны некоторые особенности установления места совершения преступления и, соответственно, места производства предварительного следствия).

Кроме того, негативным фактором является также некачественное проведение доследственных проверок, отсутствие наступательности со стороны органов предварительного следствия системы МВД России.

Следует отметить, что процесс расследования любых преступлений, в том числе рассматриваемых, состоит из следственных и иных процессуальных действий, осуществляемых следователем на основании имеющегося плана расследования и направленных на формирование доказательственной базы и выполнение предписаний уголовно-процессуального законодательства.

При этом итог расследования зависит не только от выбранного следователем комплекса следственных действий, закрепляющих доказательственную информацию по делу, но и от качества указанных действий,

их соответствия требованиям Конституции Российской Федерации и действующего уголовно-процессуального законодательства.

В случае нарушения прав участников уголовного судопроизводства, процедуры проведения следственного действия, неполучения в необходимых случаях согласия различных субъектов (например, руководителя следственного органа, суда) результаты такого следственного действия будут признаны на основании ст. 75 УПК РФ недопустимыми доказательствами по делу, не будут иметь юридической силы. Они не смогут использоваться в качестве основы обвинения, а также для доказывания любого из обстоятельств, входящих в предмет доказывания.

В связи с изложенным особое значение имеет осмотр предметов (а именно средств сотовой связи), проводимый при расследовании мошенничества данного вида, результаты которого, как правило, крайне важны для изобличения преступника и закрепления доказательств его виновности. Важность осмотра обусловлена тем, что сотовый телефон по таким делам является одним из главных одновременно следообразующих и следовоспринимающих объектов[1].

Путем осмотра названного объекта по уголовным делам о преступлениях рассматриваемой категории можно получить информацию, имеющую порой определяющее значение для расследования: выявить контакты мошенника и установить иных членов преступной группы (практика показывает, что данные преступления совершаются именно группами), определить иных потерпевших, не заявлявших в правоохранительные органы о совершенном в отношении их мошенничестве, установить следы, хранящиеся в памяти сотового телефона и свидетельствующие о соединениях с потерпевшим, и др.

От того, насколько качественно будет проведено данное следственное действие, может зависеть судьба уголовного дела, восстановление нарушенных

[1] Янин, С.А. К вопросу о некоторых элементах криминалистической характеристики мошенничеств, совершаемых с использованием средств сотовой связи [Текст] / С.А. Янин // Теоретические и практические аспекты развития юридической науки: сб. ст. междунар. науч.-практ. конф., 2017. С. 179-181.

прав потерпевшего и привлечение виновного к установленной законом ответственности[1].

Полагаем, что специфика осмотра сотовых телефонов по уголовным делам о «телефонном» мошенничестве определяется тактическими особенностями и правовым режимом производства данного следственного действия. Рассмотрим названные аспекты подробнее.

Общими тактическими правилами осмотра сотовых телефонов являются своевременность, объективность, полнота, планомерность, использование помощи специалистов, а также технических средств.

Рассматриваемое следственное действие условно подразделяется на несколько этапов: подготовительный, рабочий и заключительный.

Содержание подготовительного этапа составляют определение места и времени проведения осмотра, подбор и приглашение участников (понятых, специалиста), подготовка технических средств.

Рабочий этап - непосредственно визуальное восприятие и изучение признаков осматриваемого телефона.

Заключительный этап - составление протокола осмотра предметов, ознакомление с ним участников осмотра, просмотр видеозаписи осмотра (в случае, если таковая производилась).

Специфика тактики осмотра телефона определяется в полной мере рабочим этапом осмотра и заключается, во-первых, в содержании действий следователя по визуальному восприятию и фиксации в протоколе внешних признаков телефонного аппарата и хранящейся в нем информации, а во-вторых, в определенной последовательности данных действий, что обусловлено особенностями объекта осмотра - сотового телефона - как сложного электронного устройства.

[1] Машлякевич, В.А. К вопросу о необходимости проведения осмотра места происшествия при расследовании мошенничеств, совершаемых с использованием средств телефонной связи [Текст] / В.А. Машлякевич // Российский следователь. 2015. N 10. С. 7-9.

Условно осмотр сотового телефона можно подразделить на несколько подэтапов:

1) внешний осмотр;

2) конструктивный осмотр;

3) осмотр информационной составляющей [1].

Каждый из них имеет некоторую специфику. При внешнем осмотре следователь воспринимает и фиксирует информацию о наружном строении и состоянии телефонного аппарата (в протоколе отмечаются марка, модель, тип, форма аппарата, материал и цвет корпуса, линейные размеры; наличие маркировочных, фирменных логотипов, объективов фото- и видеокамер, разъемов зарядного устройства, наушников; наличие и расположение отверстий микрофона, динамика; количество и расположение клавиш).

Кроме того, по общим тактическим правилам осмотра предметов обязательно указание на специфические приметы аппарата (сколы, царапины, потертости, отсутствие определенных элементов); наличие чехлов, наклеек, гарнитуры и др.

На подэтапе конструктивного осмотра производится изучение и фиксация конструкции телефона по его составным частям (задняя крышка телефона и (или) аккумуляторной батареи, флеш-карта). Данные части описываются по общим правилам описания предметов - материал, форма, линейные размеры, маркировочные обозначения (наименование, марка, модель, емкость и др.), цвет, идентификационные номерные обозначения, наличие логотипа оператора связи.

На подэтапе осмотра информационной составляющей аппарата подлежат изучению и фиксации сведения, содержащиеся в памяти телефона, на флеш- и Б!М-картах (контакты, записи, сообщения, фото- и видеофайлы и др.).

Данный этап рекомендуется начинать с указания в протоколе процедуры разблокировки клавиатуры телефона, после чего перечисляются графические

[1] Васюков, В.Ф. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел [Текст] / В.Ф. Васюков, А.В. Булыжкин // Российский следователь. 2014. N 2. С. 2-4

элементы, которые отобразились на его экране после разблокировки. Затем нажатием комбинации клавиш *#06# производится проверка серийного-номера мобильного телефона (отображается на экране). После этого в протоколе осмотра последовательно указывается информационное содержимое телефона - список контактов мошенника, сообщений, наличие изображений, фотографий (где также могут быть снимки соучастников мошенничества), видеороликов и т.д. При описании определенного вызова указывается его вид (входящий, исходящий, не принятый), время, длительность, данные абонента, с которым предполагаемым мошенником осуществлен контакт, а также его абонентский номер. Последнее особенно важно для установления иных соучастников мошенничества, как уже было отмечено выше, и потерпевших, не обращавшихся в полицию по факту совершенного в отношении их преступления. Описание SMS-, MMS-сообщения включает соответственно его текстовое и (или) графическое содержимое (тип, размер, время создания файла, кто изображен, продолжительность ролика).

В ходе осмотра важной представляется последовательность перечисленных этапов. В случае, если телефонный аппарат выключен, осмотр производится в вышеописанном порядке. Если телефон включен, то целесообразно провести вначале внешний осмотр, затем осмотр информационной составляющей и только после этого конструктивный осмотр, так как последний предполагает отключение телефона из-за необходимости отсоединения аккумуляторной батареи, флеш и SIM-карт. В дальнейшем, вероятно, быстро включить телефон не представится возможным ввиду его блокировки и необходимости введения кода блокировки (PIN-кода), так как предполагаемый мошенник, как правило, добровольно сообщать его не будет. Изложенные обстоятельства могут исключить возможность незамедлительного полноценного исследования его информационного содержимого.

В ходе осмотра на каждом из перечисленных выше этапов необходимо проводить детальную фотосъемку аппарата и его содержимого (внешней, оборотной, боковых панелей телефона - при внешнем осмотре; внешней и

оборотной стороны аккумуляторной батареи, флеш- и SIM-карты, внутренней стороны корпуса аппарата так, чтобы на снимке был виден его IMEI-номер, - при конструктивном осмотре; экрана телефона с информацией, представляющей значение для уголовного дела, - при осмотре информационной составляющей). Следует рекомендовать применение видеосъемки для визуальной фиксации большого объема сведений, содержащихся в информационной среде телефона.

Для повышения эффективности следственного действия и исключения возможности уничтожения информации при неумелом обращении с ней представляется целесообразным также привлечение для участия в осмотре специалиста соответствующей категории. Иными участниками осмотра являются понятые, а также при необходимости потерпевший, подозреваемый (в зависимости от принадлежности осматриваемого телефона).

Кроме тактических аспектов осмотра, необходимо учитывать и требования норм права[1], при несоблюдении которых результаты даже качественно проведенного следственного действия с точки зрения его организации и тактики могут быть признаны недопустимыми доказательствами.

УПК РФ не содержит положения, прямо регламентирующие порядок осмотра средств сотовой связи. По этой причине следователь, изучая информационное содержимое телефонного аппарата, может допустить нарушение положений Конституции Российской Федерации, что чревато серьезными последствиями для него как должностного лица и для перспектив уголовного дела.

Данный аспект обусловлен следующими факторами. В сотовом телефоне имеется информация, в том числе носящая личный характер. Кроме сведений о входящих и исходящих вызовах, в памяти телефона могут храниться личные фотографии, СМС-переписка, различные записи и др. Доступ к подобной информации, исходя из требований ст. 23 Конституции Российской Федерации,

[1] Бутенко, О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия [Текст] / О.С. Бутенко // Lex Russica. 2016. N 4. С. 49-60.

может осуществляться только при условии личного согласия владельца в силу права на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, ограничение которого допускается только на основании судебного решения.

Выработку единой позиции относительно правового режима осмотра затрудняет и неоднозначная судебная практика, противоречие судебных решений различных инстанций друг другу.

Например, определением Конституционного Суда Российской Федерации от 2 октября 2003 г. N 345-О установлено, что право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления. В силу этого информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи. Для доступа к указанным сведениям органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения.

В надзорном определении Верховного Суда Российской Федерации от 2 июня 2006 г. по делу N 9-ДП06-10 относительно выемки документов, содержащих информацию только о входящих и исходящих сигналах соединений телефонных аппаратов, без прослушивания и фиксации содержания последних указана противоположная точка зрения: «при производстве выемки у операторов связи документов о входящих и исходящих сигналах соединений похищенного мобильного телефона тайна содержания переговоров сохраняется, поскольку

целью выемки является только информация о входящих и исходящих звонках с похищенного телефона.

Ссылки на определение Конституционного Суда Российской Федерации от 2 октября 2003 г., утверждение, что подобным следственным действием будут нарушены права граждан на тайну телефонных переговоров, Судебная коллегия находит несостоятельными».

Определением Конституционного Суда Российской Федерации от 8 апреля 2010 г. N 433-О-О гражданину Тарасову Н.А., оспаривавшему конституционность ч. 1 ст. 176 и ч. 1 ст. 285 УПК РФ, которые, по его мнению, вопреки правовой позиции Конституционного Суда Российской Федерации, выраженной в определении от 2 октября 2003 г. N 345-О, позволяют органам предварительного следствия без вынесения соответствующего судебного решения производить осмотр мобильных телефонов, изъятых у подозреваемых в совершении преступлений при заключении их под стражу, а при исследовании в судебном заседании протоколов следственных действий - оглашать сведения, содержащиеся в электронной памяти этих мобильных телефонов, было отказано в принятии жалобы по следующим основаниям.

Данные законоположения лишь устанавливают основания для производства следственных действий в виде осмотра материальных объектов, имеющих значение для уголовного дела, а также правила оглашения в судебном заседании протоколов следственных действий. Они, таким образом, не могут рассматриваться как нарушающие права подозреваемых и обвиняемых в совершении преступления, в том числе права заявителя, гарантированные статьями 23 (ч. 2), 24 (ч. 1) и 46 (ч. 1) Конституции Российской Федерации. Определение же того, были ли в ходе судебного производства по уголовному делу Н.А. Тарасова соблюдены требования закона, а также проверка законности и обоснованности правоприменительных решений, принимавшихся при проведении следственных действий, не входят в компетенцию Конституционного Суда Российской Федерации, установленную статьей 125 Конституции Российской

Федерации и статьей 3 Федерального конституционного закона «О Конституционном Суде Российской Федерации».

В кассационном определении Омского областного суда N 22-2225/12 от 24 мая 2012 г. указано: «несмотря на то, что глава 25 УПК РФ прямо не закрепляет обязанность следователя получать судебное разрешение на осмотр СМС-переписки, эта обязанность вытекает из других норм как уголовно-процессуального закона и положений Конституции Российской Федерации, так и из международных норм... подлежащих безусловному применению в Российской Федерации.

Очевидно, что приведенные выше положения предполагают защиту тайны личной жизни, требуя судебного разрешения на любые оперативно-розыскные мероприятия и следственные действия, которые могут ее нарушить».

Кроме вышеприведенных, имеется еще ряд судебных решений по вопросам специфики правового режима осмотра средств сотовой связи, также неоднозначно трактующих положения Конституции Российской Федерации и УПК РФ, что, несомненно, не способствует формированию единой судебно-следственной практики осмотра.

При этом известно, что органы, осуществляющие уголовное судопроизводство, ориентируются с учетом специфики своей деятельности на мнение Верховного Суда Российской Федерации, по сути, нарушая при этом основополагающие принципы соблюдения прав и свобод граждан, установленные Конституцией Российской Федерации и разъясненные Конституционным Судом Российской Федерации.

Представляется, что в случае обращения граждан, права которых будут ущемлены подобным подходом, в Европейский Суд по правам человека, решение данной инстанции окажется не на стороне российских правоохранительных органов по причине того, что она не связана рамками национального законодательства, а рассматривает дело, исходя из установленных

национальными законами и международными правовыми актами прав и свобод человека и гражданина.

Таким образом, можно сделать следующий вывод. Использование сотовых телефонов в качестве вещественных доказательств при расследовании мошенничества, совершаемого с их использованием, обладает спецификой, определяемой, во-первых, особенностями осматриваемого объекта как электронного устройства, на котором хранится информация, а во-вторых, правовым режимом исследования таких объектов.

При этом с позиции тактики представляется целесообразным рекомендовать следователям производить осмотр по рассмотренным в статье правилам с привлечением специалиста в сфере высоких технологий соответствующей квалификации.

С правовой же точки зрения, несмотря на имеющуюся позицию Верховного Суда Российской Федерации, следователям в случае необходимости производства осмотра информации, хранящейся в сотовом телефоне, рекомендуется обращаться за согласием к его владельцу, а при отсутствии такого согласия - в суд.

Таким образом можно сделать вывод, что при использованию средств сотовой связи и компьютерной техники в качестве вещественных доказательств не потребует значительных временных затрат и дополнительных усилий, однако в полной мере будет способствовать качественному и результативному изучению рассматриваемых объектов, что, в свою очередь, позволит получить важные фактические данные и повысить качество доказательственной базы по делу и исключить негативные последствия в виде вынесения решений Европейским Судом по правам человека о неправомерности действий отечественных правоохранительных органов.

2.2 Типичные следственные ситуации первоначального этапа расследования мошенничества, совершенного с использованием средств сотовой связи и сети интернет

В результате изучения уголовных дел о мошенничествах с использованием средств сотовой связи были выделены наиболее типичные следственные ситуации, складывающиеся на первоначальном этапе расследования:

1) мошенник лично получил у потерпевшего денежные средства;

2) денежные средства (по требованию мошенника) переведены через банковские учреждения в указанный им город на имя конкретного получателя или через платежные терминалы QIWI на определенный номер мобильного телефона;

3) денежные средства были переданы потерпевшим курьеру (соучастнику).

По каждой из названных ситуаций, складывающихся в процессе расследования, перед следователем стоит задача выбора наиболее рациональной и эффективной системы действий и построения их в определенной последовательности, то есть разработка алгоритма (программы) расследования мошенничества. В настоящей работе мы предлагаем своеобразный универсальный алгоритм действий следователя и органа дознания, с корректировкой отдельных моментов исходя из конкретной следственной ситуации:

1. Произвести работу с потерпевшим. Допросить его. Предмет допроса потерпевшего может составить установление следующих основных обстоятельств:

- способ связи с потерпевшим: на сотовый или стационарный телефон поступил звонок (СМС, ММС); номер телефона, с которого поступил звонок (СМС, ММС); время поступления звонка потерпевшему;

- просьбы, предложения, которые были выдвинуты: кем представился преступник, о чем он говорил, какие действия предлагал выполнить и в связи с какими событиями; запомнил ли потерпевший голос преступника, может ли охарактеризовать его, сможет ли опознать преступника (по каким характерным признакам); какую сумму денежных средств и за какие услуги преступник просил передать;

- способ передачи денежных средств: если блиц-переводом - на чье имя (Ф.И.О.), адрес этого лица; если через посредника - в какое время и в каком месте осуществлялась передача денег; подробное описание человека, которому были переданы деньги (может ли потерпевший его опознать и составить фоторобот); был ли посредник на автомобиле (описание транспортного средства, государственный номер автомобиля); если переводом на счет определенного номера сотового телефона - на какой номер сотового телефона была зачислена денежная сумма;

- иные обстоятельства, имеющие значение для уголовного дела: звонил ли потерпевший своим родственникам (например, при требовании денег за родственников по различным причинам), в какой момент, что было установлено из разговора; звонил ли потерпевший преступнику повторно, если да, то о чем он говорил с ним, предлагал ли преступник передать ему еще денежные средства, если да, то за какие услуги, сделал ли это потерпевший, если нет, то почему.

При допросе потерпевшего обязательно установить возможность опознания потерпевшим голоса преступника. Направить потерпевшего в экспертное подразделение для составления фотокомпозиционного портрета преступника, приобщить результаты к материалам уголовного дела.

2. Установить источник телефонного звонка потерпевшему:

- получить детализацию звонков потерпевшего в день совершения преступления и последующие дни, когда осуществлялась связь с

преступником или посредниками, которую приобщить к материалам уголовного дела;

- среди входящих и исходящих вызовов детализации звонков потерпевшего установить абонентский номер сотового телефона преступника;

- направить запрос в сотовую компанию или Бюро специальных технических мероприятий УМВД России конкретного региона (одним из направлений деятельности которого является выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи[1]) об установлении анкетных данных лица, на имя которого зарегистрирован тот или иной номер;

- подготовить материалы для возбуждения ходатайства перед судом о получении информации о соединениях между абонентами и (или) абонентскими устройствами, а именно: о предоставлении разрешения на получение данных о входящих и исходящих соединениях, установлении IMEI-номера, с которым работала сим-карта, с указанием привязки к базовой станции ее адреса местоположения и азимута направления, о движении денежных средств по абонентскому номеру, на который были перечислены денежные средства, и о том, с какими IMEI-номерами работал абонентский номер в интересующий период времени;

- после получения судебного решения копии направить в соответствующие компании операторов сотовой связи региона, в номерную емкость которых входит абонентский номер;

- произвести осмотр полученных протоколов телефонных соединений мобильных телефонов, по которым возможно установление данных абонента и IMEI-номера используемого аппарата;

[1] Управление «К» МВД России[Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации (https://xn--b1aew.xn--p1ai/). – Режим доступа: https://xn--b1aew.xn--p1ai/

- выполнить запрос по IMEI-номеру используемого аппарата сведений обо всех соединениях между абонентами или абонентскими устройствами с указанным IMEI-номером в сотовых компаниях конкретного региона с указанием адресов базовых станций, телефонных номеров абонентов и сведений об анкетных данных, осмотр полученных протоколов соединений[1];

- в случае регистрации установленного лица за пределами региона необходимо сообщить об этом в Управление уголовного розыска УМВД России соответствующего региона с целью последующего направления в установленный регион телеграммы;

- в случае звонка на стационарный городской телефон получить в суде разрешение на получение в телефонной компании, обслуживающей абонентский номер телефона, детализации соединений телефона потерпевшего в день совершения преступления, в дальнейшем направить запрос в телефонную компанию на предоставление этих сведений, после чего произвести выемку и приобщить данные к материалам уголовного дела.

Следует учитывать, что данный вид «заочного» мошенничества в большинстве случаев совершается осужденными лицами, отбывающими наказание в местах лишения свободы, в том числе в других регионах страны. Соответственно, при нахождении базовой станции в районе близлежащего исправительного учреждения необходимо направить в подразделение уголовного розыска поручение о проведении оперативно-розыскных мероприятий с целью установления личности преступника с использованием возможностей оперативных подразделений исправительной колонии, а также направить запрос в Главное управление ФСИН России по региону, в номерной емкости которого

[1] Зимин, Р.В. К вопросу о расследовании мошенничеств в сфере кредитования физических лиц, совершенных с использованием поддельных документов [Электронный ресурс] / Р. В. Зимин // Справочно-правовая система «Консультант-Плюс»(http://www.consultant.ru/). - Режим доступа: http://www.consultant.ru/ .

находился абонентский номер, с целью установления факта изъятия интересующих мобильных телефонов и сим-карт у лиц, отбывающих наказание в данном учреждении.

Установленных лиц проверить по всем имеющимся оперативно-справочным, криминалистическим и розыскным учетам информационных центров, в том числе других регионов России.

3. Допросить лицо, на чье имя зарегистрирован номер сим-карты, с использованием которой был совершен звонок (СМС, ММС) с целью мошеннических действий, в результате чего установить: когда, где и при каких обстоятельствах это лицо приобрело сим-карту, используемую преступником; использовало ли оно эту сим-карту в собственных интересах, как долго; где в настоящее время находится данная сим-карта; каким образом сим-карта вышла из владения этого лица;передало ли оно какому-либо лицу данную сим-карту; если передало, то когда, где, при каких обстоятельствах, имеются ли установочные данные гражданина, которому была передана сим-карта; имеются ли среди окружения лица ранее судимые, если имеются, где они в настоящий момент, какие их связывают отношения и т. д.

4. Направить запрос в организации, осуществляющие денежные переводы: «Юни-стрим», «МОБИ.Деньги», «Яндекс.Деньги», «WebMoney» и др. При получении ответов провести анализ, из которого установить местоположение абонента на момент совершения преступления, предполагаемые связи преступника, получателей денежных средств.

5. Произвести работу с посредником - получателем денег от потерпевшего:

- в случае использования преступниками при получении денежных средств автомобиля надлежит немедленно организовать его розыск (путем объявление плана «Перехват», направления запросов в службы

такси, а также посредством систем учетов ГИБДД, оперативно-справочных, криминалистических и розыскных);

- допросить посредника, установив: когда, где, в каком размере, с предъявлением каких документов он получал денежные средства; как распорядился этими средствами; по чьей просьбе он получал денежные средства; как познакомился с данным гражданином; как ему объяснили просьбу получения денежного перевода, знал ли он о том, что деньги получены преступным путем; дать подробное описание внешности гражданина; выяснить, сможет ли посредник его опознать;

- получить у данного лица детализацию входящих и исходящих соединений с его абонентского номера;

- произвести выемку записей телефонных переговоров между заказчиком такси и оператором службы.

6. По выполнению вышеописанных указаний наметить последующие следственные и оперативно-розыскные мероприятия согласно материалам, собранным в рамках уголовного дела, и полученной информации. При получении проверенных данных, указывающих на окончание преступления на территории другого субъекта России, информировать соответствующее Следственное управление для решения вопроса о передаче уголовного дела для дальнейшего расследования в порядке ст. 152 Уголовно-процессуального кодекса Российской Федерации.

Очевидно, что перед следователем и органом дознания стоит задача планирования по выбору наиболее рациональной и эффективной системы действий и построения их в определенной последовательности, то есть разработка алгоритма расследования мошенничеств, в том числе с использованием средств сотовой связи. Алгоритмизация и планирование позволяют своевременно проработать основные пути расследования, тактику и последовательность производства следственных действий, оперативно-розыскных и организационных

мероприятий, определить и обеспечить эффективность использования дополнительных сил, средств и времени для выполнения определенного объема работ.

Отдел "К" УМВД РФ отмечает, что на 2017 год выявлено множество номеров телефонов, которые регулярно используются мошенниками с целью введения в заблуждение граждан и выманивания у них денежных средств.

Можно привести ряд номеров, которые используются мошенниками:

- +74957296019 - просьба перезвонить для получения "приза" на радио,

- +79021005421 - просьба пополнить счёт на номер 89613793578,

- +79031936251 - приходит сообщение с просьбой вернуть деньги, ошибочно перечисленные абоненту,

- +79046377386 - приходит сообщение абоненту с просьбой о помощи,

- +79052975318 - приходит сообщение с просьбой о том, чтобы положили денежные средства на номер телефона,

- +79062981070 - приходит сообщение о утере паспорта, в сообщении злоумышленники просят через терминал закинул от 1000-5000 рублей,

- +79062997798 - приходят сообщения абонентам на телефон, мошенники просят положить деньги на телефон,

- +79062998100 - мошенники звонят после размещения объявления на сайтах о потерянных вещах,

- +79062999030 - мошенники звонят гражданам после размещения объявления на сайтах о потерянных вещах,

- +79062999253 - мошенники звонят после размещения объявления на сайтах о потерянных вещах,

- +79117548598 - мошенники присылают сообщение о просьбе положить денежные средства на новый номер телефона 89650251297,

- +79121437627 - мошенники присылают сообщение о выигрыше автомобиля, чтобы получить информацию, надо позвонить на номер,

- +79121465693 - мошенники присылают сообщение о том, что выиграл компьютер от Европа плюс,

- +79125284414 - мошенники звонят, представляются сотрудниками технического отдела Билайн, просят назвать данные, которые нужны для уточнения данных абонентов,

- +79128336593 - представляются центром технической поддержки Билайн, грозят блокировкой сим-карты,

- +79134689587 - приходит сообщение, что у сына проблемы, перезвонит сотрудник ДПС и поможет решить возникшую проблему,

- +79151310600 - представляются сотрудниками Билайн, для перерегистрации телефонного номера просят отправить смс на номер 8444, после чего списываются деньги со счета.

При допросе потерпевшего обязательно установить возможность опознания потерпевшим голоса преступника. Направить потерпевшего в экспертное подразделение для составления фотокомпозиционного портрета преступника, приобщить результаты к материалам уголовного дела.

Установить источник телефонного звонка потерпевшему:

- получить детализацию звонков потерпевшего в день совершения преступления и последующие дни, когда осуществлялась связь с преступником или посредниками, которую приобщить к материалам уголовного дела,

- среди входящих и исходящих вызовов детализации звонков потерпевшего установить абонентский номер сотового телефона преступника,

- направить запрос в сотовую компанию или Бюро специальных технических мероприятий УМВД России конкретного региона (одним из направлений деятельности которого является выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи об установлении анкетных данных лица, на имя которого зарегистрирован тот или иной номер,

- подготовить материалы для возбуждения ходатайства перед судом о получении информации о соединениях между абонентами и (или) абонентскими устройствами, а именно:

- о предоставлении разрешения на получение данных о входящих и исходящих соединениях, установлении IMEI-номера, с которым работала симкарта, с указанием привязки к базовой станции ее адреса местоположения и азимута направления,

- о движении денежных средств по абонентскому номеру, на который были перечислены денежные средства,

- о том, с какими IMEI-номерами работал абонентский номер в интересующий период времени,

- после получения судебного решения копии направить в соответствующие компании операторов сотовой связи региона, в номерную емкость которых входит абонентский номер,

- произвести осмотр полученных протоколов телефонных соединений мобильных телефонов, по которым возможно установление данных абонента и IMEI-номера используемого аппарата,

- выполнить запрос по IMEI-номеру используемого аппарата сведений обо всех соединениях между абонентами или абонентскими устройствами с указанным IMEI-номером в сотовых компаниях конкретного региона с указанием адресов базовых станций, телефонных номеров абонентов и сведений об анкетных данных, осмотр полученных протоколов соединений.

Общим для мобильных "разводов" является то, что преступник всегда просит перечислить деньги авансом, то есть до обещанного решения проблем якобы попавшего в беду родственника либо оплаты налога за выигрыш или его доставки. Способами получения денег преступниками являются как пополнение счета его мобильного телефона, либо, в случаях, если принимающим номером является оператор Би-Лайн, непосредственное обналичивание денег со счета мобильного телефона в отделениях Юнистрим - банка, получение блиц-перевода

в отделениях Сбербанка России, обналичивание денег через платежные системы "QIWI" и многие другие.

Для запутывания следов выхода на непосредственного получателя денег, мошенники часто пользуются услугами лиц, занимающихся частным извозом, телефонные номера которых узнают у диспетчеров транспортных компаний. Часть переводимых таксистами сумм, по указанию мошенника, причитается им (таксистам) в качестве вознаграждения.

Отдел "К" УМВД РФ отмечает, что звонки на номера потерпевших совершаются с других регионов. Существует договоренность с другими службами, поэтому информация сразу же передается о том, из какой точки страны был сделан звонок. Однако поймать с поличным телефонных мошенников практически невозможно - они используют либо электронные деньги, либо присылают такси с просьбой доставить наличные. Выявить, на кого именно зарегистрирован номер, тоже практически невозможно. У частных дилеров можно приобрести сим-карты, зарегистрированные на других людей. Соответственно, человек может вообще не подозревать, что на него зарегистрированы определенные номера.

Подводя итог, следует отметить, что в настоящее время профилактика и предупреждение телефонных мошенничеств, приобретают все большую актуальность. В своей преступной деятельности мошенники охватывают широкий круг лиц, но все же, чаще всего жертвами становятся люди пенсионного (пожилого) возраста.

Дознаватель в ходе досудебного производства по уголовному делу на основании части второй статьи 158 (Окончание предварительного расследования) УПК РФ и требований приказа МВД России от 19.01.2006 № 19 «О деятельности органов внутренних дел по предупреждению совершения преступлений» обязан выявлять причины и условия, способствовавшие совершению преступления, и направлять соответствующие представления в организации или должностным лицам для их устранения.

При выполнении мероприятий профилактического характера дознавателю, также целесообразно использовать не процессуальные формы профилактики - выступления в печатных изданиях, на радио, телевидении, выступления в учебных и трудовых коллективах, а также использовать современное средство информации—Интернет.

3 ТАКТИКА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПРИ РАССЛЕДОВАНИИ МОШЕННИЧЕСТВА, СОВЕРШЕННОГО С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ СОТОВОЙ СВЯЗИ И СЕТИ ИНТЕРНЕТ

3.1 Особенности рассмотрения заявления (сообщения) о преступлении по факту мошенничества с использованием мобильных средств связи

Заявление (сообщение) о преступлении по факту совершения мошеннических действий с использованием мобильных средств связи поступает:

- от физических лиц (о хищении с его мобильного счета или банковской карты денежных средств в результате обмана третьих лиц);

- из других источников (банков, кредитных организаций, средств массовой информации и других).

В соответствии с п. 4 ч. 1 ст. 140 УПК РФ таким сообщением является постановление прокурора о направлении материалов, свидетельствующих о совершении мошеннических действий с использованием мобильных средств связи, путем перевода денежных средств с банковских карт потерпевших на банковские счета третьих лиц. в орган предварительного расследования для решения вопроса об уголовном преследовании[1].

Данный вид преступлений носит межрегиональный характер. Используемые при совершении мошенничеств счета и платежные карты финансовых и кредитных организаций, а также SIM-карты операторов связи оформляются в разных регионах Российской Федерации. Это вызывает трудности у органов следствия и дознания при определении места преступления, при проведении неотложных следственных действий и оперативно-розыскных мероприятий (далее—ОРМ).

[1] Уголовно-процессуальный кодекс Российской Федерации (принят Государственной Думой 22.11.2001 г.) (в редакции федеральных законов от 01.04.2019 № 46-ФЗ) [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа:www.pravo.gov.ru.

Указанием врио Министра внутренних дел Российской Федерации генерал-полковника полиции А.В. Горового от 13.07.2015 № 1/5562 «Об организации работы по противодействию отдельным видам мошенничеств» территориальным органам МВД России, принявшим заявление (сообщение), предписано принять решение о возбуждении уголовного дела.

По делам о мошенничестве в первоочередном порядке производятся: осмотр места совершения преступления; допросы потерпевшего, свидетелей преступления, подозреваемого (обвиняемого): обыск или выемка предметов (документов): осмотр и исследование предметов (документов), носителей компьютерной информации; назначение соответствующих экспертиз и иные действия, направленные на выяснение и фиксацию значимой информации по делу.

В случае установления в ходе расследования точного места совершения преступления за пределами обслуживаемой территории после производства неотложных следственных действий следует передавать уголовное дело прокурору для направления по подследственности в порядке, установленном статьей 152 УПК РФ.

В соответствии со статьей 144 УПК РФ проверка сведений, содержащихся в заявлении (сообщении), для принятия решения о возбуждении уголовного дела, осуществляется посредством: получения объяснений от лица, которому противоправными действиями причинен вред, свидетелей и лица, совершившего преступление.

При получении объяснения от заявителя необходимо установить следующую информацию:

- о платежной карте, с которой переведены денежные средства (дата получения, срок действия, вид платежной системы, банк-эмитент карты, документы о получении карты);

- об обстоятельствах, в связи с которыми им перечислены денежные средства: о содержании разговора (SMS) с лицом, совершившим преступление; об

абонентском номере, с которого пришло сообщение, состоялся разговор; о персональных данных, переданных заявителем лицу, совершившему преступление (адрес места жительства, наличие денежных средств. PIN и т. п.);

- о способе перечисления и сумме денежных средств, наличии квитанции или других документов, подтверждающих проведенную операцию;

- о предпринятых действиях после обнаружения факта мошеннических действий (сообщение в банк-эмитент, получение выписки по счету и т. д.).

При получении объяснения от участников проверки сообщения о преступлении следует выяснять следующие вопросы у сотрудников банков:

- круг обязанностей;

- процедура осуществления платежей: наличие договора с заявителем как держателем платежной карты, обращения о ее блокировке, о выписке по лицевому счету, о проверке правомерности списания денежных средств со счета;

- сумма списанных с лицевого счета заявителя денежных средств за указанный в сообщении временной период, какие документы это подтверждают;

- у сотрудников организаций, на банковских (лицевых) счетах которых аккумулировались похищенные денежные средства: какие документы, удостоверяющие личность, предъявляло виновное лицо, характер его действий: наличие соучастников, транспортного средства: имеются ли в зале камеры видеонаблюдения.

При получении объяснения от лица, совершившего преступление, необходимо установить следующие обстоятельства:

- время, характер и способ совершения обмана с целью хищения чужих денежных средств: порядок действий по приготовлению к совершению преступления (приобретение телефона. SIM-карт, открытие банковского (лицевого) счета, перечень подключенных услуг сотового оператора, приискание сообщников и т. д.);

- время и источник получения информации о потерпевших, наличие средств на их банковских счетах: сумма похищенных денежных средств,

направления их расходования; круг соучастников, роль каждого из них; причины (мотивы) совершения преступления;

- способы сокрытия преступления (уничтожение телефонных аппаратов, SIM-карт);

- оформление счетов, телефонных номеров на подставных лиц. по подложным документам.

Так же в ходе проведения проверочных мероприятий необходимо установить и приобщить к материалам проверки:

- документы, регулирующие отношения между держателем карты и банком-эмитентом: выписки по банковским (лицевым) счетам заявителя и виновных лиц;

- журнальные ленты банкоматов: договор о предоставлении услуги «короткий номер»;

- чек оплаты сотовой связи;

- сведения о владельце «электронного кошелька» платежной системы;

- регистрационные данные доменных имен: IP-адрес владельца сайта;

- договор об оказании услуг доступа в интернет: другие материалы, необходимость в которых возникнет в процессе предварительной проверки.

При рассмотрении заявлений (сообщений) данной категории может производиться осмотр места происшествия (места установки платежных терминалов, банкоматов и других).

В ходе осмотра стоит решать задачи по поиску возможных источников доказательств (в частности, следует установить наличие видеокамер и принять меры по изъятию видеозаписи).

В процессе проведения проверки целесообразно давать органу дознания обязательное для исполнения письменное поручение о проведении ОРМ, к которым могут относиться:

- опрос банковского персонала и работников других организаций: наведение справок путем направления запросов в банки, регистрационные организации, процессинговые компании и т. д.;

- выявление лиц. совершивших преступление. организация наблюдения за ними, их связями и имуществом (местами встреч, дачами, гаражами и т. д.);

- получение информации о соединениях между абонентами и (или) абонентскими устройствами в случае оставления преступником информации с указанием номера телефона или установления факта общения заявителя с преступником.

Если предложенные преступником способы связи или перевода денежных средств осуществляются с помощью сети информационно-телекоммуникационной сети «Интернет», следует поручить органу дознания проведение ОРМ с целью получения сведений об установочных данных лица, указанных при регистрации на Интернет-ресурсе (номер телефона, адрес электронной почты, которая указывалась при регистрации профилей, информации об IP-адресах, с которых осуществлялось администрирование, а также за кем закреплены данные IP-адреса).

В случае необходимости возможно изъятие технических средств, используемых заявителем и лицом, совершившим преступление и направить их на комплексную компьютеро-техническую экспертизу, позволяющую получить доступ к информационным носителям с последующим их исследованием.

В соответствии со статьей 195 УПК РФ судебная экспертиза может быть назначена и проведена до возбуждения уголовного дела.

Примерный перечень вопросов эксперту при проведении комплексной компьютеро-технической экспертизы.

Исправен ли представленный информационный носитель? Если нет, то каковы причины неисправности? Если да, то рассмотреть при дальнейшем исследовании следующие вопросы.

Имеется ли на представленном информационном носителе (указать каком именно) программное обеспечение для работы с электронными платежными системами? Если да, то имеется ли информация об учетных (регистрационных) данных пользователей, зарегистрированных в таких системах?

Установлено ли на представленном информационном носителе вредоносное программное обеспечение, заведомо приводящее к модификации, блокированию, копированию, распространению компьютерной информации?

Возможно ли с представленного технического средства осуществление доступа к информационно-телекоммуникационной сети «Интернет»? Если да, то каким образом?

Имеются ли файлы, содержащие следующие «ключевые выражения»

(текстовые последовательности):…..(может указываться содержание SMS или иных сообщений, полученных заявителем?

Имеются ли файлы, являющиеся электронными копиями документов, представленных для сравнительного анализа (распечатки SMS или иных сообщений)? Если да, то какова дата их создания, изменения, направления, удаления?

В случае, если заявитель или лицо, совершившее преступление, использовали в качестве технического средства мобильный телефон (смартфон), к выше перечисленным вопросам, возможно добавить следующие.

Имеется ли на информационных встроенных (внутренняя память), съемных (флэш-карта или иное) носителях представленного технического средства (указать какого) файлы. SMS, MMS или иные сообщения, переданные с помощью Интернет-ресурсов. являющиеся электронными копиями документов, представленных для сравнительного анализа? Если да, то какова дата их создания, изменения, направления, удаления, с какого технического устройства и по средствам какого программного обеспечения они переданы?

Имеются ли на информационных носителях данные об использовании представленного технического средства для осуществления звонков, передачи

сообщений на техническое устройство, используемое заявителем, если да то в какой период времени (дата/время), при помощи какого программного обеспечения (Интернет-ресурса) осуществлена передача информации?

Кроме того, при рассмотрении заявлений (сообщений) граждан и расследовании уголовных дел о совершении хищений денежных средств со счетов банковских карт с использованием информационно-телекоммуникационной сети «Интернет», при размещении потерпевшим на Интернет-ресурсах объявлений предлагается использовать положительный опыт УМВД России по Мурманской области по производству проверочных мероприятий.

Так. в ходе опроса (допроса) заявителя (потерпевшего), лица, совершившего преступление, подозреваемого (обвиняемого) устанавливаются:

- когда и какое по содержанию объявление было размешено в информационно-телекоммуникационной сети «Интернет», на каких Интернет-ресурсах: регистрационные данные (ФИО, номер телефона, адрес электронной почты, территориальное место расположения, причина подачи объявления (продажа, обмен или приобретение имущества, знакомство, получение (предоставление) услуг или иного характера), использованные заявителем при размещении объявления: регистрационные данные (ФИО, номер телефона, адрес электронной почты, территориальное место расположения и иная значимая информация), использованные подозреваемым (обвиняемым) при обращении к объявлению заявителя (потерпевшего);

- каким техническим средством пользовался заявитель (потерпевший), лицо совершившее преступление, подозреваемый (обвиняемый) (мобильный телефон (смартфон), компьютер (стационарный, портативный, планшетный и т. д.): наличие документов на право предоставления компанией-провайдером услуг по выходу в информационно-телекоммуникационную сеть «Интернет» и статистики посещения заявителем (потерпевшим), подозреваемым (обвиняемым)

Интернет-ресурсов за необходимый временной период (с момента размещения объявления до совершения преступления);

- информация о пользователях (регистрационные данные (в случаях регистрации на данном Интернет-ресурсе), дата/время. IP-адреса), обращавшихся к объявлению, размещенному заявителем у администрации Интернет-ресурсов.

Таким образом, нужно сделать вывод, что особенности рассмотрения заявления (сообщения) о преступлении по факту мошенничества с использованием мобильных средств связи определены спецификой способов совершения, данного вида преступления и перечисления полученных денежных средств на счет совершившего преступное деяние лица.

3.2 Особенности тактики отдельных следственных действий при расследовании мошенничества, совершенного с использованием средств сотовой связи и сети интернет на первоначальном этапе расследования

При расследовании преступлений, связанных с хищением денежных средств в сфере компьютерной информации, основными следственными действиями являются:

1. Осмотр места происшествия;

2. Обыск;

3. Осмотр предметов;

4. Выемка (в том числе, электронных носителей информации, электронной почтовой корреспонденции);

5. Допрос (потерпевшего, свидетеля, эксперта, специалиста, подозреваемого, обвиняемого);

6. Получение информации о соединениях между абонентами и (или) абонентскими устройствами;

7. Назначение экспертизы.

Рассмотрим, каждое из вышеуказанных следственных действий.

1. Осмотр места происшествия. Данное следственное действие, проводится, как правило, до возбуждения уголовного дела, и в минимально кратчайшие сроки после совершения преступления, а поэтому его результаты несут в себе максимальное количество информации о событии преступления, следах преступника и размере причиненного вреда. По преступлениям, связанным с хищением денежных средств в сфере компьютерной информации местом происшествия будут являться:

- место расположения компьютеров, принадлежащих потерпевшему;
- место, где было обнаружено хищение денежных средств;

В ходе осмотра места происшествия можно установить:

- имеются ли на месте происшествия следы события преступления;
- какие предметы содержат следы расследуемого преступления; -

какие технические средства или документы использовались для совершения преступления;

- кто мог стать очевидцем совершенного преступления;

Сущность указанного следственного действия состоит в обследовании места преступления, с целью отыскания, фиксации и изъятия следов, оставленных лицом его совершившим, а также получения иных значимых сведений. Так как осмотр места происшествия производится в минимально кратчайшие сроки после его выявления, то и сведений о самом преступлении у следователя минимальное количество. Задача состоит в том, чтобы собрать как можно больше информации о преступлении, его материальных и идеальных следов.

Прибыв на место происшествия, следователь получает сведения о событии преступления, обнаруженных следах и объектах хищения денежных средств, изменениях внесенных в исходную обстановку.

По преступлениям, совершаемым в сфере компьютерной информации, основная часть доказательств содержится в компьютерной технике, носителх электронной информации (жесткие магнитные диски, компакт-диски, флешкарты), а также документах выполненных в бумажном виде. Поэтому в

первую очередь надо обращать внимание на указанные предметы, на них могут быть обнаружены следы преступной деятельности, указывающие на хищение денежных средств в сфере компьютерной информации. Следователю необходимо зафиксировать в протоколе осмотра места происшествия, где были обнаружены указанные предметы, их функциональное назначение, индивидуальные признаки, имеющиеся на них маркировки, надписи.

Определенную специфику осмотра места происшествия, представляет помещение, где имеется сервер (например, кредитная организация), на котором возможно будет находиться информация, относящаяся к событию преступления. В протоколе осмотра следователь должен зафиксировать факт присутствия технических средств, к которым нет логического доступа из осматриваемого помещения, так как место, откуда осуществляется управление сервером, находится, как правило, в ином помещении. Также необходимо указать на то, откуда производится доступ администраторов к серверу на логическом уровне. Данное место доступа также должно быть осмотрено следователем.

Особенностями осмотра места происшествия будет являться, поиск информации не только о самом событии преступления, но и о его подготовке и сокрытии. На это могут указывать средства электросвязи, вредоносные программы на компьютерных носителях информации, электронные записи, хранящиеся в памяти компьютера (сетевые адреса, PIN-коды, сведения об электронных счетах).

Отметим, что к следственному осмотру необходимо обязательно привлекать специалиста в области компьютерных технологий и использовать его знания, для фиксации и изъятия следов преступления.

По результатам осмотра места происшествия, следователь может установить, использовались ли компьютерные технологии при совершении преступления, если да, то каким образом.

2. Обыск. Основанием для проведения любого вида обыска, является наличие достаточных данных у следователя, свидетельствующих о том, что при

лице, либо в его автомашине, жилище или ином помещении могут находиться орудия преступления, похищенное имущество, предметы и документы, с помощью которых было совершено преступление, а также иные вещи, имеющие значение для дела.

С учетом имеющейся у следователя информации по делу, производится подготовка к обыску. В подготовку входит: изучение предварительной информации о месте обыска (характеристика здания, сооружения, количество этажей, комнат, наличие в помещении компьютерной техники и т.д.), о лицах находящихся в здании (их количестве, характеристики), наличии охранной сигнализации, тревожной кнопки, наличии домашних животных (собак и т.д.), пути подхода и отхода. Определяется место установки электрического распределительного щита.

Исходя из собранной информации формируется следственнооперативная группа, приглашаются соответствующие специалисты, подбираются необходимые технические средства, в том числе дополнительные средства фиксации хода и результатов следственного действия, осветительные приборы и т.д. Подготавливаются предметы, необходимые для упаковки изымаемых объектов (коробки, конверты, пакеты, фольга, нить, листы бумаги с оттисками печатей, клей, липкая лента скотч, степлер).

По преступлениям, связанным с хищением денежных средств в сфере компьютерной информации, в ходе обыска целесообразно направить усилия на обнаружение и изъятие таких вещей и предметов, как компьютерная техника, мобильные средства связи, флеш-карты, CD-, DVD-диски, и иные носители электронной информации. Следует также обратить внимание на такие объекты, имеющие значение для дела, как поддельные кредитные банковские карты, бумажные носители информации с записями логинов, паролей и аккаунтов, номера ПИН-кодов, электронные адреса других пользователей, номера банковских счетов, банковские реквизиты, информация об электронных переводах, переписка, свидетельствующая о связях преступника и т.д. Также

необходимо при обыске искать денежные средства, полученные от преступной деятельности, договоры на доступ к сети Интернет, расчетно-кассовые и бухгалтерские документы, а также личные документы преступника и т.д.

«При производстве обыска следует учитывать, что в современном мире, многие носители электронной информации могут быть преобразованы в различные предметы. Например, флеш-карты могут быть интегрированы с банковскими картами, кулонами, ручками, пулями, игрушками, брелоками и т.д. Поэтому целесообразно использовать специальный прибор (нелинейной локации), который позволит обнаружить средства мобильной связи и электронные носители информации в любом помещении, автомобиле и при личном обыске. Если на месте происшествия изымаются носители электронной информации, то в обязательном случае должен участвовать специалист. Владелец изымаемого носителя электронной информации, либо владелец самой информации вправе заявить ходатайство о производстве копирования информации с изымаемого электронного носителя. В связи с этим специалист, в присутствии понятых производит копирование информации с изымаемых электронных носителей, на другие электронные носители, которые в последующем остаются у собственника данной информации» ч. 3.1 ст. 183 УПК РФ.

В ходе обыска подлежат изъятию: стационарные ЭВМ, ноутбуки, планшеты, мобильные средства связи и другая компьютерная техника, а также носители электронной информации и записи на бумажных носителях относящиеся к событию расследуемого преступления. При обнаружении компьютерной техники для ее последующего изъятия, следователю необходимо получить консультацию у специалиста, соединены ли компьютеры единой сетью и имеют ли сервер, если имеется сервер, он подлежит изъятию, так как на нем содержится вся информация подключенных к сети компьютеров. На практике следователи не всегда устанавливают данные обстоятельства, и после изъятия компьютеров, на их жестких дисках информация отсутствует, так как она хранилась на сервере. При осмотре места происшествия следователю необходимо

помнить о том, что с целью противодействия выявлению и расследованию совершаемых преступлений серверы зачастую хранятся в других помещениях, т.е. отдельно от компьютеров. Системные блоки и серверные устройства изымаются в сборе, и каждое из этих устройств упаковывается в отдельную картонную коробку, клапаны которой закрываются, заклеиваются листами бумаги с оттисками печати подразделения, проводящего изъятие. Способ изъятия с заклеиванием, например, липкой лентой-скотч разъемов является неправильным, так как в полной мере не может предотвратить доступ третьих лиц к информации, содержащейся на компьютере, что в последующем защитники могут использовать как обстоятельства влекущие недопустимость доказательств. При изъятии компьютерной техники необходимо обращать внимание на записки, стиккеры, находящиеся рядом с рабочим местом оператора. При их обнаружении они так же подлежат изъятию, так как могут нести информацию о кодах доступа к компьютерным программам.

Изъятие мобильных телефонов и планшетных компьютеров также имеет свои особенности. Сам сотовый телефон и планшетный компьютер может содержать на себе массу доказательств, свидетельствующих о том, что именно подозреваемый пользовался данным телефоном или планшетом. Это, например, следы пальцев рук, микрочастицы, следы биологического происхождения, запаховые следы и т.д. Учитывая, что следователь может не в совершенстве обладать знаниями о правилах изъятия и сохранения следов, следует приглашать специалиста в целях исключения их возможной утраты.

При изъятии сотового телефона и планшетного компьютера, их необходимо перевести в режим «полет», не выключая полностью. Телефон и планшетный компьютер для исключения возможности получения сигнала извне, оборачивается в фольгу, после чего упаковывается стандартным образом в упаковку, исключающую любой доступ к технике посторонних лиц.

Вместе с сотовыми телефонами необходимо изымать и зарядные устройства, что касается и ноутбуков. Во время изъятия необходимо предпринять

меры по установлению кода доступа к меню телефона и планшетного компьютера. Данными мерами будут являться результаты оперативно-розыскной деятельности, а также обнаружение и изъятие личных записей владельца телефона.

Предоставление изъятых образцов техники (особенно сотовых телефонов и планшетных компьютеров) для проведения экспертного исследования необходимо обеспечить в кратчайшие сроки.

В протоколе следует отражать все действия, производимые в ходе обыска. Таковыми являются: нажатия на клавиши клавиатур, подсоединения и отсоединения проводов, место обнаружения каждого объекта, имеющего значение для дела.

3. Осмотр предметов. Далеко не все следователи имеют полное представление о том, какая информация может содержаться на компьютерной технике или мобильном средстве связи и о правилах ее изъятия. Поэтому при их осмотре рекомендуется приглашать для участия специалиста и с его помощью осматривать данные технические средства, так как, не имея специальных знаний в области компьютерных и информационных технологий, малейшее неправильное действие может привести к безвозвратной утрате значимой для дела информации.

Осмотр предметов делится на два этапа. Первый этап – это внешний осмотр, и второй этап – это детальный осмотр.

На первом этапе, производится внешний осмотр технического средства. В протоколе осмотра отражается, какое техническое средство осматривается, его модель, марка, производитель. Также указываются размеры технического средства, цвет, наличие внешних разъемов, для Mini(Micro)USB, зарядных устройств и т.д. Обращается внимание на наличие особых примет, видимых повреждений, дополнительных атрибутов. Если осматривается мобильное средство связи, то необходимо производить осмотр аккумуляторного устройства со съемом задней крышки, сим-карты, флеш-карты. В ходе осмотра устройства, производится его детальная фотосъемка внешней, оборотной и боковых сторон.

Фотографирование производится и тех частей, на которых имеются надписи, либо стиккеры с надписями, обязательно IMEIномера, таким образом, чтобы надписи отчетливо читались.

На втором этапе, производится более детальный осмотр предмета. С его включением и осмотром содержимого, находящегося в памяти устройства. Вся последовательность осмотра фиксируется в протоколе следственного действия. При включении устройства производится фотосъемка экрана с содержащимися на нем файлами и папками. Все названия файлов и папок, расположенных на рабочем столе устройства, заносятся в протокол осмотра по порядку. Далее каждая папка детально осматривается, с занесением в протокол всего ее содержимого. Обязательно в протоколе указывается размер каждой папки и файла.

В протоколе осмотра указывается список контактов, время и дата осуществления звонков, номера телефонов абонентов, с которыми происходило соединение абонента, длительность разговоров. Если это SMScообщение, то указывается его полное текстовое содержание, время доставления.

Так как компьютерная техника и мобильное устройство это довольно таки сложное достижение современной информационной среды, при визуальном ее осмотре невозможно увидеть всю ту информацию, которая на ней содержится. Так, эти устройства обладают способностью хранить в себе всю информацию, которая когда-либо на них имелась и удалялась. У экспертов в специализированных лабораториях имеется специальное оборудование, которое позволяет восстановить все удаленные или скрытые файлы, содержащиеся на компьютерном или мобильном устройстве. В связи с этим, следователям, занимающимся расследованием преступлений, связанных с хищением денежных средств в сфере компьютерной информации, рекомендуется назначать компьютерные экспертизы, которые дадут более детальное описание содержимого осматриваемого устройства.

Хотелось бы отметить, что доступ к информации в современных мобильных устройствах сотовой связи, компьютерах, ноутбуках ограничивается их законными пользователями с помощью паролей. Если в ходе оперативно-розыскных или следственных мероприятий такой пароль выяснить удалось, то осмотр устройства следователь может провести без особых проблем. Если же владелец отказывается сообщить пароль и какимлибо другим путем установить его не представляется возможным, то следует помнить, что в экспертных учреждениях существуют специальные устройства, которые позволяют войти в операционную систему такого устройства, минуя пароль, либо «взломав» его[1].

4. Выемка (в том числе электронных носителей информации, электронной почтовой корреспонденции). Выемка производится в том случае, когда у следователя имеется достоверная информация о том, что в определенном месте находятся имеющие значение для расследуемого дела предметы, документы, электронная корреспонденция, электронные носители информации и т.д. Если необходимые документы и предметы содержат государственную или иную охраняемую федеральным законом тайну, а также информацию о вкладах и счетах граждан в банках и иных кредитных организациях, в этом случае следователь подготавливает ходатайство в суд о получении разрешения на выемку таких предметов и документов. В рассматриваемой нами категории преступлений основными предметами выемки будут являться компьютерная техника, либо электронные носители информации, поэтому целесообразно использовать помощь специалиста при проведении данного следственного действия. В качестве специалиста в указанном случае можно пригласить любое лицо, обладающее знаниями в области компьютерных технологий, и имеющее документальное подтверждение своей квалификации.

[1] Скобелин, С.Ю. Юридическая основа и процессуальное оформление извлечения и анализа данных из мобильных устройств [Текст] / С.Ю. Скобелин // Расследование преступлений: проблемы и пути их решения: Сборник научно-практических трудов. Вып. 1. М.: Буки Веди, 2013. С. 183.

Определенную специфику по преступлениям, связанным с хищением денежных средств в сфере компьютерной информации, представляет производство выемки электронной почтовой корреспонденции. Выемка указанной корреспонденции производится только на основании судебного решения. Поскольку такая корреспонденция охраняется законом как тайна связи[1].

Перед проведением выемки, необходимо тщательно спланировать производство следственного действия. Необходимо учитывать, что при вынесении постановления о выемке нельзя указывать в качестве изымаемых неопределенные объекты, документы, стоит конкретизировать, что вы хотите изъять.

Изъятые в ходе выемки носители электронной информации упаковываются таким образом, чтобы исключить возможность доступа к изъятым предметам, документам и обеспечить сохранность имеющейся на них информации. Достижения компьютерных технологий настолько велики, что, даже находясь на расстоянии можно уничтожить находящуюся на устройстве информацию, путем удаленного доступа.

5. Допрос (потерпевшего, свидетеля, эксперта, специалиста, подозреваемого, обвиняемого).

Допросы потерпевшего и свидетеля по преступлениям, связанным с хищением денежных средств, совершенным с использованием компьютерной информации будут включать практически один и тот же перечень вопросов, подлежащих выяснению:

- каким способом произошло завладение компьютерной информацией;

- не проявлял ли кто-либо интереса к компьютерной информации, программному обеспечению, компьютерной технике данной организации;

[1] Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» ст. 63 [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа:www.pravo.gov.ru.

- не присутствовал ли кто-либо из посторонних лиц в помещении, где находится компьютерная техника, с которой осуществляется доступ к охраняемой информации;

- не было ли сбоев в работе компьютерных программ или пропажи носителей компьютерной информации;

- каким образом осуществляется защита компьютерной информации, методы и средства;

- проверяются ли программы на наличие вирусов и как часто;

- как часто происходит обновление программного обеспечения, где оно приобретается и кто его обновляет;

- каков порядок работы с компьютерными программами, как она обрабатывается и передается;

- кто еще подключен к компьютерной сети, каким образом осуществляется доступ в сеть, кто из пользователей имеет право на доступ к сети, каковы их полномочия;

- имелись ли факты несанкционированного доступа к компьютерной информации ранее;

- кто является собственником или законным владельцем компьютерной информации;

Как правило, по указанным делам в качестве свидетелей следует допрашивать лиц различной категории. К ним будут относиться: программисты, оператор ЭВМ, сотрудники службы информационной безопасности, системный администратор, сотрудники вычислительного центра и т.д.[1]

При расследовании уголовного дела о хищении денежных средств в сфере компьютерной информации, специалиста стоит приглашать не только для участия в производстве определенных следственных действий, но и допрашивать его. Специалист может разъяснить не понятные следователю вопросы: в отношении

[1] Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации [Текст]: Учебное пособие / Под ред. проф. Н.Г. Шуруховна. – М.: ЮИ МВД РФ, Книжный мир, 2001. – С. 57.

технических, организационных аспектов компьютерных технологий, особенности функционирования локальных сетей, действия той или иной программы, выхода в «Интернет» и т.д. Также он может расшифровать какие-либо жаргонные понятия характерные для хакеров и геймеров. Своего рода специалист будет выступать в качестве переводчика следователю с кибернетического языка на общедоступный.

Допрос эксперта, как правило, проводится для разъяснения следователю данного им заключения. Так как одной из назначаемых экспертиз, является компьютерная, в ходе допроса эксперта нужно раскрыть сущность отдельных технических терминов, содержащихся в заключении.

Планируя допрос подозреваемого, обвиняемого, следует тщательно к нему подготовиться, так как преступления в сфере компьютерной информации достаточно сложный состав, имеющий свою специфику и требующий определенных специальных познаний. В первую очередь необходимо детально изучить личность подозреваемого, обвиняемого. Проконсультироваться и допросить специалиста для того, чтобы иметь представление о принципе работы определенных программ, обозначении тех или иных компьютерных терминов. Целесообразно также привлекать специалиста к проведению следственного действия «допрос подозреваемого», с целью расшифровки указанных терминов подозраеваемым. Если подозреваемый, обвиняемый идет на контакт и дает показания, необходимо у него выяснить, какие изменения им были внесены в программу, какой вирус им был использован для несанкционированного доступа в систему. Действовал он один или с кем-то, кому передавалась информация[1]?

Для того, чтобы допрос подозреваемого, обвиняемого был успешным, следователю необходимо изучить все материалы уголовного дела, все возможные доказательства имеющиеся в деле прямо или косвенно указывающие на виновность лица.

[1] Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р. Криминалистика [Текст]: Учебник для вузов. / Под ред. заслуженного деятеля науки Российской Федерации, профессора Р.С. Белкина. – М.: Издательство НОРМА (Издательская группа НОРМАИНФРА М), 2002. – С. 960.

6. Получение информации о соединениях между абонентами и (или) абонентскими устройствами. Информацией о соединениях между абонентскими устройствами по рассматриваемой категории преступлений будет являться интервалы подключений к сети Интернет, сведения об IPадресах. Лицо, производящее расследование по уголовному делу, на основании имеющихся достаточных данных, с согласия руководителя следственного органа, обращается с ходатайством в суд на получение детализации соединений интересующего абонента (потерпевшего, подозреваемого, свидетеля). После чего, если судом вынесено положительное решение, следователь производит выемку необходимой детализации в компании сотовой связи. Далее, на основании ч. 4 ст. 21 УПК РФ, следователь имеет право обратиться к операторам сотовой связи с запросом для получения справочной информации о данных абонента, звонившего потерпевшему. Затем следователь обращается в суд с ходатайством, согласованным с руководителем следственного органа, на получение сведений о соединении абонента, потенциально являющегося подозреваемым, с указанием точного географического положения мобильного устройства, IPадреса, GPRS-устройства, с использованием которого было совершено преступление, на момент его соединения с потерпевшим. После чего, производит их выемку в компании сотовой связи. Информация, полученная таким путем, может помочь следователю не только выдвинуть следственные версии, но и установить круг общения подозреваемого, его данные, местоположение, а также возможных соучастников совершенного преступления.

7. Назначение экспертиз. Основная экспертиза, назначаемая по преступлениям указанной категории судебная компьютерно-техническая (далее СКТЭ) - назначается для исследования физического и функционального состояния компьютерных устройств, которыми обеспечены сетевые и телекоммуникационные технологии.

На разрешение экспертам предлагаются следующие типичные вопросы при назначении СКТЭ:

к какому типу (марке, модели) относится аппаратное средство? Каковы его технические характеристики?

каково функциональное предназначение представленного аппаратного средства?

возможно ли использование данного аппаратного средства для решения конкретной задачи?

каково фактическое состояние (исправен, неисправен) представленного аппаратного средства?

является ли неисправность данного средства следствием нарушения правил эксплуатации?

является ли представленное аппаратное средство носителем информации?

какой вид (тип, модель, марку) имеет представленный носитель информации?

какое устройство предназначено для работы с данным носителем информации? Имеется ли в составе представленной компьютерной системы устройство, предназначенное для работы (чтение, запись) с данным носителем информации?

какие параметры имеет носитель информации?

какова общая характеристика представленного программного обеспечения?

к какому виду (общесистемное, прикладное и т. д.) относится представленное программное обеспечение?

каковы реквизиты разработчика, правообладателя представленного программного средства?

каков состав и параметры файлов представленного программного обеспечения?

какое функциональное предназначение имеет программное обеспечение?

имеется ли на электронных носителях информации программное обеспечение для решения конкретной задачи?

какие системы защиты применялись в представленной на экспертизу системе?

имеются ли на представленных компьютерных носителях информации какие-либо средства для осуществления несанкционированного доступа и средства разграничения прав пользователей?

когда и каким образом осуществлялся несанкционированный (и санкционированный) доступ к информации?

имеется ли в представленных на экспертизу программных средствах возможность фальсифицировать или априорно задавать результат работы программы?

каков алгоритм работы представленного программного средства? Подвергалось ли представленное программное средство модификации? В чем это нашло отражение?

имеются ли на представленных образцах с программным обеспечением программы, фрагменты программ, программного обеспечения, свидетельствующие о копировании (полном или частичном) с представленных легитимных образцов?

имеется ли в составе представленного программного обеспечения функции, предназначенные для несанкционированной модификации, уничтожения и распространения информации, нарушения работы аппаратных и программных средств?

какие свойства, характеристики и параметры имеют данные на носителе информации?

к какому типу относятся выявленные данные (текстовые документы, графические файлы и т. д.) и с помощью каких программных средств они могут обрабатываться?

каково содержание обнаруженной информации? какие данные на носителе информации имеют отношение к фактам и обстоятельствам конкретного дела или лица (в том числе и юридического)?

какие данные с представленных на экспертизу образцов и в каком виде находятся на носителе информации?

Подводя итог можно сделать вывод, что перечисленные типичные вопросы формируются с учетом конкретных объектов исследований и складывающейся следственной ситуации. Например, при исследовании мобильных устройств на разрешение эксперту или специалисту могут быть поставлены типовые вопросы общего диагностического характера о наличии в устройстве (включая внешние карты памяти и сим-карты) каких-либо файлов (текстовых, графических, музыкальных, видео, фотофайлов, СМС-сообщений и др.), и эксперт извлекает весь физический носитель памяти. Если же следователя интересует какая-либо конкретная информация, то задаются соответствующие вопросы с указанием временного интервала удаления файлов. Кроме этого, перед назначением экспертизы следователю желательно согласовать перечень вопросов поставленных на исследование, с экспертами, так как некоторые из них могут оказаться не целесообразными или неверно сформулированы.

ЗАКЛЮЧЕНИЕ

На основании исследования по теме: Методика расследования мошенничества, совершенного с использованием средств сотовой связи и сети Интернет можно сделать следующие выводы:

1) В уголовно-правовой характеристики такого вида мошенничества следует выделить, что основным объектом преступления, предусмотренного ст. 159.6 УК РФ признаются отношения собственности. Объективной стороной является хищение чужого имущества или приобретение права на чужое имущество, совершенным вводом, удалением, блокированием, модификацией компьютерной информации либо иное вмешательство в информационную или телекоммуникационную сеть. Субъект преступления – общий, а субъективная сторона – корыстный умысел.

Следует отметить, что на 2018 год существует множество самых разнообразных способов мошенничества с использованием сотовой связи и сети Интернет, что при краже имущество тайно похищается помимо и вопреки воле потерпевшего, при мошенничестве присутствует "добровольная" передача имущества собственником или владельцем преступнику.

2) Подготовкой к совершению преступления, является сбор данных о жертвах, их банковских счетах, социальном положении и т.д. Наиболее опасным и сложным в расследовании способом совершения преступлений является хищение денежных средств, в системе дистанционного банковского обслуживания.

Еще одной особенностью являются место совершения преступления, оно может быть хоть по месту жительства или месту работы, хоть в станции метро, это может быть обычный с виду банкомат или вообще другая страна по средствам сети Интернет. Временем совершения преступления чаще всего является день зарплаты либо крупной сделки потерпевшего.

Личность преступника представляет собой специально обученного человека в области программирования, системного администрирования, автоматизированных систем, которые используются в деятельности определенных отраслей, в частности, банковской, обладать определенным уровнем образования в данных сферах. Кроме того, они владеют определенными навыками и умениями, которые ими используются при работе с компьютерами.

Мошенничество в сети Интернет обладает рядом отличий по сравнению с традиционным мошенничеством. Эти отличия обусловливают особенности расследования данного преступления. В частности, такие особенности проявляются при производстве оперативно-розыскных мероприятий и следственных действий.

3) При использованию средств сотовой связи и компьютерной техники в качестве вещественных доказательств не потребует значительных временных затрат и дополнительных усилий, однако в полной мере будет способствовать качественному и результативному изучению рассматриваемых объектов, что, в свою очередь, позволит получить важные фактические данные и повысить качество доказательственной базы по делу и исключить негативные последствия в виде вынесения решений Европейским Судом по правам человека о неправомерности действий отечественных правоохранительных органов.

4) В настоящее время профилактика и предупреждение телефонных мошенничеств, приобретают все большую актуальность. В своей преступной деятельности мошенники охватывают широкий круг лиц, но все же, чаще всего жертвами становятся люди пенсионного (пожилого) возраста.

Дознаватель в ходе досудебного производства по уголовному делу на основании части второй статьи 158 (Окончание предварительного расследования) УПК РФ и требований приказа МВД России от 19.01.2006 № 19 «О деятельности органов внутренних дел по предупреждению совершения преступлений» обязан выявлять причины и условия, способствовавшие совершению преступления, и

направлять соответствующие представления в организации или должностным лицам для их устранения.

При выполнении мероприятий профилактического характера дознавателю, также целесообразно использовать не процессуальные формы профилактики - выступления в печатных изданиях, на радио, телевидении, выступления в учебных и трудовых коллективах, а также использовать современное средство информации – Интернет.

5) Особенности рассмотрения заявления (сообщения) о преступлении по факту мошенничества с использованием мобильных средств связи определены спецификой способов совершения, данного вида преступления и перечисления полученных денежных средств на счет совершившего преступное деяние лица.

Подводя итог, следует отметить, в большинстве случаев, мошенникам удается ввести в заблуждение граждан из-за, излишней доверчивости, отсутствия осторожности при общении с незнакомцами, нехватки опыта в пользовании интернет-магазинов и приложений на телефонах, которые тем или иным образом касаются перевода денежных средств.

Мошенники разбираются в психологии, и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении. Чаще всего в сети телефонных мошенников попадаются пожилые люди или доверчивые подростки. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности. Мошенничество с использованием средств телефонной связи является единственным видом мошенничества, случаи которого увеличиваются с каждым годом. Основная доля потерпевших проживают в других городах Российской Федерации, и это намного осложняет работу полицейских. Львиная доля преступлений совершается из мест лишения свободы, к тому же этот вид преступности оказывает сильное влияние на наркотизацию общества в целом.

Основная проблема, связанная с выявлением телефонных мошенничеств, заключается в нежелании граждан сотрудничать с правоохранительными

органами. Обычно мошенники требуют небольшие суммы, из-за которых обманутые люди не хотят обращаться в правоохранительные органы. Некоторые не обращаются, потому что считают, что виноваты во всем сами.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Нормативно-правовые акты

1.1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа:www.pravo.gov.ru.

1.2. Уголовный кодекс Российской Федерации (принят Государственной Думой 24.05.1996 г.) (в редакции федеральных законов от 23.04.2019 № 65-ФЗ) [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа:www.pravo.gov.ru.

1.3. Уголовно-процессуальный кодекс Российской Федерации (принят Государственной Думой 22.11.2001 г.) (в редакции федеральных законов от 01.04.2019 № 46-ФЗ) [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа:www.pravo.gov.ru.

1.4. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 28.12.2016) [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru). – Режим доступа: www.pravo.gov.ru.

2. Научная и учебная литература

2.1. Алпатов, А.С. Мошенничество и причинение имущественного ущерба путем обмана или злоупотребления доверием [Текст] / А.С. Алпатов // Трибуна молодого ученого. – 2016. – № 2. – С. 16-37.

2.2. Антонов, А.М. Безопасность применения банкоматов и предупреждение мошенничества с банковскими картами [Текст] / А.М. Антонов // Вестник Волжского университета им. В.Н. Татищева. – 2016. – № 6. – С. 32-41.

2.3. Антошина, С.М. Мошенничество в современных телекоммуникациях [Текст] / С.М. Антошина // История и право. – 2016. – № 3. – С. 12-27.

2.4. Багера, И.Н. Некоторые элементы криминалистической характеристики преступлений, совершаемых с использованием средств сотовой связи [Текст] / И.Н. Багера // Известия Юго-Западного государственного университета. – 2016. – № 4. – С. 88-95.

2.5. Баранов, И.Р. Виды телекоммуникационного мошенничества [Текст] / И.Р. Баранов // Вестник Владимирского юридического института. – 2015. – № 2. – С. 218-243.

2.6. Батоев, В.Б. Обстановка преступлений в сфере мобильных телекоммуникаций [Текст] / Д.В. Петров // Евразийская адвокатура. – 2016. – № 4. – С. 27-38.

2.7. Власова, И.Р. Наиболее распространенные приемы телефонного мошенничества [Текст] / И.Р. Власова // Вестник Владимирского юридического института. – 2015. – № 3. – С. 21-47.

2.8. Волченкова, Л.М. Информационная система определения мошенничества [Текст] / Л.М. Волченкова // Проблемы правоохранительной деятельности. – 2017. – № 2. – С. 15-21.

2.9. Гавло, М.С. Социально-экономическая обусловленность дифференциации уголовной ответственности за мошенничество в уголовном законодательстве России [Текст] / М.С. Гавло // Ученые труды Российской академии адвокатуры и нотариата. – 2016. – № 4. – С. 16-32.

2.10. Гончарова, А.В. Обеспечение безопасности мобильных устройств [Текст] / А.В. Гончарова // Вестник Владивостокского государственного университета экономики и сервиса. – 2017. – № 1. – С. 32-46.

2.11. Гусев, В.Н. Вопросы обеспечения телефонной безопасности [Текст] / В.Н. Гусев // Вестник Казанского юридического института МВД России. – 2015. – № 2. – С. 34-42.

2.12. Зверев, А.И. Проблемы расследования преступлений, связанных с мошенническими действиями, совершенных с использованием средств сотовой телефонной связи [Текст] / А.И. Зверев // Правозащитник. – 2016. – № 5. – С. 14-19.

2.13. Иванников, Г.И. Актуальные вопросы правового обеспечения деятельности оперативных аппаратов по раскрытию телефонного мошенничества [Текст] / Г.И. Иванников // Правовая информатика. – 2016. – № 1. – С. 7- 16.

2.14. Изотов, Р.В. О некоторых вопросах квалификации действий лиц, совершивших кражу денежных средств с использованием системы дистанционного банковского обслуживания "Мобильный банк" [Текст] / Р.В. Изотов // Университет им. В.И. Вернадского. Специальный выпуск. – 2016. – № 38. – С. 33-51.

2.15. Качмазов, Г.А. Совершение мошенничества в отношении граждан при помощи средств сотовой связи: проблемы практики [Текст] / Г.А. Качмазов // Бизнес в законе. – 2015. – № 1. – С. 191-215.

2.16. Кириллов, И.С. Проблемы выявления телефонного мошенничества [Текст] / И.С. Кириллов // Современное право. – 2017. – № 2. – С. 13-25.

2.17. Королев, Н.В. Мошенничество с помощью мобильного телефона в контексте теории фреймов [Текст] / Н.В. Королев // Право и жизнь. – 2016. – № 6. – С. 32-41.

2.18. Красников, А.П. Отличие мошенничества от смежных преступлений: проблемы квалификации [Текст] / А.П. Красников // Вестник университета имени О.Е. Кутафина (МГЮА). – 2014. – № 1. – С.31-48.

2.19. Кузнецов, А.Л. Эвристические признаки Bluetooth-вирусов для мобильных устройств [Текст] / А.Л. Кузнецов // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2016. – № 9. – С. 12-23.

2.20.Кулев А.С. Телефонное мошенничество [Текст] / А.С. Кулев // Российская юстиция. – 2016. – № 5. – 45-63.

2.21.Лабутин, В.Н. Мошенничества и аферы с сотовыми телефонами / В.Н. Лабутин // Юрист и право. – 2017. – № 1. – С. 21-35.

2.22.Лазарев, С.В. Способы совершения мошенничества в отношении граждан [Текст] / С.В. Лазарев // Вестник Уральского юридического института МВД России. – 2016. – № 11. – С. 15-42.

2.23.Мазера, В.Н. Связь в северных регионах Российской Федерации [Текст] / В.Н. Мазера // Вестник Томского государственного университета. – 2016. – № 10. – С. 28-37.

2.24.Маркелова, А.С. Схемы мошенничества в Интернет и по мобильной связи [Текст] / А.С. Маркелова // Вестник Казанского юридического института МВД России. – 2015. – № 6. – С. 44-63.

2.25.Мартынов, А.В. Киберпреступность как новая криминальная угроза [Текст] / А.В. Мартынов // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2016. – № 1. – С. 164-178.

2.26.Мартынова, Г.И. Особенности профессиональной деятельности следователя [Текст] / Г.И. Мартынова // Правовая информатика. – 2017. – № 5. – С. 17- 25.

2.27.Миненко, К.В. Алгоритм действий следователя и органа дознания при расследовании мошенничеств с использованием средств сотовой связи [Текст] / К.В. Миненко // Адвокат и право. – 2016. – № 9. – С. 23-41.

2.28.Никитина, Ю.Г. Организационно и правовое и информационное обеспечение расследования преступлений, совершаемых с использованием средств мобильной связи [Текст] / Ю.Г. Никитина // Вестник Нижегородского государственного университета им. Н.И. Лобачевского. – 2016. – № 6. – С. 257-262.

2.29.Новикова, А.А. Новые способы совершения преступлений в сфере сотовой связи [Текст] / А.А. Новикова // Актуальные проблемы экономики и права. – 2017. – № 1. – С. 38-52.

2.30.Обухова, Ю.О. Мошенничество при помощи SMS-сообщений [Текст] / Ю.О. Обухова // Вестник Воронежского института МВД России. – 2016. – № 3. – С. 6- 25.

2.31.Пашнев, С.Б. Мошенничество и причинение имущественного ущерба путем обмана или злоупотребления доверием: сравнительно-правовой анализ [Текст] / С.Б. Пашнев // Вестник Чувашского университета. – 2014. – № 3. – С. 57-73.

2.32.Поляков, М.Б. Опасности, возникающие в повседневной жизни и безопасное поведение [Текст] / М.Б. Поляков // Российский юридический журнал. – 2016. – № 2. – С. 66-74.

2.33.Ревина, Н.Н. Финансовое мошенничество в сети Интернет [Текст] / А.В. Ревина // Вестник Владивостокского государственного университета экономики и сервиса. – 2016. – № 2. – С. 66-75.

2.34.Розенцвайг, В.Б. Признаки телефонного мошенничества [Текст] / В.Б. Розенцвайг // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2016. – № 2. – С.22-38.

2.35.Ростокинский, В.А. Угрозы безопасности мобильных платформ и практические пути их разрешения [Текст] / В.А. Ростокинский // Вестник Санкт Петербургской юридической академии. – 2016. – № 3. – С. 49-57.

2.36.Силантьева, В.П. Механизмы привлечения к уголовной ответственности за телефонное мошенничество [Текст] / В.П. Силантьева // Учёные труды Российской академии адвокатуры и нотариата. – 2016. – № 7. – С. 7-24.

2.37.Смирнова, В.А. Индустрия мобильного вредоносного программного обеспечения [Текст] / В.А. Смирнова // Вестник Воронежского института МВД России. – 2015. – № 2. – С. 16-24.

2.38.Сомова, Д.В. Телефонные пираты [Текст] / Д.В. Сомова // Бесплатная юридическая помощь: зарубежный и российский опыт. – 2016. – С. 15-21.

2.39.Старшинский, Р.Г. Телефонное мошенничество: вопросы теории и практики [Текст] / Р.Г. Старшинский // Российская юстиция. – 2016. – № 4. – С. 24-31.

2.40.Степанов, А.А. К вопросу об особенностях раскрытия и расследования преступлений, связанных с использованием средств сотовой связи [Текст] / А.А. Степанов // Вестник Восточно-Сибирского института МВД России. – 2015. – № 1. – С. 12-19.

2.41.Сугробов, Л.А. "Мобильные" мошенничества: основные способы совершения [Текст] / Л.А. Сугробов // Адвокат. – 2014. – № 8. – С. 39-48.

2.42.Теплова, А.Н. Способы совершения мошенничества в отношении граждан [Текст] / А.Н. Теплова // Мониторинг правоприменения. – 2017. – № 2. – С. 54- 67.

2.43.Тропина, Н.В. Особенности современной криминальной ситуации, связанной с рецидивом корыстных преступлений [Текст] / Н.В. Тропина // Актуальные проблемы гуманитарных и естественных наук. – 2016. – № 3. – С. 198-211.

2.44.Тюлеева, О.В. Проблемы квалификации мошенничества в сфере компьютерной информации [Текст] / О.В. Тюлеева // Современное право. – 2016. – № 4. – С. 48-57.

2.45.Фекленко, М.Г. Рекомендации правоохранительных органов для защиты от телефонных мошенников [Текст] / М.Г. Фекленко // Вестник Балтийского федерального университета им. И. Канта. – 2016. – № 9. – С. 157-164.

2.46.Филиппов, С.А. Телефонные мошенничества (предупреждает управление "к" МВД России) [Текст] / С.А. Филиппов // Национальные интересы: приоритеты и безопасность. – 2016. – № 12. – С. 16-24.

2.47.Хасанов, А.А. Использование криминалистического компьютерного моделирования при планировании расследования преступлений [Текст] / А.А. Хасанов // Адвокат. – 2016. – № 8. – С. 15-24.

2.48.Шаззо, Л.К. Некоторые особенности мошенничества, совершаемого в сфере и с использованием высоких технологий [Текст] / Л.К. Шаззо // Право и жизнь. – 2016. – № 6. – С. 32-41.

2.49.Шалимов, О.Н. Проблемы безопасности электронной коммерции в сети Интернет [Текст] / О.Н. Шалимов // Вестник Томского государственного университета. – 2016. – № 1. – С. 16-32.

2.50.Яджин, А.В. Проблемы рисков в системе электронных денег [Текст] / А.В. Яджин // Вестник Новгородского государственного университета им. Ярослава Мудрого. – 2016. – № 8. – С. 52-74.

2.51 Яджин Н. В., Егоров В. А. Некоторые элементы криминалистической характеристики преступлений, совершаемых с использованием средств сотовой связи [Текст] / Н.В. Яджин, В.А. Егоров // Научно-методический электронный журнал «Концепт». – 2014. – № 29. – С. 56–60.

3. Материалы правоприменительной практики

3.1. Постановление Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс] // Официальный интернет-портал правовой информации (www.pravo.gov.ru).– Режим доступа: www.pravo.gov.ru.

3.2. Справка Камчатского краевого суда [Электронный ресурс] // Официальный сайт Камчатского краевого суда (oblsud.kam.sudrf.ru). – Режим доступа: oblsud.kam.sudrf.ru