Краснодарский университет МВД России

А. А. Рясов

МЕТОДИКА РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Учебное пособие

Краснодар
2021

ББК 67.52
УДК 343.98
Р 997

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Рецензенты:
О. А. Анопко (Следственная часть по расследованию организованной преступной деятельности ГУ МВД России по Ставропольскому краю);
С. А. Лубин, кандидат юридических наук, доцент (Нижегородская академия МВД России).

Рясов А. А.
Р 997 Методика расследования мошенничества в сфере компьютерной информации : учебное пособие / А. А. Рясов. – Краснодар : Краснодарский университет МВД России, 2021. – 48 с.

ISBN 978-5-9266-1796-9

В учебном пособии содержится криминалистическая характеристика и особенности расследования мошенничества в сфере компьютерной информации. Материал является базовым для профессиональной подготовки сотрудников правоохранительных органов, расследующих правонарушения в сфере компьютерной информации.

Пособие предназначено для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России, сотрудников органов внутренних дел Российской Федерации.

ББК 67.52
УДК 343.98

ISBN 978-5-9266-1796-9

Введение

В реалиях сегодняшнего дня ежегодно повышается объем информации, хранящейся и обрабатываемой компьютерными системами. С одной стороны, данное обстоятельство несет в себе позитивную составляющую. Этот процесс позволяет ускорить социально-экономические преобразования, происходящие в современном мире, а также увеличить скорость информационного обмена между различными государственными и частыми структурами. В настоящее время мобильные банки и переводы стали частью нашей жизни и сейчас уже невозможно себе представить нашу жизнь без компьютеров, смартфонов и прочих электронных гаджетов. С другой стороны, там, где есть деньги, всегда найдутся те, кто захочет их украсть. Поэтому оборотной стороной данного процесса стало появление киберпреступности. «Так, экономике России действиями киберпреступников разного уровня нанесен ущерб в 203,3 млрд рублей, что равно 0,25 % объема ВВП, в 2015 г. прямой финансовый ущерб составил 123,5 млрд рублей (0,15% от ВВП), а затраты на ликвидацию последствий более – 79,8 млрд рублей (0,1% от ВВП). Такие сведения опубликованы в совместном исследовании Group-IB, Фонда развития интернет-инициатив (ФРИИ) и Microsoft. В течение четырех кварталов, со II квартала 2015 г. по I квартал 2016 г., киберпреступники украли около 5,5 млрд рублей, что на 44 % больше похищенного за предыдущий отчетный период, сделала вывод Group-IB в исследовании»[1].

«Ущерб от киберпреступлений в России только за 2019 г. превысил 10 млрд рублей. Каждое седьмое преступление совершается при помощи IT-технологий. Об этом заявил начальник Главного управления экономической безопасности и противодействия коррупции МВД России генерал-лейтенант полиции Андрей Курносенко»[2].

Одним из наиболее опасных видов киберпреступлений является мошенничество.

В соответствии с данными, предоставленными Генеральной прокуратурой РФ, количество преступлений, совершенных в форме мошенничества (ст. 159–159.6 Уголовного кодекса Российской Федерации), по сравнению с аналогичным периодом прошлого года увеличилось на 19,6 % и составило 257 187 преступлений. Возросло на 12,1 % число предварительно расследованных преступлений данного вида, составив 64 378 деяний, из которых 47 869 (+6,3 %) уголовных дел направлены в суд. Наибольший рост мошенничеств наблюдается в г. Москве (на 4 895; +20,1 %), Ростовской области (на 3 509; +59,2 %), Краснодарском крае (на 2 869; +26,5 %),

[1] URL: http://www.kubsau.ru/upload/iblock/5d4/5d4cf06fde9e804c3fd0d2c98eebc08c.pdf (дата обращения: 02.01.2018).

[2] URL: https://rg.ru/2019/12/10/mvd-ushcherb-ot-kiberprestuplenij-prevysil-10-milliardov-rublej.html (дата обращения: 02.03.2020).

Республике Татарстан (на 1 785; +30,8 %), Ставропольском крае (на 1 777; +35,6 %)[1].

В настоящее время в электронной среде сосредоточено огромное количество информации, в том числе персональной, о действиях различных организаций и граждан, об их перемещениях, сделках, о банковских и иных финансовых операциях, имеющемся в их распоряжении движимом и недвижимом имуществе и т. д. Развитие компьютеризации общества и появление электронных баз данных, с одной стороны, способствуют процессу развития общества в целом. Однако, с другой стороны, эти же процессы открывают большую возможность для преступников, которые, подключаясь к компьютерным сетям, совершают преступления, находясь на большом удалении от своей жертвы, что значительно затрудняет выявление и расследование таких преступлений и повышает уровень их латентности.

Таким образом, в России возникла необходимость принятия соответствующих мер, которые позволят эффективно противодействовать мошенническим действиям, совершаемым в сфере компьютерной информации. Президент РФ В. Путин в ходе выступления на расширенном заседании Генеральной прокуратуры Российской Федерации (16 марта 2020 года) поручил разработать комплекс мер по борьбе с киберпреступностью»[2].

С этой целью 23.11.2012 Государственной думой был принят Федеральный закон №207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», которым мошенничество в сфере компьютерной информации было выделено в самостоятельную норму – ст. 159.6. Мошенничество в сфере компьютерной информации.

Введение данной нормы не решило проблемы расследования данного вида преступлений, и необходимо понимать, что эффективной борьба с мошенничеством в сфере компьютерной информации будет возможной только при достаточном вооружении правоохранительных органов научными положениями и разработанными на их основе практическими рекомендациями по расследованию данного вида преступлений. На сегодняшний день серьезных научных разработок по данному вопросу нет. Практическим работникам приходится пользоваться рекомендациями по расследованию компьютерных преступлений, которые имеют другую специфику и, кроме того, несут в себе тенденцию к ежегодному устареванию. Данное обстоятельство не может не оказывать отрицательного влияния на качество расследования мошенничества в сфере компьютерной информации.

---

[1] Состояние преступности в России за январь–декабрь 2019 г. URL: https://genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf (дата обращения: 02.03.2020).

[2] URL: https://rg.ru/2020/03/17/putin-poruchil-razrabotat-kompleks-mer-po-borbe-s-kiberprestupnostiu.html (дата обращения: 20.03.2020).

Нельзя не отметить в качестве негативного фактора, оказывающего существенное влияние на качество расследования данного вида преступлений, слабую профессиональную подготовку лиц, расследующих данные преступления.

Таким образом, актуальность данного исследования обусловлена, с одной стороны, недостаточной разработанностью отдельных положений методики расследования мошенничества в сфере компьютерной информации, а с другой – ее высокой практической значимостью.

Глава 1. Криминалистическая характеристика мошенничества в сфере компьютерной информации

§ 1. Общая характеристика мошенничества в сфере компьютерной информации

Вопрос о криминалистической характеристике – определении места, значения и роли ее в науке, уже давно является предметом дискуссии многих ученых криминалистов[1] и, несмотря на это, она давно и прочно утвердилась как первый и основной элемент частной криминалистической методики.

Криминалистическая характеристика преступлений представляет собой не что иное, как научную абстракцию, состоящую из познаний о типовой системе признаков, их связях и взаимообусловленностях, что позволяет назвать ее основным понятием и структурным элементом криминалистической методики расследования преступлений. Используя данные, содержащиеся в криминалистической характеристике, в качестве базы криминалисты разрабатывают практические рекомендации по раскрытию, расследованию и предупреждению различных видов преступлений.

В настоящий момент среди ученых продолжается дискуссия о научном значении криминалистической характеристики отдельных видов и групп преступлений, а также о ее значимости при разработке частных методик расследования отдельных видов преступлений[2]. По данному вопросу ученые придерживаются разных мнений, от положительного[3] до резко отрицательного[4]. Так, «Белкин Р.С. в своих последних работах писал, что данная категория, не оправдав возлагавшихся на нее надежд и ученых, и практиков, изжила себя и из реальности превратилась в иллюзию»[5].

Мы не будем сильно углубляться в детали данного спора, так как он не имеет прямого отношения к рассматриваемой нами теме исследования. Однако отметим, что, на наш взгляд, криминалистическая характеристика

---

[1] Криминалистика. Том 1. История, общая и частные теории / под ред. Р.С. Белкина, В.Г. Коломацкого, И.М. Лузгина. М., 1995. С. 63.; См.: Драпкин Л.Я., Карагодин В.Н. Криминалистика: учеб. М., 2007. С. 349; Лавров В.П. Криминалистическая характеристика преступления / под ред. А.Ф. Волынского, В.П. Лаврова. М., 2009. С. 30; Шурухнов Н.Г. Криминалистика: учеб. М., 2004. С. 451.

[2] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 19.

[3] Рубцов И.И. Криминалистическая характеристика преступлений как элемент частных методик расследования: дис. … канд. юрид. наук., СПб., 2017. С. 225.

[4] Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М., 2001. С. 221.

[5] Там же. С. 221.

преступления необходима и должна оставаться в качестве важнейшего системного элемента частной методики расследования любого преступления вследствие того, что она раскрывает взаимосвязь всех элементов, содержащих типичную криминалистически значимую информацию о преступлении.

Рассматривая криминалистическую характеристику на более конкретном примере, применительно к теме нашего исследования, следует сказать, что в условиях недостатка информации на первоначальном этапе расследования большое значение имеет информация общеориентирующего характера, которую мы и можем почерпнуть из типовой криминалистической характеристики мошенничества в сфере компьютерной информации.

Одно из первых упоминаний о криминалистической характеристике преступлений было дано в работах А.Н. Колесниченко[1]. Это послужило отправной точкой разработки данного понятия в криминалистической науке, о чем свидетельствует анализ научной литературы, отражающей различные точки зрения относительно определения данного понятия[2].

Криминалистическую характеристику преступлений зачастую определяют как модель криминальной ситуации и сопутствующих ей обстоятельств, а также последствий преступлений определенного вида (материальных и идеальных следов), механизма противоправного деяния, способа преступления, предмета преступного посягательства. На основе этой модели выдвигаются версии о расследуемом событии в целом или об отдельных его обстоятельствах и прогнозируется тактическая перспектива расследования[3].

Так, В.П. Лавров под криминалистической характеристикой понимает систему сведений о типичных признаках определенной категории преступлений, анализ которых позволяет делать выводы об оптимальных путях их раскрытия и расследования[4].

Нельзя не согласиться с мнением авторов о том, что «криминалистическая характеристика имеет сугубо поисковое, ориентирующее значение.

---

[1] Колесниченко А.Н. Научные и правовые основы расследования отдельных видов преступлений: автореф. дис. ... д-ра. юрид. наук: 12.00.09. Харьков, 1967. С. 10, 14.

[2] Коломинов, В.В. Указ. соч. С. 19.

[3] См.: Митричев С.П. Методика расследования отдельных видов преступлений // Криминалистика и судебная экспертиза. Киев, 1973. № 10. С. 26; Пантелеев И.Ф. Методика расследования преступлений. М., 1975. С. 9–10 ; Танасевич В.Г., Образцов В.А. О криминалистической характеристике преступлений // Вопросы борьбы с преступностью. М., 1976. № 25; Возгрин И.А. Общие положения методики расследования отдельных видов преступлений. Л., 1976. С. 6–9; Криминалистика: учеб. / под ред. Н.П. Яблокова, В.Я. Колдина. М.: Изд-во МГУ, 1990. С. 324; Криминалистика: учеб. / под ред. Р.С. Белкина. М.: НОРМА, 2001. С. 687–688; Шурухнов Н.Г. Криминалистика: учеб. М.: Юристъ, 2003. С. 451.

[4] Лавров В.П. Криминалистика. М.: Норма, 1999. С. 33.

Этому служат статистически определяемые корреляционные связи (вероятностные зависимости) между ее элементами, позволяющие ориентироваться в предмете и направлениях поиска»[1].

Изучив мнения ученых о криминалистической характеристике различных видов преступлений, можно выделить особенности формирования основных элементов криминалистической характеристики расследования мошенничества в сфере компьютерной информации.

Принципиальным для рассмотрения понятия криминалистической характеристики является то, что в нее необходимо включать максимальное число признаков, имеющих криминалистическое значение. Вместе с тем в литературе нет единого мнения о понятии «криминалистическая значимость». Представляется, что им «можно считать фрагменты действительности, которые объективно могут взаимодействовать в рамках его подготовки, совершения и сокрытия, и в силу этого способны отразить криминалистически значимую (а не иную, хотя бы и связанную с преступлением и условиями его расследования) информацию»[2].

Вопрос о количестве обстоятельств, имеющих значение для расследования, зависит от того, насколько они выражены и насколько могут повлиять на другие элементы методики расследования отдельных видов преступлений.

Вместе с тем следует помнить о недопустимости чрезмерного расширения этих элементов путем заимствования их из других разделов криминалистики или даже из других наук, являющихся общеизвестными данными. В противном случае, это может привести к кризису данного понятия, о котором и говорил Р.С. Белкин[3].

Применительно к мошенничеству в сфере компьютерной информации, на наш взгляд, следует выделить элементы криминалистической характеристики, предложенные А.А. Протасевичем и Л.П. Зверянской, которые выделяют их применительно к «киберпреступлениям:

– способ совершения преступления;

– особенности следовой информации;

– особенности обстановки совершения преступления (место совершения преступления, время совершения преступления и др.);

– личностная характеристика преступника;

---

[1] Белкин Р.С. Криминалистическая энциклопедия. 2-е изд. доп. М.: Мегатрон XXI, 2000. С. 103.

[2] Князьков А.С. Тактико-криминалистические средства досудебного производства: дис. ... д-ра юрид. наук: 12.00.12. Томск, 2014. С. 144.

[3] Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М., 2001. С. 221.

– особенности непосредственного предмета преступного посягательства»[1].

Вместе с тем данные элементы следует рассматривать как базисные и нуждающиеся в определенной корректировке применительно к криминалистической характеристике мошенничества в сфере компьютерной информации с учетом специфики данного преступления.

К особенностям рассматриваемых элементов следует прежде всего отнести такие элементы, как орудия и средства совершения преступления; способ совершения мошеннических действий в сфере компьютерной информации; обстановка и место совершения преступлений, их следует изучать во взаимосвязи и взаимообусловленности.

Данные элементы следует выделять вследствие имеющихся особенностей их проявления при совершении изучаемого нами преступления, а также их влиянии на механизм совершения преступления, а отсюда и выбор технологии расследования данного вида преступлений.

Рассмотрение вышеуказанных элементов криминалистической характеристики мошенничества в сфере компьютерной информации следует начать со способов их совершения. Следует согласиться с мнением А.А. Комаровой, которая полагает, что «определяющим признаком любой формы мошенничества является способ совершения преступления: обман или злоупотребление доверием, являющиеся единственным, исключительным способом совершения данного вида преступлений»[2].

Спецификой мошенничества в сфере компьютерной информации является то, что деятельность по сокрытию следов преступления преступники осуществляют уже на этапе подготовки его совершения. С этой целью создаются вредоносные программы, позволяющие предоставлять злоумышленнику удаленный доступ к компьютеру жертвы или получение доступа к мобильному банку, разрабатываются сайты, заходя на которые жертва заражает свой компьютер вирусами, спецификой является также и длительное общение с жертвой с использованием социальных сетей, электронной почты, мессенджеров или телефонной связи и т. п.

В качестве орудий и средств совершения рассматриваемых преступлений выступают компьютерно-технические средства и компьютерные сети.

Анализ следственно-судебной практики, а также научной и нормативно-правовой литературы позволяет констатировать, что единого подхода к классификации способов совершения мошенничества в сфере компьютерной информации не сегодняшний день нет.

---

[1] Айвазова О.В. Криминалистическая характеристика преступлений как систематизированное отражение механизма преступной деятельности: результаты научной полемики // Вестник Томского государственного университета. 2014. № 389. С.153–157.

[2] Комарова А.А. Интернет-мошенничество: проблемы детерминации и предупреждения: монография. М.: Юрлитинформ, 2013. С. 9.

Обусловлено это тем, что в случае использования того или иного способа деяние может быть квалифицировано по другой, нежели мошенничество, статье Уголовного кодекса или их совокупности. Так, например, М.И. Третьяк отмечает, что компьютерное мошенничество является специальным составом к компьютерным преступлениям (ч. 2 ст. 272 и ч. 2 ст. 273 УК РФ) и рассмотренные в законе, теории и практике определения модификации компьютерной информации следует использовать и при характеристике компьютерного мошенничества, однако с учетом того, что в диспозиции ст. 159.6 УК РФ, в отличие от статей гл. 28 УК РФ, термины «удаление (уничтожение)», «блокирование» и «модификация» характеризуют способ компьютерного мошенничества»[1]. Именно такой позиции придерживается Верховный Суд[2].

С учетом вышесказанного, по нашему мнению, невозможно представить исчерпывающий перечень способов совершения мошенничеств в сфере компьютерной информации. Мы понимаем, что такой подход значительно усложняет возможность квалификации преступлений при появлении новых способов мошенничества в сфере компьютерной информации. Тем не менее, другой альтернативы, к сожалению, нет. Свидетельством тому является и аналогичный подход к компьютерным мошенничествам в Конвенции ООН «О преступности в сфере компьютерной информации»[3].

Не смотря на это, попытки классифицировать способы совершения компьютерного мошенничества предпринимались и ранее. Так, например, кодификатор рабочей группы Интерпола в обобщенном виде компьютер-

---

[1] Третьяк М.И. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества // Уголовное право. 2016. № 2. С. 95–101; Третьяк М.И. Проблема законодательной регламентации преступлений против собственности в сфере высоких технологий // Законность. 2016. № 7. С. 41–46.

[2] в п. 12 Постановления Пленума Верховного Суда РФ «О судебной практике по делам о мошенничестве, присвоении и растрате» определил, что в случаях, когда указанные деяния сопряжены с неправомерным внедрением в чужую информационную систему или с иным неправомерным доступом к охраняемой законом компьютерной информации кредитных учреждений либо с созданием заведомо вредоносных программ для электронно-вычислительных машин, внесением изменений в существующие программы, использованием или распространением вредоносных программ для ЭВМ, содеянное подлежит квалификации по ст. 159 УК РФ, а также, в зависимости от обстоятельств дела, по ст. 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.

[3] в ст. 8 которой определено, что для того чтобы квалифицировать в качестве уголовных преступлений, согласно ее внутригосударственному праву, в случае совершения преднамеренно и без права на это лишения другого лица его собственности путем: а) любого ввода, изменения, удаления или блокирования компьютерных данных; б) любого вмешательства в функционирование компьютерной системы, мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.

ные мошенничества предлагает определять и классифицировать следующим образом:

– компьютерные мошенничества, связанные с хищением наличных денег из банкоматов;

– компьютерные подделки: мошенничества и хищения из компьютерных систем путем создания поддельных устройств;

– мошенничества и хищения, связанные с игровыми автоматами;

– манипуляции с программами ввода-вывода: мошенничества и хищения посредством неверного ввода в компьютерные системы или вывода из них путем манипуляции программами;

– компьютерные мошенничества и хищения, связанные с платежными средствами;

– телефонное мошенничество: доступ к телекоммуникационным услугам путем посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы[1].

Новые способы совершения компьютерных мошенничеств появляются ежедневно, постоянно модернизируются и изменяются, что и делает невозможным их полное перечисление. Однако отдельные авторы предпринимают попытки разделить их на определенные типы. Согласно основным направлениям мошеннической деятельности А.А. Комарова выделяет следующие их типы:

1. Виртуальный товарообмен.
2. Легкие деньги.
3. Лже-благотворительность.
4. Мошенничество в сфере интернет-знакомств.
5. Телеработа, удаленный заработок.
6. Мошенничество в сфере услуг.
7. Инвестиционное мошенничество.
8. Компьютерное мошенничество[2].

Подобные типологии нельзя признать исчерпывающими вследствие проявления чудес изобретательности компьютерных мошенников по созданию все новых и новых их способов. Тем не менее, именно способы совершения мошенничеств становятся основанием для их классификации.

Невозможно представить себе рассмотрение криминалистической характеристики любого преступления без изучения механизма следообразования. Не является исключением и рассматриваемое нами преступление. Именно данный механизм является главной особенностью, отличающей мошенничество в сфере компьютерной информации от других видов мо-

[1] См.: Вопросы международного сотрудничества в борьбе с компьютерными преступлениями. URL: crime-research.ru/news (дата обращения: 17.04.2014).

[2] Комаров А.А. Интернет-мошенничество: проблемы детерминации и предупреждения. М.: Юрлитинформ, 2013. С. 31–32.

шенничеств. Информация о преступном событии, содержащаяся в следах совершения данного вида преступлений, представляет собой особую категорию. Для того чтобы оценить относимость выявленных следов по компьютерным мошенничествам, следует подвергнуть их глубокому анализу не только с технической точки зрения, с использованием специальных познаний, но путем определения их связи с совершенным преступлением, установлением являются ли они предметом доказывания, а также соотнесения их с имеющимися версиями по данному преступлению. При этом очень важно проконтролировать целостность компьютерной информации, не допустить ее изменения.

Оценка достоверности полученных доказательств состоит в анализе всех этапов процесса образования компьютерной информации. К таковым следует отнести условия их возникновения, обнаружения, фиксации и сохранения.

В связи с этим, на наш взгляд, представляется интересным мнение отдельных ученых по модернизации устоявшейся в трасологии классификации следов по их материальному состоянию.

Обоснованием для такой классификации служит специфичность следов, оставляемых при совершении компьютерных мошенничеств. Дело в том, что устоявшаяся система классификации следов на материальные и идеальные не может в себя включить следы, остающиеся в памяти электронных устройств, облачных хранилищ, электронных сетей и т.д. В связи с этим некоторые авторы предлагают ввести в трасологии новую группу следов – виртуальные следы[1]. Под виртуальными следами В.А. Мещеряков предлагает понимать «любое изменение состояния автоматизированной информационной системы, связанное с событием преступления и зафиксированное в виде компьютерной информации. Данные следы занимают условно промежуточную позицию между материальными и идеальными следами»[2].

Противники данной позиции аргументируют свое мнение тем, что «понятие «виртуальный» – устоявшийся термин, применяющийся в квантовой теории поля для характеристики частиц, находящихся в промежуточном состоянии или в состоянии неопределенности (координаты которых и сам факт их существования в данный момент времени можно назвать лишь с определенной долей вероятности). В таком смысле будет

[1] См.: Мещеряков В.А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Изд-во Воронеж. гос. ун-та, 2002. С. 94–119; Краснова Л.Б. Компьютерные объекты в уголовном процессе и криминалистике: автореф. дис. ... канд. юрид. наук. Воронеж, 2005. С. 15–17; Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. ... канд. юрид. наук. Омск, 2008. С. 13.

[2] Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. ... доктора юрид. наук. Воронеж, 2001. С. 33.

понят термин «виртуальный след» любым человеком, знакомым с этим понятием»[1]. Тем не менее, использование данного понятия в физике имеет узко-специфическую сферу применения. В то время как основная масса людей вкладывает совершенно иной смысл в данный термин. Виртуальный – «не существующий в действительности, но появляющийся благодаря программному обеспечению»[2].

«Как справедливо отмечает А.Г. Волеводз, изучая вопросы следообразования в компьютерных сетях, можно с уверенностью констатировать, что при расследовании преступлений, совершаемых с использованием компьютерных сетей, могут использоваться их следы, представляющие собой сведения о прохождении информации по проводной, радио-, оптической и другим электромагнитным системам связи (электросвязи), которые носят обобщенное название «сведения о сообщениях, передаваемых по сетям электрической связи (электросвязи)», либо сохраняемые поставщиками услуг (провайдерами) «исторические данные» о состоявшихся сеансах связи или переданных сообщениях, либо «данные о потоках» или «данные о потоках информации»[2]. Указанную систему образования следов следует положить в основу разработки системы и последующей дифференциации следов компьютерных преступлений, в том числе рассматриваемого нами мошенничества в сфере компьютерной информации»[3].

Следует согласиться с мнением ученых, отмечающих специфическое отличие данных следов: «они не имеют геометрической формы, цвета, запаха и иных характеристик, традиционно рассматриваемых криминалистикой, в которых могли бы отразиться отельные черты преступника, например, его ДНК, запах, папиллярный узор и т. д.»[4].

Следует отметить, что в литературе встречаются и другие предложения по названию данных следов. Так, Г.Г. Камалов называет их информационными[5]. На наш взгляд, такое предложение является спорным, так как любые следы несут в себе информацию и в этом смысле все следы можно называть информационными.

Кроме того, в криминалистической литературе отдельные авторы предлагают термин «бинарные следы». В качестве обоснования они отмечают, «что изменения в компьютерной информации, являющиеся следами преступления, в подавляющем большинстве случаев доступны восприятию

---

[1] Черкасов В.Н., Нехорошев А.Б. Кто живет в «киберпространстве»? // Управление защитой информации. 2003. Т. 7. № 4. С. 468.

[2]URL:https://ru.wikipedia.org/wiki/%D0%92%D0%B8%D1%80%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%8C.;

[3] Коломинов В.В. Указ. соч. С. 33.

[4] Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений // Доклады ТУСУРа. 2014. № 2 (32). С. 162–166.

[5] Камалова Г.Г. Криминалистическая методика расследования преступлений в сфере компьютерных технологий // Криминалистика: курс лекций для бакалавров / под ред. М.К. Каминского, А.М. Каминского. Ижевск, 2012. С. 303.

не в виде двоичных кодов (что собственно и представляет собой бинарный след), а в преобразованном виде: запись в файле реестра, изменение атрибута файла, электронном почтовом сообщении»[1].

Другим немаловажным элементом криминалистической характеристики мошенничеств, совершенных в сфере компьютерной информации, является место совершения преступления.

Место преступления в криминалистике традиционно определяется как место, в котором реализуется объективная сторона преступления»[2]. Именно место совершения преступления влияет на формирование следовой картины по рассматриваемому преступлению. Само по себе оно может быть носителем различных следов, а, следовательно, оказывает влияние на весь процесс расследования.

В этой связи при совершении компьютерных мошенничеств может быть не одно, а несколько мест происшествий.

По итогам данного параграфа можно сделать вывод о том, что криминалистическая характеристика мошенничества в сфере компьютерной информации представляет собой обобщенное описание системы криминалистически значимой информации о признаках и свойствах преступления, предусмотренного ст. 159.6 УК РФ, состоящее из определенного множества элементов, таких как: непосредственный предмет преступного посягательства; способ совершения преступления, орудия и средства преступления; следы и механизм следообразования; обстановка совершения преступления, его пространственно-временной континуум, которые, в свою очередь, характеризуются корреляционной зависимостью между собой и специфичностью проявлений во внешней среде (киберпространстве) [3].

Также следует констатировать, что на сегодняшний день в криминалистике нет единой системы знаний о виртуальных следах как объекте криминалистического исследования ввиду малой изученности механизма их образования, передачи, сохранения и возможности их идентификации, что требует отдельного, более глубокого и дополнительного исследования.

---

[1] Лыткин Н.Н. Использование компьютерно-технических следов в расследовании преступлений против собственности: автореф. дис. ... канд. юрид. наук: 12.00.09. М., 2007. С. 11.

[2] Белкин Р.С. Криминалистическая энциклопедия. Место преступления, участок местности или помещение, где было совершено преступление. 2-е изд. доп. М.: Мегатрон XXI, 2000. С. 115.

[3] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 177.

§ 2. Криминалистическая характеристика мошенничеств, сопряженных с использованием платежных карт

Продолжая рассмотрение общего вопроса о криминалистической характеристике мошенничеств, совершенных с использованием средств компьютерной техники в сфере компьютерной информации, нам хотелось бы рассмотреть его более подробно на примере одной из сфер совершения подобных преступлений, а именно на примере мошенничеств, сопряженных с использованием платежных карт.

Совершение подобных преступлений является составной частью мошенничества в сфере компьютерной информации, тем не менее, как и любой вид мошенничеств, совершенных в сфере компьютерной информации, имеет свою специфику. Преследуя цель продемонстрировать необходимость создания и изучения частных методик расследования мошенничеств в сфере компьютерной информации каждого ее вида, в отдельности, используя классификацию, приведенную нами в первом параграфе, по способу их совершения, мы и предприняли попытку рассмотрения данного вопроса.

Для начала необходимо выделить то обстоятельство, что объектом преступного посягательства при совершении мошенничеств, сопряженных с использованием платежных карт, являются денежные средства держателя банковской карты, помещенные на счете. Самостоятельно банковская платежная карта никак не считается предметом преступного посягательства, так как она предполагает лишь инструмент допуска к денежным средствам карты, размещенным на его счетах.

Рассматривая криминалистическую характеристику данного преступления, можно выделить следующие обстоятельства, подлежащие установлению:

1. Место совершения преступления. В соответствии с постановлением Пленума Верховного Суда РФ от 27.12.2007 № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» местом совершения преступления признается реальное местоположение отдела банка, в котором был открыт счет, укрепленный БПК, с которого совершается кража денежных средств.

2. Структура и численность организованной группы, так как данный вид преступлений крайне редко совершается преступниками-одиночками, значимость и роль любого из соучастников. Необходимо учитывать вероятность работы международных организованных групп (преступных сообществ) при мошеннических действиях.

3. Методы совершения мошенничества с применением поддельных банковских платежных карт или иным другим способом.

Обстановка совершения преступления отождествляется с расследуемым событием, определяя ее как территориальную, климатическую, демо-

графическую и иную специфику места совершения преступления, а также как обстоятельства, характеризующие непосредственно место, время, условия и другие моменты совершения преступления.

Кроме того, необходимо отметить, что существуют определенные трудности при сопоставлении понятий «обстановка» и «ситуация» ввиду их определенного сходства. В общем словоупотреблении обстановка – это положение, обстоятельства, условия существования кого-нибудь, чего-нибудь, а ситуация – совокупность обстоятельств, положение, обстановка. И ситуация, и обстановка связаны с функционированием системы деятельности. Криминалистическое разграничение данных понятий видится в следующем. Понятием «ситуация» охватываются основания принятия решения при планировании и осуществлении деятельности. Именно ситуация детерминирует формирование способа совершения преступления. Обстановка же характеризует внешние условия, которые влияют на изменение первоначального плана субъекта деятельности. С изменением обстановки вследствие функционирования системы обратной связи происходит коррекция деятельности в соответствии с желаемым результатом.

Таким образом, обстановка совершения преступления может быть представлена в виде системы из окружающей преступника в момент совершения преступления среды и участников события преступления. Сам преступник в подавляющем большинстве случаев не является структурным элементом обстановки совершения преступления. Он вынужден взаимодействовать с обстановкой, учитывать ее, иногда способен вносить в нее выгодные для себя изменения, но не имеет возможности полностью ее изменить, даже если от этого зависит, по его мнению, успех преступления.

Как показывает практика, место совершения мошенничества выбирается преступником в зависимости от способа его совершения.

В целом обстановка совершения мошенничества в значительной степени отличается от обстановки совершения других преступлений. При совершении мошенничества потерпевшие некоторое время, иногда довольно длительное, находятся с мошенниками в спокойной обстановке. Применение насилия для мошенничества не характерно, поскольку потерпевший даже не подозревает, что его обманывают[1].

При совершении хищения денежных средств путем обмана и злоупотребления доверием, т. е. мошенничества, преступники используют следующие способы[2]:

---

[1] Имаева Ю.Б. Характеристика личности преступника, совершившего хищение с использованием банковских карт и их реквизитов. URL: http://www.eurasialegal.info/index.php?option=com_content&view=article&id=5773:2017-09-11-09-47-43&catid=224:2013-03-21-08-33-12&Itemid=1

[2] Злоупотребление доверием как способ совершения мошенничества. URL: http://studbooks.net/1120241/pravo/zloupotreblenie_doveriem_sposob_sovershenіya_moshennichestva

1. Тайное изменение в программах, обеспечивающих проведение расчетов с использованием пластиковых карт. В данном случае требуется дополнительная квалификация по ст. 273 УК РФ («Создание, использование и распространение вредоносных компьютерных программ»), так как данный способ хищения сопряжен с внесением изменений в существующие программы для электронно-вычислительных машин.

2. Хищение денежных средств, принадлежащих банку путем получения карты по поддельному удостоверению личности либо на подставное лицо.

3. Хищение денежных средств недобросовестным держателем карты путем обмана или введения в заблуждение ее эмитента.

4. Хищение денежных средств путем обмана или введения в заблуждение держателя карты при осуществлении платежно-расчетной операции (хищения данным способом совершают, как правило, сотрудники сервисных и торговых предприятий).

Так, «Н., находясь в торгово-развлекательном центре, реализуя свой преступный умысел, направленный на хищение денежных средств, обратился с просьбой к С. воспользоваться его банковской картой с целью установления интернет-обслуживания. При этом Н. дезинформировал С., который, не подозревая о преступных намерениях Н., осуществил в банкомате с использованием своей карты операции, продиктованные Н., и предоставил ему две выданные банкоматом квитанции с данными о своей банковской карте и о находящихся на ней денежных средствах. Завладев конфиденциальной информацией, Н. перевел денежные средства в размере 12 тыс. руб. с банковской карты С. на банковскую карту своего знакомого З. через Интернет. Далее Н., используя банковскую карту З., получил похищенные денежные средства в банкомате. В результате тайного хищения потерпевшему С. причинен значительный ущерб»[1].

5. Нарушение правил оформления расчетных операций с использованием платежно-расчетных карт работниками мерчанта эквайера или эмитента («Эмитент (Issuer) – банк или компания, выпускающая карты) (Эквайер (Acquirer) – банк или компания, создающая обслуживающую сеть. Процесс создания сети делится на две составляющие – установка терминалов в торгово-сервисной сети и банкоматов) (Мерчант от англ. Merchant – купец, торговец, коммерсант) – название для широкой категории финансовых услуг, предназначенных для использования в бизнесе»[2]. Наиболее часто это название относится к службе, которая позволяет принимать платежи с использованием банковской пластиковой карты).

---

[1] Болсуновская Л.М. Мошенничество в сфере компьютерной информации: анализ судебной практики. URL: https://pravo163.ru/moshennichestvo-v-sfere-kompyuternoj-informacii-analiz-sudebnoj-praktiki (дата обращения: 08.01.2018).

[2] URL: http://kunegin.narod.ru/ref6/ecom/glossary.htm (дата обращения: 08.01.2018).

6. Использование поддельных платежных банковских карт.

7. Создание и использование сайтов-двойников, лжепредприятий.

8. Использование данных действующих пластиковых карт и личных персональных данных их держателей, а также реквизитов несуществующих пластиковых карт.

Таким образом, при совершении преступлений с использованием расчетных и кредитных карт метод совершения дает возможность существенно охарактеризовать отдельные индивидуальные сведения преступления.

В основной массе ситуации потерпевшим признается юридическое лицо (банк либо торгово-сервисная организация), по этой причине этот компонент не представляет криминалистической заинтересованности.

Рассматривая данный вид преступления, нельзя обойти вопрос о механизме следообразования при совершении компьютерного мошенничества.

Процесс осуществления любого платежа, поступающего на абонентский номер мобильного телефона, всегда имеет примерно одинаковую последовательность. Рассмотрим ее на примере показаний свидетеля К., работающего системным администратором в ИП «Ж.»[1]. При осуществлении платежа плательщиком заполняется заявка на оплату услуг связи, где указана сумма платежа, абонентский номер, на который поступает платеж, дата платежа, а также ставится подпись клиента. Данную заявку, после проведения операции по зачислению денежных средств, плательщик может оставить у себя. Далее оператор заносит данные, указанные в заявке, в программу Pinpay, установленную на рабочем компьютере. В общем виде программное обеспечение платежных систем состоит из серверной части и клиентских частей. При этом сервер осуществляет следующие операции[2]:

– процессинг (деятельность по обработке информации, используемой при совершении платежных операций);

– взаиморасчеты между участниками платежной системы;

– контроль работы клиентских частей платежной системы;

– взаимодействие с внешними системами (системы поставщики, другие платежные системы (платежные шлюзы);

– веб-интерфейс сервера для разных категорий пользователей (администратор, сотрудник, агент, терминал).

В свою очередь, клиентские части отвечают:

– за проведение платежей;

– связь с сервером;

---

[1] Приговор № 10-27/2017 от 28.07.2017 по делу № 10-27/2017. URL: http://sudact.ru/regular/doc/YhCN0qu9cvod (дата обращения: 08.01.2018).

[2] Клиентское и серверное программное обеспечение. URL: https://studfiles.net/preview/931097/page:31 (дата обращения: 08.01.2018).

– графический интерфейс взаимодействия с плательщиком;

– управление работой своих компьютерных устройств.

Для нас важно, что сервер позволяет «увидеть» любой платеж, произведенный в подконтрольной ему точке. Список платежей, а также сведения о техническом обеспечении проводимых операций, могут быть предоставлены в распоряжение следователя на основании запроса в рамках уголовного дела, а также путем дачи показаний от представителя оператора по приему платежей от физических лиц (как правило, это системный администратор), в качестве свидетеля.

После передачи денежных средств плательщиком, оператор выдает ему чек, в котором указывается дата и время оплаты, сумма платежа и реквизиты индивидуального предпринимателя. В системе Pinpay отображается и статус платежа, т.е. информация о том, поступил ли платеж абоненту.

Принцип действия платежных терминалов имеет схожие черты. Основными отличиями является самостоятельное заполнение заявки на экране терминала абонентом, а также программное обеспечение, используемое в терминале. Оно может зависеть от фирмы-производителя, либо потребностей владельца терминала.

Анализируя изложенный материал, мы приходим к выводу о том, что следовая информация при выборе преступником способа передачи денежных средств посредством зачисления их на абонентский номер мобильного телефона, будет следующего характера:

Материальные следы:

– кассовые чеки, платежные поручения, находящиеся у потерпевшего и подтверждающие факт внесения им денежных средств на определенный абонентский номер сотового телефона;

– заявка на проведение платежа, находящаяся у плательщика (в случае, когда потерпевший для зачисления денежных средств обратился в специализированный отдел по приему платежей, а не пользовался, к примеру, мультикассой);

– сведения о техническом обеспечении проводимых операций, предоставленные представителем оператора платежной системы.

Идеальные следы:

– показания свидетелей – очевидцев осуществления платежа. Как правило, такими свидетелями являются операторы торговых точек по осуществлению оплаты услуг мобильной связи.

Электронно-цифровые следы:

– сведения о соединениях по абонентскому номеру, на который были внесены денежные средства потерпевшим, отражающие информацию о том, когда, сколько и на какой счет были внесены потерпевшим денежные средства;

– списки платежей, предоставленные системным администратором оператора платежной системы.

В абсолютном большинстве случаев после перевода денежных средств потерпевшим на абонентский номер мобильного телефона, указанный преступником, последний обналичивает полученные деньги, пользуясь возможностями компании «Юнистрим денежные переводы». Обналичивание денежных средств осуществляется, как правило, доверенными лицами преступника. В процессе обналичивания также образуются некоторые следы, могущие иметь значение для успешного раскрытия и расследования мошенничества, совершаемого с использованием электронных платежных систем.

В глобальной сети Интернет имеются электронные ресурсы, позволяющие осуществлять перевод денежных средств с лицевого счета абонента мобильного телефона на счет определенного физического лица, открытого в банке. Для этого необходимо произвести следующие действия: посредством использования персонального компьютера либо мобильного телефона с возможностью выхода в сеть Интернет, с установленным программным обеспечением (браузер Opera, Mozilla Firefox, Chrome и т. д.) осуществляем доступ на электронный ресурс «www.Unistream.ru Денежные переводы». Далее осуществляем переход по ссылке «Денежные переводы по России и СНГ со счета абонентского номера мобильного телефона». После чего переходим на вкладку «Для абонентов Билайн (адресные переводы)», на котором описан процесс перевода средств со счета абонентского номера мобильного телефона на адрес отделения Банка. При переходе на ссылку «money.beeline.ru/kassa» указан список соотношения номеров идентификаторов с адресами отделений банков, где можно получить перевод. После чего с мобильного телефона отправляется SMS-сообщение на номер 3116 следующего вида «Uni сумма фамилия имя отчество и номер отделения банка, в который будет отправлен перевод», при этом сумма перевода составляет не менее 1000 рублей и не более 15 000 рублей. Затем указанная сумма денежных средств поступает в указанный абонентом банк. После этого на мобильный телефон приходит SMS-сообщение от банка с указанием контрольного номера денежного перевода, суммы, комиссии, адресом пункта выдачи перевода. При переводе необходимо сообщить оператору, что перевод совершен по системе «Юнистрим», указать контрольный номер перевода, сумму перевода и предъявить документ, удостоверяющий личность. После чего лицо, чьи анкетные данные были указаны в SMS-сообщении, обращается в отделение банка, где предъявив паспорт и указав вышеуказанные данные, получает указанную в SMS-сообщении сумму денежных средств. Операцию по переводу денежных средств может осуществить каждый, для этого не обязательно иметь специальные познания, весь процесс перевода доступным языком изложен на электронном ресурсе «www.Unistream.ru Денежные переводы» и для этого необходим доступ к выходу в Интернет.

Так, например, «Нофенко Л.С. совершила хищение чужого имущества путем ввода компьютерной информации посредством информационно-телекоммуникационных сетей при следующих обстоятельствах. Нофенко Л.С., посредством услуги «Мобильный банк» получив на мобильный телефон электронное сообщение о доступном лимите денежных средств в сумме... на не принадлежащем ей банковском счете, открытом на имя Ш., имея умысел на хищение указанной суммы и реализуя его, используя принадлежащий ей мобильный телефон Samsung и сим-карту с абонентским номером, зарегистрированным на имя Д., к которой ошибочно подключена услуга «Мобильный банк» Сбербанка России, предоставляющая право распоряжаться денежными средствами, находящимися на расчетном счету на имя Ш. путем ввода компьютерной информации в форме электронных сигналов – «смс-сообщения» на номер «900», посредством телекоммуникационной сети оператора сотовой связи «Билайн», в несколько приемов перечислила (похитила) денежные средства в сумме..., находившиеся на расчетном счете... и принадлежащие Ш., на счет сим-карты с абонентским номером..., причинив Ш. имущественный ущерб на общую сумму... рублей»[1].

Таким образом, при обналичивании доверенным лицом преступника денежных средств образуются следующие следы[2]:

Материальные следы:

– расходный кассовый ордер, выдаваемый банком получателю денежных средств.

Идеальные следы:

– показания свидетеля – сотрудника банка, который осуществлял выдачу денежных средств;

– показания свидетеля – доверенного лица преступника, который получал денежные средства (доверенное лицо, в большинстве случаев, не осведомлено в преступной деятельности злоумышленника).

Электронно-цифровые следы:

– записи камер видеонаблюдения отделения банка, в котором доверенное лицо преступника получало денежные средства.

У потерпевшего следует производить выемку кассовых чеков, платежных поручений, подтверждающих факт внесения им денежных средств на определенный абонентский номер мобильного телефона. Оператору связи лицом, производящим расследование, должен быть направлен запрос

[1] Приговор Грачевского районного суда Ставропольского края от 13.06.2013 по уголовному делу N 1-82/2013 // Судебные решения РФ. Единая база данных решений судов общей юрисдикции Российской Федерации. URL: http://www.gcourts.ru/case/14183520.

[2] Расследование преступлений, связанных с отмыванием (легализацией) денежных средств и иного имущества. URL: https://studfiles.net/preview/6707043/page:14.

в порядке ст. 21 УПК РФ относительно того, кому принадлежит абонентский номер, баланс которого пополнил потерпевший.

После установления абонентского номера, на который были перечислены денежные средства потерпевшим, и данных о его владельце следует установить сведения о движении денежных средств на лицевом счете абонентского номера мошенника, сведения об отправленных SMS-сообщениях, интернет-трафике, месте нахождения абонента за определенный период времени. Для получения указанных сведений у оператора связи необходимо провести следственное действие, предусмотренное ст. 186.1 УПК России, которое называется «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». Кроме того, необходимо направить запрос оператору связи для определения связи лицевого счета абонентского номера мобильного телефона со счетами в других банках.

Для дальнейшего установления лиц, причастных к совершению данных преступлений, направляется запрос в банк, в котором осуществлялось обналичивание и (или) снятие со счета денежных средств. В банке истребуются сведения об установочных данных лица, которое получило денежные средства.

Не меньший интерес представляет процедура передачи денежных средств посредством системы денежных переводов и механизм следообразования.

Под системой денежных переводов понимается организационная структура, разработавшая правила приема и передачи денежных средств между физическими лицами, подкрепившая эти правила программным обеспечением и обеспечившая передачу информации с помощью средств электронных коммуникаций. На территории Российской Федерации к системам перевода денежных средств предъявляются следующие требования:

– наличие собственного клиринг-центра;

– наличие службы сопровождения программы и поддержки партнеров, работающих с клиентами;

– наличие фирменного логотипа;

– наличие лицензии Центрального банка РФ на осуществление денежных переводов.

В настоящее время достаточно популярным сервисом оплаты платежей и осуществления переводов в Интернете являются «электронные деньги». Нормативное регулирование обращения электронных денежных средств в Российской Федерации осуществляется посредством федерального закона РФ от 27.06.2011 № 161-ФЗ «О национальной платежной системе»[1].

[1] О национальной платежной системе : федер. закон от 27.06.2011 № 161. Доступ из справочно-правовой системы «Гарант».

В соответствии с п. 18 ст. 3 данного нормативного акта, электронные денежные средства – это денежные средства, которые предварительно предоставлены одним лицом (лицом, предоставившим денежные средства) другому лицу, учитывающему информацию о размере предоставленных денежных средств без открытия банковского счета (обязанному лицу), для исполнения денежных обязательств лица, предоставившего денежные средства, перед третьими лицами и в отношении которых лицо, предоставившее денежные средства, имеет право передавать распоряжения исключительно с использованием электронных средств платежа.

Кроме того, в федеральном законе предусмотрено, что не являются электронными денежными средствами денежные средства[1]:

– полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг;

– полученные организациями, осуществляющими клиринговую деятельность и (или) деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций.

Электронные деньги являются одним из самых современных средств платежа. Следует отметить, что они являются обязательством банка, либо другого финансового института, не связанного с каким-либо конкретным счетом. При проведении транзакций посредством использования электронных денежных средств информация об их объеме в закодированном виде может быть записана на смарт-карту, имеющую встроенный микропроцессор, либо храниться на жестком диске компьютера. Переводы, осуществляемые посредством электронных денежных средств, могут происходить с «привязкой» банковских карт, а также с помощью электронных кошельков.

В целом «сетевые деньги» являются своеобразным посредником – заменителем банкнот и монет, выпускаемых Центробанком РФ. В ходе транзакций денежных средств, осуществляемых рассматриваемым нами способом, персональная информация о лице, осуществляющем расчет, никому не предоставляется. Роль финансовых посредников в этом случае сводится к минимуму.

В настоящее время электронные системы платежей успешно функционируют во всем мире. Принцип их функционирования базируется на обычном банковском счете. Осуществление платежа – это не что иное, как команда банку о переводе определенной суммы на определенный банковский счет.

---

[1] Электронные денежные средства. URL: http://www.consultant.ru/law/podborki/jelektronnye_denezhnye_sredstva// (дата обращения: 08.01.2018).

В этом контексте заслуживает внимания работа В.Н. Анохина, в которой электронный платеж определяется как «процесс перевода денежных средств получателю с помощью аппаратно-программных средств электронных платежных систем, в том числе сети Интернет, для исполнения денежного обязательства»[1].

Мошенники не часто пользуются услугами по электронному переводу денежных средств, однако же следственной практике известны случаи мошенничеств, где преступниками используются электронные кошельки. Основными способами совершения таких преступлений являются предлог сделки купли-продажи какого-либо имущества, а также сообщение о каком-либо выигрыше.

Так, подозреваемый Н. разместил заведомо не соответствующее действительности объявление о продаже автомобиля на сайте drom.ru. Потерпевший А., созвонившись с Н., договорился о покупке данного автомобиля, при этом Н. поставил условие о предоплате в размере 30.000 рублей. И, так как А. находился в другом городе, попросил перевести указанную сумму на счет электронного кошелька WebMoney. На следующий день А. через терминал оплаты перевел денежные средства на счет электронного кошелька, указанный Н., и позвонил последнему, намереваясь договориться о дате сделки. Однако номер телефона, указанный Н. в объявлении о продаже автомобиля, оказался недоступен[2].

Сам процесс зачисления денежных средств на счет электронного кошелька достаточно прост. Рассмотрим этот механизм на примере электронного кошелька WebMoney.

Существует три способа пополнения электронного кошелька:

– наличными;

– с банковского счета;

– электронными деньгами.

Применительно к рассматриваемым мошенничествам считаем целесообразным принимать во внимание лишь пополнение электронного кошелька наличными деньгами.

В свою очередь, способов зачисления наличных денег на счет WebMoney также предлагается достаточно много. К примеру, в Барнауле расположено не менее 335 объектов, позволяющих ввести денежные средства в систему WebMoney[3]. К ним относятся платежные терминалы QuickPay, Мульти-касса, Экспресс-касса, почтовые отделения, некоторые

---

[1] Электронные платежные системы в Интернете. URL: https://studfiles.net/preview/1742092 (дата обращения: 08.01.2018).

[2] Drom.ru разоблачает схему массового обмана покупателей в объявлениях о продаже машин. URL: https://www.drom.ru/info/misc/drom-ru-27654.html (дата обращения: 08.01.2018).

[3] Вывод денег с Webmoney: важное о проблеме. URL: http://dataworld.info/webmoney-to-card-free-transfer.php (дата обращения: 08.01.2018).

салоны связи («Связной») и т. д. Большинство таких объектов позволяет мгновенно зачислить деньги на счет электронного кошелька.

После ввода денежных средств в терминал плательщику выдается чек о проведенной операции.

Зачисленные на счет электронного кошелька денежные средства, как правило, сразу же переводятся преступником на другой счет. Это может быть счет мобильного телефона, банковская карта и т. д.

Отследить движение денежных средств, полученных преступником таким способом, крайне сложно. Так, зачастую злоумышленниками используется электронный кошелек Qiwi, для регистрации которого необходим лишь номер сотового телефона. Т.е. никаких данных о держателе такого кошелька, по большому счету, нет. Представители данной компании предоставляют данные лишь о номере мобильного телефона, к которому «привязан» кошелек, и отправляют сотрудников правоохранительных органов к оператору сотовой связи. Однако следует понимать, что телефонный номер, привязанный к электронному кошельку, открытому в преступных целях, вряд ли будет зарегистрирован на действительного исполнителя мошенничеств.

Исходя из сказанного, можно сделать вывод о следах, образующихся при мошенничестве, совершаемом с использованием электронных платежных систем, в котором способом передачи денежных средств было их зачисление на счет электронного кошелька.

Материальные следы:

– чек о зачислении денежных средств на счет электронного кошелька, выдаваемый потерпевшему.

Идеальные следы:

– показания свидетеля – сотрудника почтового отделения, либо салона связи, в котором потерпевший осуществлял перевод денежных средств на счет электронного кошелька.

В заключение можно отметить, что криминалистическая характеристика мошенничества с применением расчетных и кредитных карт содержит следующие структурные компоненты: криминалистически важные сведения о способах подготовки, совершения и сокрытия преступления, криминалистически значимые сведения об объекте и ситуации совершения хищения, криминалистически важные данные о лице преступника и потерпевшего (держателя карты), криминалистически важные сведения о механизме следообразования, сведения об условиях, способствовавших совершению преступления, и в их отсутствии нельзя будет отчетливо и грамотно расследовать преступление, сопряженное с применением платежных карт.

Изучение элементов криминалистической характеристики мошенничеств в сфере компьютерной информации позволяет сформировать у лиц, причастных к процессу их раскрытия и расследования, верные представле-

ния о проверочных действиях и информации, которая должна получить свое закрепление в материалах предварительной проверки. Такие звания способствуют повышению эффективности предстоящего расследования, а также сводят к минимуму возможность вынесения решения о незаконном и необоснованном возбуждении уголовного дела.

Изложенная в данном параграфе информация, хоть и описывает следовую картину, преимущественно характерную составу преступления, выходящему за пределы квалификации по ст. 159.3 УК РФ, но в то же время позволяет расширить представление о системе электронных платежей, с функционированием которой также нередко сталкиваются и в ходе расследования мошенничества с использованием пластиковых карт в случае перевода с последующим обналичиванием похищенных денежных средств через электронные платежные системы.

Глава 2. Особенности расследования мошенничества в сфере компьютерной информации

§ 1. Особенности возбуждения уголовных дел при расследовании мошенничества в сфере компьютерной информации

Начальным этапом расследования любого уголовного дела является стадия возбуждения уголовного дела. Дискуссии о необходимости данной стадии уже давно являются полем битвы различных ученых. Однако они не являются предметом нашей работы. Мы будем исходить из уже существующих реалий, закрепленных в уголовно-процессуальном законодательстве.

Возбуждению уголовного дела должна предшествовать проверка заявлений о совершенном либо готовящемся преступлении.

Изучение следственной и судебной практики по уголовным делам о мошенничестве в сфере компьютерной информации свидетельствует о том, что во всех случаях расследования дел указанной категории возбуждению уголовного дела предшествовала предварительная проверка. При этом в 27 % случаях она продолжалась достаточно длительное время (до 30 суток и более)[1].

По делам о мошенничестве в сфере компьютерной информации поводами для осуществления предварительной проверки и затем в дальнейшем, по ее результатам, основанием для возбуждения уголовного дела может являться сообщение о совершенном или готовящемся преступлении, непосредственное обнаружение органом дознания признаков преступления, явка с повинной. Данный перечень не является исчерпывающим и может быть расширен.

Так, по мнению В.Е. Козлова, по делам о мошенничестве в сфере компьютерной информации перечень поводов для возбуждения уголовного дела может включать в себя:

– заявление о преступлении, поступившее от граждан, руководителей организаций, учреждений и предприятий;

– рапорты, поступившие от сотрудников органов дознания, об обнаружении сведений, указывающих на признаки преступления, выявленных при проведении оперативно-розыскных мероприятий;

– рапорты, поступившие от сотрудников органов дознания, по результатам проверки сообщений о готовящемся или совершенном преступлении в сфере компьютерной информации;

[1] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 84.

– рапорты, поступившие от сотрудников органов дознания, о задержании лица с поличным;

– материалы контрольно-ревизионных и иных документальных проверок;

– материалы предварительного расследования по другим видам преступлений;

– информация, опубликованная в средствах массовой информации[1].

Похожей точки зрения придерживаются и другие авторы. Так, Л.Е. Чистова выделяет в качестве основания для возбуждения уголовных дел по делам данной категории следующие:

1. Заявление потерпевшего от мошеннических действий в сети Интернет.

2. Сообщение представителей благотворительных организаций о клонировании их сайтов.

3. Сообщение в печати об обнаруженном мошенничестве в сети Интернет.

4. Обнаружение правоохранительными органами признаков мошенничества в сети Интернет.

Таким образом, можно сделать вывод о том, что вышеуказанные ученые фактически предлагают однотипные поводы для возбуждения уголовных дел о мошенничестве в сфере компьютерной информации, но с некоторыми отличиями[2].

Коломинов В.В. считает, что поводом для возбуждения уголовных дел о мошенничестве в сфере компьютерной информации являлось заявление потерпевшего лица (80 % случаях). В 15 % случаях информация о совершенном преступлении была выявлена непосредственно сотрудниками правоохранительных органов. В остальных случаях о факте такого мошенничества становилось известно из средств массовой информации. При этом из всего процентного соотношения поступивших заявлений потерпевших лишь в 26% случаях такое заявление делали представители юридических лиц»[3].

Данную ситуацию можно объяснить высоким уровнем латентности рассматриваемых преступлений, а также использованием злоумышленниками таких способов совершения мошенничеств, при которых жертвами преступлений становятся лица, имеющие слабую компьютерную подготовку. Такие лица сами не всегда понимают, как это могло произойти, а, следовательно, не верят и в возможности органов предварительного расследования по поимке преступников и возврате им похищенных средств.

---

[1] Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. М., 2002. С. 336.

[2] Чистова Л.Е. и др. Методика расследования отдельных видов мошенничества: учеб. пособие / под ред. А.Г. Филиппова. М.: МосУ МВД России, 2014. С. 41.

[3] Коломинов В.В. Указ соч. С. 88.

По результатам исследования, проведенного В.В. Коломиновым, по делам о мошенничестве в сфере компьютерной информации при решении вопроса о возбуждении уголовного дела предварительная проверка правоохранительными органами проводилась во всех случаях[1].

Такая ситуация складывается вследствие того, что в условиях дефицита исходной информации по делам о подобных преступлениях на первоначальном этапе расследования очень трудно выявить все признаки совершенного преступления и их обнаружение требует проведения целого ряда первоначальных следственных и иных процессуальных действий.

С целью выбора средств предварительной проверки и определения объема, перечня и порядка проведения первоначальных процессуальных действий следователь должен оценить сложившуюся следственную ситуацию. По мнению В.В. Коломинова, на данном этапе возможно существование следующих типичных следственных ситуаций:

1. Преступники продолжают совершать незаконные действия, существует устойчивая связь между ними и лицом, в отношении которого совершается компьютерное мошенничество (20% изученных случаев).

2. Преступление окончено и связь между лицом, в отношении которого оно совершено, и мошенниками отсутствует (80% изученных случаев)[2].

Наиболее благоприятной для следствия является наличие первой следственной ситуации, что позволяет следователю задержание подозреваемых с поличным и сбор достаточного количества следов совершенных ими преступлений. Вторая ситуация является более сложной для расследования компьютерных мошенничеств, однако, как показывает приведенная нами статистика, именно она и является наиболее распространенной на начальном этапе.

Самым распространенным процессуальным действием, на первоначальном этапе расследования преступлений является получение объяснений. Ранее существовали объективные проблемы с использованием данных объяснений в качестве средств доказывания, и следователям приходилось повторно допрашивать тех лиц, которые уже ранее давали показания по расследуемым обстоятельствам. В отдельных случаях это вызывало существенные затруднения. Например, если свидетель проживает на значительном удалении от места производства расследования, в случаях болезни или даже смерти последнего. На наш взгляд, такое отношение к объяснениям было абсолютно незаслуженным. Именно в них, как правило, содержится наиболее полная и правдивая информация о совершенном преступлении, т.к. они получаются непосредственно после совершения преступления, когда у человека память еще не затуманена временем и события преступления свежи в их памяти.

---

[1] Коломинов В.В. Указ соч. С. 88.

[2] Там же. С. 92.

Данная проблема была разрешена определением Конституционного Суда РФ от 28.05.2013 № 723-О, в котором объяснения, полученные до возбуждений уголовного дела, были отнесены к иным документам[1].

Получение объяснений по делам о компьютерных мошенничествах, как правило, должно предшествовать проведению других процессуальных действий, в том числе и следственному осмотру, так как позволяет определиться с объектами и границами осмотра[2].

На всех этапах проведения доследственной проверки дознавателю по делам данной категории следует осуществлять тесное взаимодействие со специалистом в области компьютерной техники, т.к. «в базовом образовании следователя отсутствуют глубокие знания в области особенностей применения и использования компьютерно-технических средств, особенно с учетом их интенсивного развития. Поэтому весь процесс предварительной проверки должен осуществляться в тесном взаимодействии всех подразделений и служб, принимающих в ней участие»[3].

Привлечение специалиста при получении объяснений позволит проверить правдивость показаний лиц, дающих техническую информацию, касающуюся совершенного преступления. В процессе осмотра специалист может оказать существенную помощь при описании технических объектов осмотра, следовой картины, а также при изъятии и упаковке объектов, имеющих значение для расследования уголовного дела.

При расследовании компьютерных мошенничеств, прежде всего, требуется установить места сбыта похищенного. Как показывает практика, это наиболее уязвимое место в цепи преступного замысла. Какими бы хитроумными способами не совершалось данное преступление, конечным итогом должно быть получение денежных средств самим преступником. Поэтому именно на установление мест получения денежных средств должны быть направлены усилия следователя на всех этапах расследования данных преступлений. Это позволяет выявить не только самого преступника, но и его ближайшее окружение. С этой целью следователю необходимо осуществлять тесное взаимодействие с оперативными подразделениями.

Таким образом, при производстве предварительной проверки материалов по делам о компьютерных мошенничествах следователь должен произвести следующие проверочные мероприятия:

– получение объяснений от заявителей о совершенном преступлении;

---

[1] О внесении изменений в статьи 62 и 303 Уголовного кодекса Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: федер. закон Российской Федерации от 4.03.2013 № 23-ФЗ // Рос. газ. 2013. 6 марта. № 6024.

[2] Более подробно данный вопрос будет рассмотрен нами в следующем параграфе.

[3] Расследование неправомерного доступа к компьютерной информации: учеб. пособие. 2-е изд. доп. и перераб. / под ред. Н.Г. Шурухнова. М.: Московский ун-т МВД России, 2004. С. 201–202.

– производство осмотра и изъятия средств компьютерной техники, сохранившей следы совершенного преступления либо являвшейся орудием или объектом преступных действий;

– назначение проверки или ревизии деятельности юридического лица с целью установления хищения денежных средств путем совершения компьютерного мошенничества;

– производство осмотра и изъятия документов, свидетельствующих об оказании услуг подключения к сети провайдером, либо иных документов, содержащих на себе следы совершения преступления;

– назначение и производство различных экспертиз в зависимости от складывающейся следственной ситуации и находящихся в распоряжении следователя объектов и следов, имеющих значение для дела (компьютерной, технико-криминалистической экспертизы документов, фоноскопической, автороведческой, судебно-бухгалтерской и т. д.);

– дача поручений сотрудникам оперативных подразделений о производстве оперативно-розыскных мероприятий с целью установления свидетелей и лиц, совершивших преступление.

По результатам параграфа можем сделать вывод о том, что во всех случаях этапу возбуждения уголовного дела по делам о мошенничестве в сфере компьютерной информации должна предшествовать доследственная проверка.

Трудности, возникающие при проведении доследственной проверки по делам о мошенничестве в сфере компьютерной информации, обусловлены, прежде всего, дефицитом времени и большим объемом работы, которую необходимо провести с целью установления признаков состава преступления. Прежде всего, это связано с необходимостью сбора и исследования компьютерных следов и необходимости изучения достаточно запутанных мошеннических схем.

В результате проведенной доследственной проверки у следователя должно сложиться убеждение, что собраны достаточные для возбуждения уголовного дела данные о совершении мошенничества в сфере компьютерной информации.

§ 2. Проблемы производства отдельных следственных действий при расследовании мошенничества в сфере компьютерной информации

Расследование мошенничества в сфере компьютерной информации предполагает проведение большого количества следственных действий и иных процессуальных мероприятий с целью сбора доказательственной информации. Тактика же производства этих действий разрабатывается исходя из специфики способа совершения и механизма следообразования данной группы преступлений.

Система подготовки следователей в специализированных ВУЗах системы МВД России предполагает изучение курсантами и слушателями общих вопросов, касающихся устройства и правил работы с компьютером, а также особенностей работы с компьютерной информацией при расследовании уголовных дел в сфере телекомунникации. Объем получаемых знаний должен быть вполне достаточным для расследования преступлений в данной сфере, однако, к сожалению, практика говорит об обратном.

Так, в соответствии с исследованиями, проведенными В.В. Коломиновым, он приходит к выводу о том, что «эти знания не дают глубокой базы для формирования соответствующих компетенций и приобретения следователями достаточной квалификация для работы с такими специфическими источниками доказательственной информации, что, в свою очередь, приводит к трудностям в познавательно-поисковой деятельности лиц, ведущих расследование, влияет на качество их работы. Исключение составляет незначительное количество сотрудников, входящих в состав подразделений Управления «К» МВД России, осуществляющего борьбу с преступлениями в сфере информационных технологий на основе профессиональных знаний в области компьютерных систем, высоких технологий, информационной безопасности и юридических знаний»[1].

Справедливости ради следует отметить, что такая картина не является повсеместной для всех следователей. В системе МВД достаточно сотрудников следственных подразделений, обладающих высоким уровнем компьютерной грамотности. Кроме того, недостаток в таких познаниях остальные следователи могут восполнить путем привлечения к производству следственных действий соответствующих специалистов в области средств компьютерной техники и телекоммуникационных сетей. Так что сложившуюся в данной сфере ситуацию нельзя назвать критичной.

На сегодняшний день уголовно-процессуальное законодательство предусматривает достаточно большой перечень следственных действий,

[1] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 84.

которые следователи могут использовать с целью производства доказывания по делам о компьютерных мошенничествах.

Так, согласно исследованиям, проведенным В.В. Коломиновым по делам о мошенничествах в сфере компьютерной информации, чаще всего проводятся «… следующие следственные и иные процессуальные действия:

– осмотр места происшествия, осмотр предметов и документов (100 % уголовных дел);

– допрос лиц, процессуальное положение которых определено (100 % уголовных дел);

– назначение и производство судебных экспертиз (100 % уголовных дел). В 100% случаев назначалась компьютерная экспертиза; в 60 % – дактилоскопическая экспертиза; в 55 % случаев – технико-криминалистическая экспертиза документов; 25 % – трасологическая экспертиза; в 10% – психологическая экспертиза; в 5% случаев – иные;

– получение образцов для сравнительного исследования (80% уголовных дел);

– предъявление для опознания (25 % уголовных дел);

– обыск и выемка (90 % уголовных дел);

– очная ставка (85 % уголовных дел);

– следственный эксперимент и проверка показаний на месте (65 % уголовных дел);

– снятие информации с технических каналов связи (25 % уголовных дел);

– прослушивание телефонных и иных переговоров (5 % уголовных дел) и др.»[1].

Приведенный выше перечень показывает, что следователи достаточно активно используют возможности уголовно-процессуального доказывания по уголовным делам данной категории. Вместе с тем следует отметить, что на практике при расследовании мошенничеств в сфере компьютерной информации следователи сталкиваются с необходимостью поиска и получения информации, имеющей значение для расследуемого уголовного дела в сети Интернет (социальные сети, сайты объявлений и др.), и в случае обнаружения такой информации, возникает дилемма: как данную информацию приобщить к материалам уголовного дела и использовать ее в качестве доказательств? Попробуем рассмотреть возможности, предоставляемые нам для этого уголовно-процессуальным законодательством.

1. Назначение и производство экспертизы. Действительно данный способ получения доказательств является наиболее логичным. Назначить производство компьютерной экспертизы и пусть сам эксперт, обладающий специальными познаниями, найдет и предоставит следователю интересу-

[1] Коломинов В.В. Указ. соч. С. 108–109.

ющую его информацию. Однако в соответствии с п. 2 ч. 4 ст. 57 УПК РФ эксперт не в праве самостоятельно собирать материалы для экспертного исследования. Это задача следователя.

В том случае если следователь самостоятельно найдет интересующую его веб-страницу и укажет ее адрес в постановлении о назначении судебной экспертизы, то опять же нет никакой гарантии того, что к моменту производства экспертизы содержание данной страницы не изменится.

2. Производство обыска или выемки. Проведение обыска в данном случае не подходит из-за отсутствия принудительности обследования и отсутствия определенного законодателем вида обыска. Выемка документов возможна, но возникает целый ряд вопросов: у кого производить выемку? Кому вручать постановление о ее производстве, а затем протокол? Так что выемка в данном случае для получения содержимого веб-страницы тоже не подходит.

3. Следственный осмотр. Действительно, осмотр предполагает проведение поисковых действий, возможность в необходимых случаях привлечения специалистов и других участников осмотра. Использование технических средств осмотра. Однако возникает закономерный вопрос: осмотр чего? Законодатель в статье 176 УПК РФ нам предлагает следующие виды осмотра: «осмотр места происшествия, местности, жилища, иного помещения, предметов и документов, а также трупа». Веб-страница в сети Интернет не всегда может быть местом происшествия, предметом ее тоже не назовешь. Скорее всего, ее можно назвать документом. Вот какое определение нам предлагает Википедия «Веб-страница (англ. Web page) – документ или информационный ресурс Всемирной паутины, доступ к которому осуществляется с помощью веб-браузера. Типичная веб-страница представляет собой текстовый файл в формате HTML, который может содержать ссылки на файлы в других форматах (текст, графические изображения, видео, аудио, мультимедиа, апплеты, прикладные программы, базы данных, веб-службы и прочее), а также гиперссылки для быстрого перехода на другие веб-страницы или доступа к ссылочным файлам. Многие современные браузеры позволяют просмотр содержания ссылочных файлов непосредственно на веб-странице, содержащей ссылку на данный файл. Современные браузеры также позволяют прямой просмотр содержания файлов определенных форматов, в отрыве от веб-страницы, которая на них ссылается»[1]. Таким образом, при осмотре веб-страницы следователь может составить протокол осмотра документа, в котором зафиксирует имеющуюся для дела информацию. Вместе с тем следует отметить возможные трудности, с которыми он может столкнуться в дальнейшем в процессе проведения предварительного расследования или даже в процессе судебного разбирательства. Так, указав в протоколе осмотра адрес веб-страницы и ее

[1] Википедия. URL: https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D1%82%D1%80%D0%B0% D0%BD%D0%B8%D1%86%D0%B0.

содержание, у следователя нет никакой гарантии того, что через небольшой промежуток времени эта информация сохранится на сайте в неизменном виде. Информация на ней может быть изменена правообладателем, удалена провайдером, уничтожена вирусом или злоумышленником и т.д. В целях предупреждения подобных ситуаций следователь должен прибегать к применению технических средств фиксации путем фото или видеосъемки, а также путем копирования данной веб-страницы или ее содержания на электронный носитель. Нам представляется, что с этой целью наиболее оптимальным будет использование скриншотов экрана и сохранение их в виде графических файлов (BMP, JPEG или в файлах с иным расширением). Главное чтобы при этом не происходило чрезмерное сжатие изображения и соответственно ухудшение его качества.

На наш взгляд, такой метод имеет существенное преимущество перед использованием текстовых редакторов – это невозможность их редактирования.

Местом проведения такого осмотра будет кабинет следователя или иное место нахождения компьютера, подключенного к сети Интернет. В качестве технических средств следует указывать соответствующий компьютер и соответствующее оборудование, позволяющее осуществлять выход в сеть Интернет. Хотя осмотр документа и предполагает осмотр уже имеющегося у следователя документа без проведения поисковых действий, однако прямо об этом в ст. 176–177 УПК РФ ничего не сказано.

Другим не менее важным следственным действием по делам данной категории является допрос. Допрос на первоначальном этапе расследования может производиться в отношении свидетеля, подозреваемого, обвиняемого, специалиста или эксперта.

Не затрагивая общие тактические условия и приемы производства данного следственного действия, следует отметить, специфика его производства заключается в том, что следователь должен иметь соответствующие познания в области компьютерного оборудования, программных устройств и информационно-телекоммуникационных сетей, а также знания способов совершения мошенничеств при их использовании. В противном случае допрашиваемый легко может ввести в заблуждение следователя относительно совершенного преступления.

Допрос специалиста или эксперта может оказать существенную помощь в устранении вопросов, касающихся использованной в заключении терминологии, причин расхождения в поставленных перед ним вопросах и полученными ответами, рассмотрения методики исследования и устранения возможного противоречия полученным выводам, разъяснения значения полученных при исследовании выводов и др.

С определенными трудностями следователь может столкнуться также и при производстве таких следственных действий, как обыск и выемка.

В процессе производства данных следственных действий важно учитывать необходимость изъятия всех возможных носителей компьютерной информации, даже тех, которые, на первый взгляд, не имеют отношения к делу (CD, DVD диски с играми или фильмами, карты памяти в электронных книгах или MP3 плейерах). Объясняется это требование тем, что преступники могут хранить скрываемую информацию на данных носителях, ведь этикетки на дисках с играми или музыкой могут являться «ширмой», призванной замаскировать информацию имеющую значение для расследуемого уголовного дела. Такие логотипы и этикетки можно распечатать на многих цветных принтерах.

Другой серьезной проблемой, с которой приходится сталкиваться следователям при производстве обысков и выемок компьютерной информации у юридических лиц, является, как правило, активное противодействие со стороны руководителей этих организаций. Причиной такого противодействия является невозможность осуществления ими хозяйственной деятельности.

При возникновении подобной ситуации следователю необходимо подходить к ее решению индивидуально, очень осторожно и взвешенно. Использование шаблонного подхода может привести либо к утрате доказательств, либо к множественным жалобам на действия следователя.

В качестве рекомендации можно предложить следователю во всех случаях консультироваться со специалистом. Если изымаемая компьютерная техника или носители компьютерной информации не являлись орудием или средством совершения преступления, то в большинстве случаев можно предложить ее владельцу предоставить другие машинные носители информации с целью создания для него побитовой копии изымаемых носителей. В таких случаях следует также стремиться изымать только носители информации, а не сами системные блоки. Что позволит хозяйствующему субъекту вставить в них копии изъятых носителей и продолжить осуществления своей деятельности. Однако следует помнить, что во всех случаях изъятию подлежат оригиналы машинных накопителей.

Эффективным средством в руках следователя может быть также и использование такого следственного действия, как предъявление для опознания. При этом предъявляться для опознания могут как люди (свидетель, потерпевший, подозреваемый или обвиняемый), так и предметы (компьютерная техника, похищенные предметы и др.), фотоснимки (лиц или предметов) и документы. К последним, по нашему мнению, следует относить также и предъявление для опознания компьютерной информации (электронных документов, сайтов, компьютерных программ и т. д.).

Еще одним эффективным следственным действием по делам о компьютерных мошенничествах является следственный эксперимент. Целью его производства может быть проверка возможности написания той или

иной компьютерной программы, возможности «взлома» какого-либо сайта, подключения к какому-либо компьютеру и т. д.

По итогам данного параграфа можно сделать следующие выводы:

1. Наиболее оптимальным и целесообразным способом приобщения к материалам уголовного дела информации, имеющей значение для дела и хранящейся в сети Интернет, является проведение осмотра документа.

2. При проведении допроса по делам о компьютерных мошенничествах следователь должен иметь соответствующие познания в области компьютерного оборудования, программных устройств и информационно-телекоммуникационных сетей, а также знания способов совершения мошенничеств при их использовании. В противном случае допрашиваемый легко может ввести в заблуждение следователя относительно совершенного преступления.

3. В процессе производства обыска и выемки важно учитывать необходимость изъятия всех возможных носителей компьютерной информации, даже тех, которые, на первый взгляд, не имеют отношения к делу.

4. В случаях противодействия со стороны владельца компьютерной информации по причине невозможности осуществления им дальнейшей хозяйственной деятельности, следователю необходимо подходить к решению таких ситуаций индивидуально, очень осторожно и взвешенно. Использование шаблонного подхода может привести либо к утрате доказательств, либо к множественным жалобам на действия следователя. В качестве общей рекомендации можно предложить следователю во всех случаях консультироваться со специалистом.

5. Предъявление для опознания компьютерной информации, хранящейся на машинных носителях, сайтах, а также компьютерных программ, следует оформлять путем предъявления для опознания документов.

6. Все особенности производства перечисленных следственных действий обусловлены, прежде всего, механизмом преступной деятельности, объектом и средством совершения преступлений. Для достижения положительного результата и цели любого из рассмотренных выше следственных действий следователю необходимо тщательно готовиться к их производству, используя многообразные тактические приемы и помощь специалистов.

Рассматриваемое преступление обладает своей спецификой получения доказательств, которая больше всего проявляется в необходимости использования специальных познаний в области информационных технологий при производстве различных следственных действий и, конечно же, при назначении и производстве экспертиз.

Одной из наиболее часто назначаемых экспертиз при расследовании мошенничества в сфере компьютерной информации является судебно-компьютерная экспертиза.

К основным задачам, решаемым при производстве компьютерной экспертизы, можно отнести следующие:

1. Поиск информации на машинном носителе (в средстве вычислительной техники), созданном с помощью прикладных программ;
2. Поиск информации на машинном носителе о действиях пользователя (процессах обработки файлов, ведения баз данных, работе в сетях передачи данных и т. п.);
3. Определение свойств программ и программных продуктов;
4. Определение возможности совершения каких-либо действий с помощью средств вычислительной техники;
5. Определение принадлежности программ и данных к конкретным классам;
6. Установление материальных объектов по компьютерной информации (проводится в комплексе с другими видами экспертиз);
7. Установление фактических обстоятельств совершения преступления (проводится при наличии информации, полученной из различных источников).

Из-за отсутствия достаточного количества специалистов в области компьютерных экспертиз, следователи зачастую сталкиваются с трудностями при формулировании вопросов эксперту при назначении данного вида экспертиз.

Проанализировав значительное количество литературы по данному вопросу, мы пришли к необходимости формулировки основных требований к вопросам при назначении компьютерных экспертиз. Их можно разделить на общие и частные.

Общие требования:

– использование устоявшегося понятийного аппарата, исключающего жаргонные и полупрофессиональные термины («винчестер», «логи», «взлом» и т. п.);

– четкость и однозначность постановки вопроса;

– формулировка вопроса не должна касаться этапов исследования информации;

– вопросы не должны носить справочный характер;

– вопросы не должны носить правовой характер и выходить за пределы компетенции эксперта;

– вопросы должны соответствовать существующей методической и технической базе.

Частные требования:

– вопросы должны быть направлены на установление конкретных обстоятельств расследуемого события;

– вопросы должны быть поставлены так, чтобы при решении конкретных задач расследования, затраты (финансовые, технические, временные и пр.) на проведение исследований были минимальными;

– вопросы должны соответствовать уровню подготовки и инструментальному оснащению экспертов того экспертного учреждения, которому назначается экспертиза;

– вопросы должны соответствовать представляемым на исследование вещественным доказательствам.

На разрешение эксперта при назначении компьютерных экспертиз можно поставить следующие вопросы:

1. Какое программное обеспечение установлено на носителях информации (HDD, SSD, USB-flash, CD, DVD, SD-card) (указывается только ПО, необходимое для раскрытия и расследования уголовного дела)?
2. Каковы сведения о дате его установки?
3. Имеются ли на носителях информации ПЭВМ файлы, содержащие в себе название, ключевое слово, фразу, видео, звук, в том числе и среди удаленных?
4. Каковы сведения о дате создания и изменения данных файлов?
5. Каково содержание журналов Интернет-браузеров (на какие Интернет ресурсы осуществлялся выход), программ обмена сообщений (за указывается период)?
6. Каковы сетевые настройки операционной системы, установленной на носителях информации ПЭВМ (электронного оборудования, смартфона)?
7. Установлено ли на носителях информации ПЭВМ (смартфона) программное обеспечение, определяемое антивирусным ПО, как «вредоносное»?
8. Когда и откуда оно было загружено?
9. Имеются ли SMS сообщения, текстовые, аудио и видеофайлы на мобильном телефоне (смартфоне)? Возможно ли их копирование на сторонний носитель (если да, то прошу скопировать на представленный носитель)?
10. Работает ли электронное оборудование (терминал) без подключения к сети Интернет?

Основной проблемой раскрываемости дел о компьютерном мошенничестве в сфере компьютерной информации, по нашему мнению, является недостаточное количество специалистов в области телекоммуникационных услуг и компьютерной техники. Особенно остро такая проблема стоит в удаленных от центра районах.

Необходимо осознать тот факт, что за последние десятилетия появилось огромное количество новых профессий в сфере программирования, системного администрирования, криптографии. А в правоохранительной

сфере такого разделения труда не состоялось, и такого рода специалистов практически нет[1].

Наряду с компьютерными экспертизами при расследовании данного вида преступлений могут также назначаться и традиционные экспертизы, такие как дактилоскопическая, трасологическая, почерковедческая, портретная экспертизы, экспертиза технического исследования документов и т. п. [2]. Связано это с тем, что при производстве следственных действий по делам о мошенничествах в сфере компьютерной информации изымается не только компьютерное оборудование и информация, но и различные традиционные следы, требующие назначения и производства других видов экспертиз.

[1] Степаненко Д.А. «Адаптивная модификация» криминалистики в информационном обществе как закономерная реакция на распространение киберпреступности // Российский следователь. 2015. № 15. С. 20.

[2] Аверьянова Т. В. и др. Криминалистика: учеб. / под ред. Р.С. Белкина. М., 2001. С. 415.

Заключение

В раскрытии и расследовании уголовных дел о компьютерных мошенничествах остается немало трудностей. Однако до настоящего времени взаимодействие служб правоохранительных органов в раскрытии и расследовании данных преступлений остается недостаточным.

Проведенное исследование относительно проблем, возникающих при расследовании компьютерных мошенничеств, позволило сформулировать следующие выводы:

1. Криминалистическая характеристика мошенничества в сфере компьютерной информации представляет собой обобщенное описание системы криминалистически значимой информации о признаках и свойствах преступления, предусмотренного ст. 159.6 УК РФ, состоящее из определенного множества элементов, таких как непосредственный предмет преступного посягательства; способ совершения преступления, орудия и средства преступления; следы и механизм следообразования; обстановка совершения преступления, его пространственно-временной континуум, которые в свою очередь, характеризуются корреляционной зависимостью между собой, и специфичностью проявлений во внешней среде (киберпространстве) [1].

2. Также следует констатировать, что на сегодняшний день в криминалистике нет единой системы знаний о виртуальных следах как объекте криминалистического исследования ввиду малой изученности механизма их образования, передачи, сохранения и возможности их идентификации, что требует отдельного, более глубокого и дополнительного исследования.

3. Изучение элементов криминалистической характеристики мошенничеств в сфере компьютерной информации позволяет сформировать у лиц, причастных к процессу их раскрытия и расследования, верное представление о проверочных действиях и информации, которая должна получить свое закрепление в материалах предварительной проверки. Таковые звания способствуют повышению эффективности предстоящего расследования, а также сводят к минимуму возможность вынесения решения о незаконном и необоснованном возбуждении уголовного дела.

4. Трудности, возникающие при проведении доследственной проверки по делам о мошенничестве в сфере компьютерной информации, обусловлены дефицитом времени и большим объемом работы, которую необходимо провести с целью установления признаков состава данного преступления. Прежде всего, это связано с необходимостью сбора и исследования компьютерных следов и необходимости изучения достаточно запутанных мошеннических схем.

---

[1] Коломинов В.В. Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Иркутск, 2017. С. 177.

5. Наиболее оптимальным и целесообразным способом приобщения к материалам уголовного дела информации, имеющей значение для дела и хранящейся в сети Интернет, является проведение осмотра документа.

6. При проведении допроса по делам о компьютерных мошенничествах следователь должен иметь соответствующие познания в области компьютерного оборудования, программных устройств и информационно-телекоммуникационных сетей, а также знания способов совершения мошенничеств при их использовании. В противном случае допрашиваемый легко может ввести в заблуждение следователя относительно совершенного преступления.

7. В процессе производства обыска и выемки важно учитывать необходимость изъятия всех возможных носителей компьютерной информации, даже тех, которые, на первый взгляд, не имеют отношения к делу.

8. В случаях противодействия со стороны владельца компьютерной информации по причине невозможности осуществления им дальнейшей хозяйственной деятельности, следователю необходимо подходить к решению таких ситуаций индивидуально, очень осторожно и взвешенно. Использование шаблонного подхода может привести либо к утрате доказательств, либо к множественным жалобам на действия следователя. В качестве общей рекомендации можно предложить следователю во всех случаях консультироваться со специалистом.

9. Предъявление для опознания компьютерной информации, хранящейся на машинных носителях, сайтах, а также компьютерных программ следует оформлять путем предъявления для опознания документов.

10. Все особенности производства перечисленных следственных действий обусловлены механизмом преступной деятельности, объектом и средством совершения преступлений. Для достижения положительного результата и цели любого из рассмотренных выше следственных действий следователю необходимо тщательно готовиться к их производству, используя многообразные тактические приемы и помощь специалистов.

11. Основной проблемой постоянного ухудшения состояния мошенничества в сфере компьютерной информации, по нашему мнению, является недостаточное количество специалистов в области телекоммуникационных услуг и компьютерной техники. Особенно остро такая проблема стоит в удаленных от центра районах.

Литература

1. Конституция Российской Федерации: принята всенародным голосованием 12 дек. 1993г.: (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6 – ФКЗ. Доступ из справочно-правовой системы «КонсультантПлюс».

2. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ. Там же.

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ. Там же.

4. Об оперативно-розыскной деятельности: федер. закон Рос. Федерации от 12.08.1995 № 144-ФЗ. Там же.

5. О полиции: федер. закон Рос. Федерации от 07.02.2011 № 3-ФЗ. Там же.

6. Drom.ru разоблачает схему массового обмана покупателей в объявлениях о продаже машин. URL: https://www.drom.ru/info/misc/drom-ru-27654.html.

7. Абдурагимова Т.И. Раскрытие и расследование изготовления, сбыта и использования поддельных кредитных и расчетных пластиковых карт. дис. канд. юрид. наук. М., 2001.

8. Аверьянова Т.В. Криминалистика: учеб. / под ред. Р.С. Белкина. М., 2009.

9. Баяхчев В.Г., Улейчик В.В. Расследование хищений, совершаемых в кредитно-финансовой сфере с использованием электронных средств // Законодательство. 2000. № 6. С. 53−59.

10. Брылев В.И., Полинчук А.В. Мошенничества в сети Интернет с использованием пластиковых карт // Юридический вестник Кубанского ГОСЮ Университета. 2012. № 3 (12). С. 7−18.

11. Варданян А.В., Никитина Е.В. Расследование преступлений в сфере высоких технологий и компьютерной информации. М., 2007.

12. Википедия. URL:https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0

13. Вопросы эксперту на почерковедческой экспертизеж. URL: http://sud-expertiza.org/pocherkovedcheskaya/voprosy.

14. Вывод денег с Webmoney: важное о проблеме. URL: http://dataworld.info/webmoney-to-card-free-transfer.php

15. Выявление и раскрытие рассматриваемых преступлений происходит в условиях следующих типичных оперативно-следственных ситуаций. URL: https://studopedia.ru/15_88731_ot--N--u-ot--N--u.html.

16. Допрос в рамках уголовного дела: особенности производства. URL: https://ad-ab.ru/osobennosti-proizvodstva-doprosa-v-ramkah-ugolovnogo-dela

17. Ефимова Л.Г. Правовые аспекты безналичных денег // Закон. 1997. № 1 С. 97−103.

18. Злоупотребление доверием как способ совершения мошенничества. URL: http://studbooks.net/1120241/pravo/zloupotreblenie_ doveriem_sposob_sovershenіya_moshennichestva.

19. Имаева Ю.Б. Характеристика личности преступника, совершившего хищение с использованием банковских карт и их реквизитов. URL: http://www.eurasialegal.info/index.php?option=com_content&view=article&id=5773:2017-09-11-09-47-43&catid=224:2013-03-21-08-33-12&Itemid=1

20. Имаева Ю. Б. Особенности расследования хищений, совершенных с использованием кредитных и расчетных карт: дис. … канд. юрид. наук. Уфимский юридический институт МВД России. Уфа, 2015.

21. Клиентское и серверное программное обеспечение. URL: https://studfiles.net/preview/931097/page:31.

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

23. Криминалистика / под ред. И.Ф. Герасимова, Л.Я. Драпкина. М., 2014.

24. Криминалистика: учеб. / под ред. А.Г. Филиппова. 3-е изд., перераб. и доп. М.: Спарк, 2014.

25. Криминалистика: учеб. / под ред. И.Ф. Крылова, А.И. Бастрыкина. М., 2011.

26. Аверьянова Т.В. и др. Криминалистика: учеб. / под ред. Р.С. Белкина. М., 2001. С. 415.

27. Методические рекомендации по расследованию преступлений связанных с незаконным оборотом платежных карт. URL: http://zakoniros.ru/?p=2064

28. Мишина И.М. Расследование мошенничества, совершенного с использованием банковских карт: криминалистические и уголовно-процессуальные аспекты. дис. … канд. юрид. наук: 12.00.09. М., 2009.

29. Мошенничество с банковскими картами. Новый вид мошенничества. URL: https://businessman.ru/new-moshennichestvo-s-bankovskimi-kartami.html

30. Объективная сторона, объект мошенничества с использованием платежных карт. URL: http://justsolution.ru/ugolovnye-dela/ moshennichestvo/ moshennichestvo-s-ispolzovaniem-platezhnyx-kart

31. Приговор № 10-27/2017 от 28 июля 2017 г. по делу № 10-27/2017. URL: http://sudact.ru/regular/doc/YhCN0qu9cvod

32. Причины и факторы, способствующие совершению хищений с использованием интернет-технологий. URL: https://pravo.studio/ kriminalisticheskaya-taktika/prichinyi-faktoryi-sposobstvuyuschie-76257.html

33. Протосевич А.А., Зверянская Л.П. Криминалистическая характеристика компьютерных преступлений // Российский следователь. 2013. № 11. С 45−47.

34. Расследование преступлений, связанных с отмыванием (легализацией) денежных средств и иного имущества. URL: https://studfiles.net/preview/6707043 /page:14

35. Семикаленов А.И., Сергеева К.А. Мобильные телефоны сотовой связи – новые объекты судебной компьютерно-технической экспертизы // Законы России: опыт, анализ, практика 2011. № 12. С. 89−94.

36. Скворцова С.А. Уголовно-правовая характеристика преступлений, совершаемых с использованием банковских карт: автореф. дис. … канд. юрид. наук. М., 2000.

37. Состояние преступности в России за январь−декабрь 2019 г. URL: https://genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf

38. Способы совершения преступлений с использованием банковских платежных карт. URL: https://www.liveinternet.ru/users/ zzyzx_zzyzx/post120667197

39. Статья 159 УК РФ «Мошенничество». Консультация адвоката и юридическая помощь по ст. 159 УК РФ. URL: http://ugolovkinet.ru/statya-159-uk

40. Судебная экспертиза полимерных материалов, пластмасс, резин и изделий из них/ URL: https://studfiles.net/preview/5970189/page:110

41. Степаненко Д.А. «Адаптивная модификация» криминалистики в информационном обществе как закономерная реакция на распространение киберпреступности // Российский следователь. 2015. № 15. С. 20.

42. Тема 11 следственный осмотр. URL: https://studfiles.net/ preview/5080535/ page:20

43. Электронные денежные средства. URL: http://www.consultant.ru/law/podborki/ jelektronnye_denezhnye_sredstva

44. Электронные платежные системы в Интернете. URL: https://studfiles.net/preview/1742092

Оглавление

Учебное издание

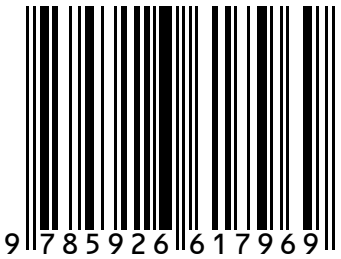
Рясов Александр Алексеевич

МЕТОДИКА РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Учебное пособие

Редактор *С. Н. Маслюкова*
Компьютерная верстка *С. Н. Маслюковой*

ISBN 978-5-9266-1796-9



Подписано в печать 20.08.2021. Формат 60х84 1/16.
Усл. печ. л. 2,8. Тираж 30 экз. Заказ 563.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.