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

Кафедра криминалистики

О. П. Бердникова
Н. А. Андроник

Особенности расследования хищений, совершенных с использованием IT-технологий

Учебно-практическое пособие

Екатеринбург
2022

ББК 67.523.12
Б483

Бердникова О. П.

Б483 ***Особенности расследования хищений, совершенных с использованием IT-технологий:*** *учебно-практическое пособие* / О. П. Бердникова, Н. А. Андроник. – Екатеринбург: Уральский юридический институт МВД России, 2022. – 72 с.

ISBN 978-5-88437-853-7

Рецензенты: **А. Л. Пермяков,** заместитель начальника кафедры криминалистики Восточно-Сибирского института МВД России, кандидат юридических наук, доцент;
А. В. Шебалин, заместитель начальника кафедры криминалистики Барнаульского юридического института МВД России, кандидат юридических наук, доцент

В учебно-практическом пособии раскрывается криминалистическая характеристика хищений, совершенных с использованием IT-технологий, организационно-тактические аспекты расследования данных преступлений. Рассматривается порядок назначения судебных экспертиз, а также вопросы, которые следует формулировать в постановлении о назначении экспертизы. Использование учебно-практического пособия в образовательном процессе позволит повысить уровень теоретических и практических навыков по расследованию отдельных видов преступлений.

Издание предназначено для курсантов и слушателей образовательных организаций системы МВД России, обучающихся по специальностям 40.05.01 Правовое обеспечение национальной безопасности, 38.05.01 Экономическая безопасность, направлению подготовки 40.03.02 Обеспечение законности и правопорядка, сотрудников территориальных органов внутренних дел Российской Федерации.

Обсуждено на заседании кафедры криминалистики УрЮИ МВД России (протокол № 1 от 12 января 2022 г.).

Рекомендовано к использованию в образовательном процессе методическим советом УрЮИ МВД России (протокол № 6 от 7 февраля 2022 г.).

ISBN 978-5-88437-853-7 ББК 67.523.12

Введение

Развитие компьютерных технологий расширило возможность применения мобильной связи и банковских мобильных приложений, интернет-банкинга, как в повседневной жизни, так и производственной деятельности. Одновременно с позитивными тенденциями развития современного общества не только совершенствуются информационно-телекоммуникационные технологии, но и создаются предпосылки для их использования в преступных целях. В результате появилось целое направление вредоносного мобильного программного обеспечения, которое подменяет интерфейсы мобильных магазинов, производителей и банковских мобильных приложений, перехватывает СМС. Преступления, совершенные с использованием современных информационных технологий, являются одним из наиболее развивающихся видов интеллектуальной преступности. Лицо, совершая общественно опасное деяние, не только причиняет имущественный вред, но и посягает на национальную безопасность страны. Продолжается рост хищений, совершенных с использованием кредитных и расчетных карт. Следователь (дознаватель) при расследовании преступлений в большинстве случаев сталкивается с противодействием расследованию. Для преодоления противодействия следователю (дознавателю) необходимо в полном объеме обладать теоретическими знаниями частной криминалистической методики расследования конкретного вида преступлений. В настоящее время, как показывает опыт правоприменительной практики, имеются определенные трудности при расследовании хищений с использованием IT-технологий из-за недостаточности методик расследования указанных преступлений.

Состав преступлений, связанных с хищением чужого имущества, совершенных с использованием информационно-телекоммуникационных технологий, охватывается п. «г» ч. 3 ст. 158, 159.3, 159.6 УК РФ. Количество IT-преступлений за период с января по июнь 2021 г. по сравнению с 2020 г. выросло на 81,4 %, а удельный вес таких деяний достиг 19,9 % от общего числа[1].

Актуальность работы обусловлена необходимостью получения обучающимися систематизированных знаний в методике расследования хищений, совершенных с использованием IT-технологий. Использование пособия в деятельности сотрудников правоохранительных органов позволит повысить уровень знаний и практических навыков по осуществлению служебных обязанностей, а также сформировать профессиональные компетенции у сотрудников органов внутренних дел.

[1] См.: Судебный департамент при Верховном Суде РФ. URL: http//www.cdep.ru (дата обращения: 15.09.2021).

Основной целью работы является разработка теоретических положений и практических рекомендаций по организации расследования хищений, совершенных с использованием IT-технологий. Обеспечение сотрудников органов внутренних необходимыми знаниями в особенностях расследования указанных преступлений, а также подготовка обучающихся в образовательных организациях системы МВД России к будущей профессиональной деятельности.

Данная цель достигается путем решения следующих задач:

– ознакомление обучающихся с нормативно-правовыми актами, регламентирующими методику расследования хищений, совершенных с использованием IT-технологий;

– изучение криминалистической характеристики отдельных видов преступлений;

– изучение криминалистических средств и методов, используемых в раскрытии и расследовании преступлений;

– освоение обучающимися организации первоначального этапа расследования преступлений;

– овладение обучающимися особенностями тактики производства следственных действий в ходе расследования преступлений;

– формирование навыков предупреждения, пресечения, выявления, раскрытия и расследования хищений, совершенных с использованием IT-технологий.

Учебно-практическое пособие способствует освоению элементов криминалистической характеристики хищений, совершенных с использованием IT-технологий; особенностей возбуждения уголовного дела; особенностей организации первоначального этапа расследования указанных преступлений в типичных следственных ситуациях; специфики использования специальных знаний; тактики производства отдельных следственных действий, и формированию следующих профессиональных компетенций в правоприменительной деятельности:

– способности проводить следственные действия, оформлять и использовать данные, полученные в результате их проведения;

– способности применять специальные знания при проведении первоначальных и других следственных действий;

– способности выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения;

– способности применять в профессиональной деятельности теоретические основы раскрытия и расследования преступлений, использовать в целях установления объективной истины по конкретным делам, технико-криминалистические методы и средства, тактические приемы производства следственных действий, формы организации и методику раскрытия и расследования отдельных видов и групп преступлений;

– способности реализовывать мероприятия по получению юридически значимой информации, проверять, анализировать, оценивать ее и использовать в интересах предупреждения, пресечения, раскрытия и расследования преступлений;

– способности организовывать работу малого коллектива исполнителей, планировать и организовывать служебную деятельность исполнителей, осуществлять контроль и учет ее результатов.

При разработке учебно-практического пособия использовались действующие нормативные правовые акты, акты судебных органов, учебная и научная литература, а также информация, размещенная на официальных сайтах.

Глава 1. Криминалистическая характеристика хищений, совершенных с использованием IT-технологий

Проблема методики расследования преступлений в криминалистической науке рассматривается со времен Г. Гросса. Австрийский ученый Ганс Гросс, который впервые ввел в научный оборот сам термин «криминалистика», разработал отдельные направления методики расследования преступлений, основываясь на данных судебной практики. Он предложил классифицировать методику расследования преступления на отдельные элементы: способы подготовки, совершения и сокрытия преступления, механизм следообразования и т. п., выделив в качестве составной части методики расследования преступления криминалистическую характеристику преступления[1].

Известный советский ученый, профессор Р. С. Белкин предложил понимать под криминалистической методикой расследования «систему научных положений и разрабатываемых на их основе рекомендаций по организации и осуществлению расследования и предотвращения отдельных видов преступлений»[2].

Поскольку криминалистическая методика расследования носит вспомогательный характер, она содержит рекомендации, а не прямые указания или руководство к действию. Это обусловлено тем, что органы следствия и дознания сталкиваются в своей деятельности с непосредственными событиями и ситуациями, исходя из которых, применяют или не применяют знания из методик расследования преступлений. Обратного порядка быть не может, поскольку методика хоть и носит обобщающий характер, но не универсальна. Так автор, разрабатывая частную методику расследования, исходит из анализа уже сложившейся практики по конкретному виду преступлений и может добавить свое суждение по тому или иному вопросу, применяя научные теоретические знания, но не в состоянии предусмотреть всех вариантов развития событий и предугадать все способы совершения исследуемого вида преступлений[3].

Криминалистическая характеристика – это термин, существующий в криминалистике примерно с середины двадцатого столетия. Несмотря на столь долгое существование, споры о структуре, видах криминалистической характеристики и ее целесообразности продолжаются. Впервые в криминалистической литературе этот термин появился в 1966 г. в первой главе

---

[1] См.: *Гросс Г.* Руководство для судебных следователей как система криминалистики. М., 2002 (перепеч. с изд. 1908 г.). С. 158.

[2] *Белкин Р. С.* Курс криминалистики. М., 2001. С. 237.

[3] См.: *Андроник Н. А., Виноградова О. П.* Расследование преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ: курс лекций. Екатеринбург: Урал. юрид. ин-т МВД России , 2018. С. 7.

диссертационного исследования Л. А. Сергеева «Криминалистическая характеристика хищений, совершаемых при производстве строительных работ». В 1967 г. А. Н. Колесниченко использовал термин «криминалистическая характеристика» в автореферате своей докторской диссертации как наиболее существенный элемент, общий для всех частных криминалистических методик. Необходимо заметить, что впервые о криминалистической характеристике было сказано еще в 1927 г. профессором Ленинградского государственного университета П. И. Люблинским, который, однако, вкладывал в это понятие несколько иной смысл, говоря о криминалистической характеристике того происшествия, которое предстоит расследовать[1].

К числу общих относятся следующие положения: строгое и неуклонное соблюдение законности; индивидуальность и динамичность расследования; планомерность, всесторонность, полнота, объективность расследования; использование данных криминалистической характеристики преступлений; эффективное использование научно-технических средств, приемов и методов при расследовании.

Рассматривая криминалистическую характеристику хищений с использованием IT-технологий в структуре частной криминалистической методики, целесообразно исследователь термины «компьютерная преступность», «киберпреступность». На наш взгляд, данные термины тождественны. Смысл термина «компьютерная преступность» заключается в использовании компьютера при совершении преступлений. В свою очередь, под компьютером принято понимать любую вычислительную технику, способную выполнять заданные программные действия. Наиболее распространенными видами ее являются: планшет, ноутбук, стационарный компьютер, смартфон, электронная книга, карманный компьютер и ноутбук[2].

Сеть четвертого поколения (LTE) является самой развитой сетью на сегодняшний момент времени. Данная сеть позволяет получить мгновенный доступ к глобальной сети с преимуществом в скорости и качестве по сравнению с возможностью подключения к сети с помощью обычного персонального компьютера.

В настоящее время сеть «Интернет» является общедоступным полем с рядом положительных для преступника преимуществ: простота в пользовании сетью, обеспечение анонимности пользования, высокие скорости передачи данных. Под воздействием развития информационной и компьютерной среды меняется и киберпреступность, включая в себя ряд новых преступлений.

Ряд отечественных исследователей отмечают, что киберпреступность связывается с преступлениями, совершение которых происходит в различных информационных сетях.

---

[1] См.: *Андроник Н. А., Виноградова О. П.* Указ. соч. С. 10.

[2] См.: Разновидности компьютерной техники. URL: http://inphormatika.ru/comp_ (дата обращения: 10.11.2021).

Так, С. В. Воронцов отмечает, что «термин «киберпреступность» используется для определения преступности в виртуальном пространстве, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленных в локальных и глобальных сетях»[1].

В. А. Дуленко, Р. Р. Мамлеев, В. А. Пестриков считают, что «киберпреступность» – это любое преступление, совершенное с помощью компьютерной сети, т. е. любое преступление, совершенное в электронной среде[2].

Преступления, совершаемые с использованием IT-технологий – это преступления, совершаемые в информационной среде, в которой компьютерная информация, информационные ресурсы и компьютерная техника являются средствами совершения преступления.

Применительно к особенностям расследования хищений с использованием IT-технологий рассмотрим элементы криминалистической характеристики данных преступлений.

Структура частной криминалистической методики включает:

1. Предметом преступного посягательства, предусмотренного *п. «г» ч. 3 ст. 158 УК РФ,* являются денежные средства, находящиеся на банковском счете, а равно электронные денежные средства; предметом преступления, предусмотренного *ст. 159.3 УК РФ* являются безналичные денежные средства.

Рассмотрим понятие безналичных денежных средств и электронных денежных средств.

Безналичные денежные средства – это одно из средств платежа, которым осуществляются расчеты на территории Российской Федерации, наряду с другим средством платежа – наличными расчетами (ст. 140 ГК РФ)[3].

Безналичные денежные средства, наличные денежные средства (банкноты и монеты Российской Федерации) относятся к валюте Российской Федерации, согласно подп. «б» п. 1 ст. 1 Федерального закона от 10 декабря 2003 г. № 173-ФЗ «О валютном регулировании и валютном контроле» (средства на банковских счетах и в банковских вкладах)[4].

Электронные деньги относятся к безналичным денежным средствам. Об этом говорит постановление Пленума Верховного Суда Российской Федерации № 1 от 26 февраля 2019 г. «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 32

---

[1] См.: *Воронцова С. В.* Киберпреступность: проблемы квалификации преступных деяний // Российская юстиция. 2011. № 2. С. 14–15.

[2] См.: *Дуленко В. А.* Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации. Уфа, 2017. С. 27.

[3] Гражданский Кодекс Российской Федерации: Федеральный закон от 30.11.1994 № 51-ФЗ (действ. ред.). URL: www //http:garant.ru.

[4] Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле». URL: www //http:garant.ru.

“О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем”»: «в абзаце втором слова “безналичные и электронные денежные средства заменены на безналичные денежные средства, в том числе электронные денежные средства”»[1]. О том же говорится и в п. 5 постановления Пленума Верховного Суда Российской Федерации № 48 от 30 ноября 2017 г. «О судебной практике по делам о мошенничестве, присвоении и растрате»[2].

Электронное средство платежа – средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств[3]. Средством осуществления преступной деятельности является поддельная или принадлежащая другому лицу кредитная, расчетная или иная платежная карта.

Предметом преступления, предусмотренного *ст. 159.6 УК РФ*[4], являются денежные средства; сведенья личного характера, которые могут скомпрометировать потерпевшего. Так, например, самыми распространенными являются пароли от аккаунтов разных социальных сетей, номера платежных карт и другие сведения подобного характера; право как на движимое, так и на недвижимое имущество. Как правило, это квартиры, дома, автомобили и драгоценные украшения[5]. Средством хищения чужого имущества или приобретения права на чужое имущество является компьютерная информация.

Анализируя предмет преступного посягательства, следует отметить, что по рассматриваемым категориям уголовных дел, предметом выступают де-

---

[1] Постановление Пленума Верховного Суда Российской Федерации № 1 от 26.02.2019 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 07.07.2015 № 32 “О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем”». URL: www //http:garant.ru.

[2] Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». URL: www//http:garant.ru.

[3] См.: *Ушаков А. Ю., Саакян А. Г., Поздышев Р. С., Степанова М. А*. Особенности квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей: метод. рекомендации. Н. Новгород: Нижегород. академия МВД России, 2020. С. 7.

[4] Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (действ. ред.). URL: www //http:garant.ru.

[5] См.: *Бердникова О. П.* Особенности первоначального и последующего этапов расследования мошенничества в сфере компьютерной информации: учеб. пособие. Екатеринбург: Урал. юрид. ин-т МВД России, 2019. С. 12.

нежные средства в безналичной форме, находящиеся на расчетном счете потерпевшего (представителя потерпевшего), распоряжение которыми возможно на удаленном расстоянии. С учетом развития информационно-телекоммуникационных технологий и обладаниями специальными знаниями отдельных категорий граждан, система хранения денежных средств становится все более уязвимой. С целью оказания противодействия правоохранительным органам по раскрытию преступления преступники переводят похищенные денежные средства через несколько счетов перед тем, как определенная сумма денежных средств поступит на их счет.

2. *Обстановка совершения преступления* является одним из основных элементов криминалистической характеристики преступления, определяющих развитие следственной ситуации. Обстановка совершения преступления включает в себя место, в котором осуществлялось преступное действие и время.

Применительно к данной категории уголовных дел место совершения преступления необходимо дифференцировать в зависимости от способа совершения преступления:

– служебное, жилое помещение, в котором имеется доступ в сеть «Интернет». Для совершения хищений используют компьютеры, ноутбуки, планшеты, имеющие техническую возможность для совершения операций. С целью оказания противодействия раскрытию и расследованию преступлений преступники принимают меры к сокрытию следов, меняя место своего пребывания. Так, преступник на этапе подготовки к совершению преступления с целью скрыть место преступления арендует помещения, при этом часто старается менять данные места, чтобы остаться незамеченным;

– возможность совершения хищений с использованием IT-технологий при помощи планшетов, ноутбуков, мобильных телефонов вне нахождения преступника в каком-либо помещении. При этом лицо может находиться на улице, при условии, что имеется доступ в сеть «Интернет»;

– хищение в торговых центрах с доступом открытого WI-FI путем захвата трафика других пользователей. Преступник запускает сканер и таким образом видит информацию, которую скачивают или передают другие пользователи. Следует отметить, что местом совершения преступления может быть метрополитен или вагон в поезде, где, соответственно, также имеется доступ к открытому WI-FI.

В отличие от места совершения преступления, место происшествия характеризуется наличием следовой картины. Для данной категории уголовных дел выделяют:

– место, где расположена компьютерная информация;

– место, где наступили вредные последствия;

– место, где производились преступные действия (осуществлялся доступ в компьютерную сеть). Перечисленные места могут совпадать, могут и от-

личаться друг от друга. Таким образом, мест происшествия может быть множество[1].

Местом совершения хищений, совершенных с использованием интернет-технологий, являются как конкретные точки и участки территории, так и те учреждения, организации, предприятия и системы, в которых используется то или иное средство электронно-вычислительной техники в какомлибо технологическом процессе. Следовательно, по делам данной категории мест совершения преступных посягательств может быть несколько, в том числе значительно удаленных друг от друга и расположенных как в разных странах, так и на различных континентах. Последнее возможно по причине практически неограниченного радиуса действия и мобильности электронных средств связи и телекоммуникаций, неотъемлемой частью которых являются СВТ.

Ярким примером этому может служить одно из уголовных дел, расследование которого осуществлялось отечественными правоохранительными органами в тесном контакте с правоохранительными органами США. Уголовное дело было возбуждено в отношении 13 граждан Российской Федерации и Нидерландов, которые вступили в сговор с целью похищения денежных средств в крупных размерах, принадлежащих «City Bank of America», расположенному в Нью-Йорке. Образовав устойчивую преступную группу, они в период с конца июня по сентябрь 2011 г., используя электронную компьютерную систему телекоммуникационной связи «Интернет» и преодолев семь рубежей многоконтурной защиты от несанкционированного доступа, с помощью персонального компьютера из офиса АО «Сатурн», находящегося в городе Санкт-Петербурге, входили в систему управления[2].

Время совершения преступлений рассматриваемой категории лишь в относительно редких случаях устанавливается с точностью до дня и очень редко – до часов и минут. Такая точность обычно требуется при выявлении отдельных эпизодов преступной деятельности. Как правило, время совершения данных преступных деяний исчисляют различными по продолжительности периодами, связанными с деятельностью определенных лиц или организаций. При этом согласно ч. 2 ст. 9 УК РФ временем совершения каждого преступления признается время окончания общественно опасного деяния независимо от момента наступления последствий.

3. Способ совершения преступления выражает функциональную сторону преступной деятельности, позволяет установить не только, каким путем

---

[1] См.: *Грибунов О. П., Старичков М. В.* Расследование преступлений в сфере компьютерной информации и высоких технологий: учеб. пособие. М.: ДГСК МВД России, 2017. С. 57.

[2] См.: *Вехов В. Б.* Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учеб.-метод. пособие. Волгоград: Перемена, 1998. С. 50.

подготавливалось, совершалась и скрывалось преступление, но и какие действия преступника отразились в окружающей среде, то есть какие следы образовались в результате преступных действий. Способ позволяет выдвинуть версии о профессиональных навыках преступника.

Рассматривая способы совершения данных преступлений, необходимо обратиться к постановлению Пленума Верховного Суда РФ « О судебной практике по делам о мошенничестве, присвоении и растрате», согласно которому вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) – ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующими программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него[1].

Способы совершения *преступлений* представляют собой основную и важную часть криминалистической характеристики преступления. В свою очередь, способ состоит из подготовительного этапа, непосредственно совершения преступления и сокрытия преступления. Следует отметить, что не всегда механизм совершения преступления состоит из трех этапов. Возможно, преступление совершается без подготовки, и преступником не были предприняты попытки по сокрытию.

Особенностью расследования хищений с использованием IT-технологий является тщательно продуманный способ подготовки к совершению преступления. На этапе подготовки принимаются меры к сокрытию следов, придумываются способы конспирации в ходе осуществления преступной деятельности, сопряженной с созданием, использованием и распространением вредоносных программ. Вредоносные программы дистанционно выводят из рабочего состояния заразившиеся устройства с уничтожением данных, хранящихся на них, что, в свою очередь, не позволяет в дальнейшем производить программно-технические судебные экспертизы по изъятым устройствам с целью установления механизма хищения денежных средств.

Одним из распространенных способов хищения денежных средств граждан, осуществляемого с использованием информационно-телекоммуникационных технологий, на сегодняшний день является неправомерный доступ

[1] Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

к их расчетным счетам. Согласно примечанию к ст. 272 УК РФ под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Компьютерная информация – это электронная информация, содержащаяся на машинном носителе, передаваемая путем использования информационно-телекоммуникационной сети.

Особенностью способа совершения хищений с использованием IT-технологий является минимальное участие человека в процессе совершения преступлений.

В настоящее время очень развита такая система дистанционного банковского обслуживания, как «Мобильный банк» (например, «Сбербанк-онлайн», онлайн «ВТБ», «Home Credit bank» и др.», которые позволяют гражданам управлять своими денежными средствами в любом месте, не посещая отделение банка). С помощью мобильных приложений, установленных на смартфоны либо на компьютеры, можно осуществлять платежи за коммунальные услуги, отправлять переводы физическим лицам, производить платежи по кредитам, оплачивать налоги, штрафы, открывать счета или вклады и многое другое. Практически большая часть населения Российской Федерации пользуется данными приложениями, которые созданы для удобства граждан, но и преступники используют созданные условия в своих корыстных целях. Они осуществляют рассылку на электронную почту граждан или СМС-сообщения на номера мобильных телефонов, подключенных к мобильному банку, с предложениями якобы от банка, например, о предоставлении кредита на выгодных условиях, или сообщений о подозрительных операциях по счету, где указывают ссылку, по которой необходимо перейти в личный кабинет для проверки или подтверждения указанной информации.

Рассмотрим наиболее распространенные способы краж с банковского счета, что актуально и в отношении электронных денежных средств:

- хищения денежных средств при помощи дистанционного доступа к мобильным устройствам или персональным компьютерам, «зараженным» вредоносными программами: потерпевшие, используя сеть «Интернет», заражают свою компьютерную технику вредоносным программным обеспечением, а преступник через это программное обеспечение получает доступ к мобильному устройству сотовой связи или компьютерной технике и похищает денежные средства;
- хищения денежных средств, связанные с несанкционированным доступом к банковской карте потерпевшего через абонентский номер, ранее находившийся в пользовании последнего, с подключенной услугой «Мобильный банк»;

- хищения денежных средств, совершенные с использованием предварительно зафиксированных субъектом преступления (в частности банковским работником) реквизитов банковской карты;
- хищения денежных средств, связанные со скимингом, который заключается в установке на банкомат специального оборудования, считывающего данные магнитной полосы банковской карты с целью создания поддельных карт-дубликатов.

Рассмотрим типичные способы хищений денежных средств с использованием электронных средств платежа:

– хищение банковской карты у владельца или находка банковской карты с целью ее дальнейшего использования для оплаты товара/услуг или снятия денежных средств посредством банкомата, когда не требуется введения ПИН-кода.

Например, приговором Миасского городского суда Челябинской области К. признан виновным в совершении преступления, предусмотренного ч. 2 статьи 159.3 УК Российской Федерации, то есть мошенничества с использованием электронных средств платежа с причинением значительного ущерба гражданину, при следующих обстоятельствах.

К., находясь в состоянии алкогольного опьянения в гостях у знакомого, с корыстной целью, в ходе распития спиртных напитков воспользовавшись тем, что потерпевший оставил на шкафу в комнате оформленную на его имя и не представляющую материальной ценности дебетовую карту ПАО «Почта Банк» с находящимися на лицевом счету лимитом денежных средств в сумме 9217 рублей 82 копеек, тайно завладел ею и, желая личного обогащения за чужой счет путем хищения денежных средств с банковского счета, открытого в ПАО «Почта Банк», путем обмана работников торговых организаций и умолчания о незаконном владении им платежной картой в магазинах, расположенных на территории г. Миасса, используя вышеуказанную дебетовую карту, произвел безналичные расчеты.

Таким образом, К. незаконными действиями причинил значительный ущерб потерпевшему на общую сумму 8811 рублей 80 копеек[1];

– присвоение банковской карты владельца с целью дальнейшего использования как электронного средства платежа в отношении кассира магазина, сотрудника банка.

Так, Д. 17 октября 2018 г. приехал в г. Барнаул к своему знакомому, в этот же день он в баре «Заправка» познакомился с потерпевшим, который рассчитывался за спиртное банковской картой, не вводя при этом в терминале пин-код. Потерпевший передал свою карту Д., чтобы тот приобретал спиртные напитки. После закрытия бара Д. проводил потерпевшего домой

[1] Приговор Миасского городского суда Челябинской области. URL: https://sudact.ru/regular/doc/vG70dKMsd6Yj/ (дата обращения: 11.10.2021).

и, вспомнив, что у него осталась банковская карта последнего, решил похитить с нее денежные средства путем безналичной оплаты товаров, стоимость которых не превышает 1000 рублей (чтобы не вводить пин-код).

Таким образом, Д., осознавая противоправный характер своих действий, действуя с единым умыслом, в период с 02-00 до 21-00 часа 18 октября 2018 г., используя для оплаты товаров в различных магазинах г. Барнаула электронное средство платежа – банковскую карту ПАО «Сбербанк России», принадлежащую потерпевшему и привязанную к банковскому счету ПАО «Сбербанк России», умалчивая перед работниками торговых организаций о принадлежности указанной карты иному лицу, то есть путем их обмана, похитил денежные средства потерпевшего на общую сумму 3392 рубля 50 копеек[1];

– использование скиммингового устройства, путем установки скрытой видеофиксации с целью визуального наблюдения снятия денежных жертв лицом (в дальнейшем жертвой) для запоминания пин-кода банковской карты последнего.

Так, 22.07.2014 неустановленное лицо из корыстных побуждений, незаконно проникнув в банкомат «ВТБ 24» (ЗАО), расположенный в ТЦ «Колизей-Атриум» по адресу: г. Пермь, ул. Ленина, д. 60, тайно похитило денежные средства в особо крупном размере на сумму 1 427 000 рублей, которые принадлежали «ВТБ 24» (ЗАО), тем самым причинив «ВТБ 24» (ЗАО) имущественный вред на указанную сумму. В ходе предварительного следствия были задержаны лица, причастные к совершению данного преступления;

– использование служебного положения сотрудником банка, владеющим информацией о банковском счете владельца и с корыстной целью использующим полученные сведения.

Проанализируем правоприменительную практику. М. в период с 08.11.2016 по 18.07.2018 в силу исполнения своих должностных обязанностей, являясь лицом, выполняющим организационно-распорядительные функции в коммерческой организации, имела доступ к досье клиентов и информации о состоянии счетов, вкладов и банковских операциях по счетам клиентов ПАО «УБРиР» посредством доступа к Централизованной Автоматизированной Банковской Системе «Банк XXI Век», а также программе «SAPCRM», в которой хранятся персональные данные клиентов банка, при этом для выполнения операций в указанных программах М. была наделена персональным логином и паролем.

Преступление было совершено при следующих обстоятельствах: М. вступила в предварительный сговор с С., направленный на хищение денежных средств в особо крупном размере с помощью Централизованной Автоматизированной Банковской Системы. Так, С., реализуя совместный с М.

[1] Приговор Железнодорожного районного суда г. Барнаула Алтайского края. URL: https://sudact.ru/regular/doc/WO4C8QmPo7Z5/ (дата обращения: 11.10.2021).

преступный умысел с целью изготовления поддельных платежных поручений о переводе денежных средств с расчетного счета ООО «Авангард» и внесения в них заведомо ложных сведений, приискал сведения о расчетных счетах физических лиц, а также банковские карты, выпущенные в рамках обслуживания этих счетов, необходимые для осуществления неправомерного перевода денежных средств с расчетного счета ООО «Авангард». После чего денежные средства свыше 5 000 000 рублей с расчетного счета ООО «Авангард» были переведены на банковские карты физических лиц с помощью Централизованной Автоматизированной Банковской Системы.

Другой пример. М., используя свои познания в области компьютерной техники, совместно с другими лицами создал и распространил вредоносную программу, приводящую к несанкционированному уничтожению, блокированию, модификации, копированию и нейтрализации средств защиты охраняемой законом компьютерной информации на компьютере ключевых пользователей и других элементах инфраструктуры Сибирского филиала Банка «Т», и использовал ее для совершения хищения денежных средств со счета банка, а также совершил неправомерный (не санкционированный его обладателем – Сибирским филиалом Банка «Т») доступ к охраняемой законом компьютерной информации, повлекший ее уничтожение, блокирование, модификацию и копирование. В результате указанных преступных действий произошло несанкционированное списание денежных средств в сумме 99 705 000 рублей, которые были перечислены в различных суммах на подконтрольные участникам организованной группы банковские счета не осведомленных о преступном умысле соучастников – физических лиц в кредитных организациях, которые были переданы ими в распоряжение участников преступной группы. После чего преступники обналичивали вышеуказанные похищенные денежные средства путем получения наличных денег в различных банкоматах в соответствии с установленной схемой распределения преступной прибыли[1].

Для мошенничества в сфере компьютерной информации бывает единый умысел на совершение мошеннических действий в отношении многих потерпевших (например, когда применяется способ, предполагающий автоматическое срабатывание вредоносного программного обеспечения, в результате чего происходит изъятие денежных средств у множества потерпевших, и виновный даже не в состоянии определить, какое количество лиц страдает в результате преступных действий и каков будет окончательный размер ущерба)[2].

---

[1] Приговор Кировского районного суда г. Екатеринбурга в отношении М. по ч. 2 ст. 273, ч. 3 ст. 272 и ч. 4 ст. 159.6 УК Российской Федерации. URL: https://sudact.ru/regular/doc/YwQr7ZHgaQgR/ (дата обращения: 11.10.2021).

[2] См.: *Уханова Н. В., Иванов Д. А.* Расследование преступлений против собственности: учеб. пособие. М.: Моск. ун-т МВД России им. В. Я. Кикотя, 2019. С. 137.

Так, приговором Фрунзенского районного суда г. Саратова М. признана виновной в совершении преступления, предусмотренного п. «а» ч. 3 ст. 159.6 УК Российской Федерации.

3 января 2017 г. М., работая в должности специалиста по сопровождению корпоративных клиентов Поволжского филиала – Саратовского регионального отделения ПАО «МегаФон», из корыстных побуждений умышленно, используя свое служебное положение, путем модификации компьютерной информации в информационно-биллинговой системе ПАО «МегаФон» незаконно осуществила перевод денежных средств в сумме 7 269 руб. 84 коп., принадлежащих ПАО «МегаФон», со счета МУ МВД России «Энгельсское» по Саратовской области на свой лицевой счет, зарегистрированный на вымышленное имя «Зотова Н.Н.» и находящийся в пользовании М., похитив тем самым указанные денежные средства и получив реальную возможность ими распоряжаться[1].

Ученый-процессуалист И. Е. Мазуров выделяет следующие способы хищений с использованием IT-технологий.

1. Проникновение непосредственно в помещение, где находится компьютерное оборудование (жилище или офис), физический доступ к компьютерно-техническим аппаратам и последующее получение информации[2].

2. Доступ внешний, при помощи удаленных устройств. Доступ дистанционный к компьютерно-техническим аппаратам при помощи интернет-технологий с дальнейшим получением данных.

3. Шифрование входной либо выходной информации, управляющих команд и команд доступа, запутывание путей для проникновения.

4. Изменения в компьютерных программах, разработка вредоносных программных средств для уничтожения сведений и вывода компьютерно-технического устройства из строя.

5. Создание спама. Распространение сведений для продвижения информации или рекламы.

6. Незаконное распространение сведений, программного обеспечения, правовых систем, книг, которые содержат компьютерные данные.

7. Способы комплексные[3].

Преступниками чаще прочих (43 %) применяются способы хищений с применением специализированных интернет-технологий, перечисленных ниже:

---

[1] Приговор Фрунзенского районного суда г. Саратова в отношении М. по п. «а» ч. 3 ст. 159.6 УК Российской Федерации. URL: https://sudact.ru/regular/doc/qtCZQWKOpk5x/t (дата обращения: 11.10.2021).

[2] Часть 1 статьи 1 закона РФ от 23.09.92 № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных». URL: www //http:garant.ru

[3] См.: *Вехов В. Б.* Компьютерные преступления: способы совершения и раскрытия / под ред. акад. Б. П. Смагоринского. М.: Право и Закон, 1996. С. 167.

1. Бесконтактный (пассивный) перехват – дистанционное осуществление перехвата электромагнитных излучений, которые испускают при работе компьютерно-технические средства обеспечения данными для сбора сведений при подготовке к хищениям, осуществляемым при использовании интернет-технологий (перехватывание электромагнитных, оптических, акустических сигналов и т. д.).

2. Контактный (активный) перехват в процессе подготовки к хищениям, осуществляемый с применением интернет-технологий, производится с помощью подключения непосредственно к компьютерно-техническому устройству, компьютерным системам, их сети либо системам передачи информации разнообразных радиоэлектронных и специализированных технических средств (непосредственно «РЭС» либо «СТС»), добытых разнообразными способами, оперативно-технических, штатных либо специально разработанных, изготовленных, приспособленных, запрограммированных.

3. Применение для компьютерно-технических устройств вредоносных программ, которое заключается в негласном внедрении какими-либо способами в сеть или систему устройства. Используются специализированные программы разных типов: разведывательного направления: «троянская матрешка», «троянский конь» и т. д.[1]

4. Уничтожающие компьютерные данные и повреждающие средства хранения информации (МНИ), передачи и обработки – «компьютерный вирус», «временная» либо «логическая бомба», что помогает собрать объем необходимых сведений при подготовке к хищениям, осуществляемым с применением интернет-технологий[2].

Значительное место в криминалистической характеристике занимает *механизм следообразования*. Механизм следообразования состоит из специфичных следов и типичных средств совершения преступления.

При применении таких способов специфичные следы представляют собой:

- скрипты вредоносных вирусов;
- информацию о процессах, происходящих в системе;
- информацию о соединениях с интернет-ресурсами;
- скрытую информацию, содержащуюся в файле (методанные);
- данные о входящей и исходящей информации, технических характеристиках поступившего письма;
- следы рук, оставшиеся на технических приборах либо магнитных носителях, разнообразных проводах либо вспомогательных приспособлениях;

[1] См.: *Мазуров И. Е.* Методика расследования хищений, совершенных с использование интернет-технологий: дис. … канд. юрид. наук. Казань. 2017. С. 105.

[2] Статья 1 закона РФ от 23.09.92 № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных». URL: www //http:garant.ru.

следы соединительных проводов, материалов для изоляции, капельки припоя, флюса, канифоли;

- признаки проплавления, надреза, прокола изоляции на проводах компьютерно-технических устройств обеспечения информацией, обнаружения участков механического сдавливания, а также приклеивания посторонних предметов;
- признаки фальсификаций первичных документов, которые отражают перемещение компьютерной документированной информации либо операции, которые с их помощью были произведены.

Так, сотрудниками отдела «К» МВД по Чувашской Республике совместно с коллегами из Управления «К» МВД России при содействии экспертов Group-IB в августе 2019 г. задержан мошенник, совершавший хищения денежных средств с банковских карт граждан с использованием вредоносного программного обеспечения. Распространение вышеуказанного ПО происходило путем маскировки его под популярное приложение для мобильных устройств. После установки пострадавшим приложения на свой смартфон автоматически загружалось вредоносное ПО, предоставлявшее преступнику доступ к системе мобильного банкинга. В ходе проведенных оперативно-розыскных мероприятий оперативниками был задержан молодой человек. В результате обыска, проведенного полицейскими по месту жительства подозреваемого, были обнаружены и изъяты компьютерная техника, жесткие диски, флэш-накопители, телефоны и SIM-карты[1].

Таким образом, правильно исследованная следовая картина позволит в кратчайшие сроки раскрыть и расследовать преступление.

Типичные средства совершения такого преступления – компьютер, ноутбук, мобильный телефон, планшет:

– предназначенные для работы в непосредственной близости либо дистанционно, блокирования, модификации, уничтожения компьютерных данных с технического оборудования для их передачи и обработки;

– программное обеспечение для хищения информации (вредоносные программы);

– программы для осуществления брутфорса (автоматический подбор пароля);

– современные программы-сканеры для захвата трафика и хищения информации со стандартным программным обеспечением и транзитные (промежуточные) МНИ.

Правильное уяснение механизма следообразования и закрепление в протоколах следственных действий имеет важное значение для методики рас-

[1] Приговор Канашского районного суда Чувашской республики. URL: https://мвд.рф/news/item/18090010 (дата обращения: 17.11.2021).

следования указанных преступлений, так как это фактически определяет сущность всех исходных данных для организации расследования.

Рассматривая *личность преступника* как один из элементов криминалистической характеристики преступления, следует отметить существенное различие личности преступников, совершающих преступление против жизни и здоровья, собственности и преступления экономической направленности. Во-первых, существенное различие по морально-психологическим критериям. Во-вторых, возрастной и образовательный ценз. В связи с появлением и увеличением роста преступлений с использованием IT-технологий появляется и относительно «новая» личность правонарушителя. Компьютерный мир сформировал свою субкультуру, свой язык. Компьютерных правонарушителей на жаргонном языке называют:

– «хакерами» – это лица, занимающиеся несанкционированным поиском способов получения неправомерного доступа к компьютерной информации;

– «крэкерами» – это лица, занимающиеся «взломом» систем защиты охраняемой законом компьютерной информации;

– «фрикерами» – это лица, уклоняющиеся от оплаты телекоммуникационных услуг с использованием конфиденциальной компьютерной информации;

– «кардеры» – это специалисты по снятию с программного обеспечения зашиты от копирования[1].

На наш взгляд, личность компьютерного преступника можно дифференцировать по следующим основаниям:

– это лица с физико-математическим образованием, знают новые компьютерные технологии. На достаточно высоком уровне владеют практическими навыками. В большинстве случаев (97 %) преступники, совершавшие хищения с применением интернет-технологий, были служащими государственных организаций или учреждений. Обычно указанные лица ранее преступления не совершали, положительно характеризовались по месту работы и являлись высококвалифицированными специалистами. У данных лиц на высоком уровне сформированы навыки в сфере информационно-телекоммуникационных технологий, умение грамотного и четкого систематизации информационного материала. Такие особенности криминалистической характеристики преступника, как правило, являются следствием его технического образования.

Оценивая данный элемент криминалистической характеристики в криминалистическом аспекте, можно выявить следующую закономерность: хищения в сфере высоких технологий в подавляющем большинстве совершаются людьми с техническим складом ума, характеризующихся логичностью и последовательностью выбранных действий;

[1] См.: *Грибунов О. П., Старичков М. В.* Указ. соч. С. 24 (160).

– лица, увлеченные компьютерной техникой. Данные лица могут быть школьниками, студентами, еще не имеющими технического образования, либо молодыми специалистами в сфере IT-технологий;

– лица, находящиеся в местах лишения свободы, обладающие знаниями в области компьютерных технологий.

Анализируя личность преступника, следует отметить, что в большинстве случаев указанные преступления совершаются группой лиц по предварительному сговору. Организаторы преступления могут не обладать специальным образованием и познаниями в этой области, однако наличие организаторских способностей позволяет создать организованную группу и длительное время находиться вне поля зрения правоохранительных органов. Возраст преступников – от 14 до 36 лет. Возраст 33 % преступников не превышал 20 лет, 13 % – старше 40 лет и 54 % – 20-40 лет.

Согласно распределенным ролям, в компьютерных сетях у каждого лица – свой «ник».

Кроме того, руководствуясь данными, приведенными статистикой, можно сделать вывод, что большинство осужденных, а именно 81 % от общего числа преступников имели высшее техническое образование или хотя бы определенные познания в данной сфере. Следовательно, данный вид преступлений совершают люди, знающие свое дело (профессионалы).

Наиболее ярким примером может считаться деятельность хакерской преступной группировки, образованной в г. Казань. В данную группировку входили студенты технических вузов г. Казани. На протяжении продолжительного промежутка времени преступная группировка совершала хищения денежных средств с банковских счетов юридических лиц. Преступления совершались с использованием специальных технических средств, которые были приобретены участниками группировки в сети «Интернет». Общий ущерб от незаконной деятельности составил свыше 2 миллионов рублей. В группировке присутствовало четкое распределение ролей. Все участники были поделены на определенные группы, деятельность которых была направлена на реализацию конкретной задачи.

Для групп, осуществляющих хищения с использованием интернет-технологий, характерны устойчивость преступного состава, высокая степень технической оснащенности, четко продуманная линия преступного поведения, ярко выраженный корыстный умысел, а также серьезная кампания по сокрытию следов совершенных деяний. Как правило, данные преступления лица совершают впервые.

Таким образом, криминалистическая характеристика личности преступника дает представление об абстрактном портрете возможного преступника – это молодой человек в возрасте от 20 до 35 лет с техническим образованием либо имеющий определенные знания в сфере информационных технологий,

активный в социальном и трудовом плане, в меру скрытный, возможно, имеющий определенные трудности в финансово-экономическом плане, ранее не судимый.

Личность потерпевшего. Потерпевшими при хищении с помощью IT-технологий могут являться физические и юридические лица, имеющие денежные средства на счетах в банках, организациях, а также держатели различных видов пластиковых карт, осуществляющие пользование электронными платежными системами.

Раскрытие и расследование хищений, совершенных с помощью IT-технологий, представляет определенную сложность вследствие объективных трудностей выявления. С каждым годом появляются новые способы совершения преступления, методы конспирации и маскировки преступниками. Поэтому изучение криминалистической характеристики преступления необходимо с целью установления следователем (дознавателем) обстановки совершения преступления и других факторов, имеющих значение для качественного и своевременного расследования уголовного дела.

Контрольные вопросы

1. Какие элементы криминалистической характеристики преступлений являются значимыми при расследовании хищений с использованием IT-технологий?
2. Назовите особенности бесконтактного (пассивного) перехвата и контактного (активного) перехвата хищений с использованием IT-технологий.
3. Охарактеризуйте типичные средства совершения данных преступлений.
4. Каковы характерные следы данных преступлений?
5. Охарактеризуйте личность преступника.

Практические задачи

1. 15 декабря 2021 г. К., работая в должности специалиста по сопровождению юридических лиц, из корыстных побуждений, умышленно, используя свое служебное положение незаконно осуществила перевод денежных средств в сумме 17 800 рублей со счета, принадлежащего ПАО «Стандарт» на свой лицевой счет.

Рассматривая элементы криминалистической характеристики преступления, охарактеризуйте личность преступника, способ совершения преступления и механизм образования следов.

2. 10 января 2022 г. М., имея умысел на тайное хищение чужого имущества и осознавая противоправный характер своих действий, используя для оплаты товаров в различных магазинах г. Екатеринбурга электронное средство платежа – банковскую карту ПАО «Сбербанк России», принадлежащую Р. и привязанную к банковскому счету ПАО «Сбербанк России»,

умалчивая перед работниками торговых организаций о принадлежности указанной карты иному лицу, то есть путем их обмана похитил денежные средства потерпевшего на общую сумму 5123 рубля.

Каким образом необходимо установить время и место совершения преступления?

Охарактеризуйте личность потерпевшего, раскройте такой элемент криминалистической характеристики, как подготовка к совершению преступления.

Глава 2. Организационно-тактические аспекты расследования хищений, совершенных с использованием IT-технологий

Факт совершения хищения денежных средств выявляется самим потерпевшим, когда происходит снятие денежных средств с банковской карты или лицевого счета. Оперативность раскрытия преступления будет зависеть от времени совершения общественно опасного деяния и сообщения потерпевшим о преступлении, совершенном с использованием информационно-телекоммуникационных технологий в правоохранительные органы. В правоприменительной практике существуют определенные проблемы, связанные с расследованием вышеуказанных преступлений из-за недостаточности разработанности частных криминалистических методик. На наш взгляд, следователю (дознавателю) необходимо обладать специальными познаниями в области информационно-телекоммуникационных технологий сети «Интернет».

Поводами для возбуждения уголовного дела о преступлениях, связанных с хищениями с помощью IT-технологий, могут быть:

– заявления граждан в территориальные органы о хищении денежных средств. Заявление в обязательном порядке должно быть зарегистрировано оперативным дежурным в КУСП.

Рассмотрим пример заявления из правоприменительной практики – заявление директора ООО «Авангард» М., зарегистрированное в КУСП ОП № 12 УМВД России по г. Екатеринбургу под № 22032, от 22.06.2018, согласно которому она просит привлечь к уголовной ответственности лиц за совершение преступления, предусмотренного ст. 159 УК РФ, в связи со списанием с расчетного счета № 4070… ООО «Авангард» денежных средств на счета не известных ей физических лиц, а именно: на расчетный счет ИФНС России № 25 по Свердловской области переведены денежные средства в сумме 649 735 рублей 84 копейки, на расчетный счет О. № 4081… переведены денежные средства в сумме 583 715 рублей,

– рапорт об обнаружении признаков преступления, зарегистрированный в КУСП территориальных органов. Например, рапорт от 15.09.2020, согласно которому в ходе расследования уголовного дела № 12001650001000056 установлено, что в период времени с 13.04.2018 по 23.04.2018 С., П., действуя группой лиц по предварительному сговору, находясь в дополнительном офисе «Ритм» ПАО КБ «УБРиР», расположенном по адресу: ул. Сухоложская, д. 8, в Чкаловском административном районе г. Екатеринбурга, путем обмана похитили денежные средства с расчетного счета ООО «Ритм» в размере более 1 000 000 рублей.

Таким образом, задачами стадии возбуждения уголовного дела являются:

– рассмотрение поступивших и обнаружение первичных данных о преступлении,

– рассмотрение наличия поводов и оснований для возбуждения уголовного дела.

Задачи данной стадии направлены на выполнение общих задач уголовного судопроизводства и реализуются через проведение предварительной проверки. Успешное расследование уголовных дел определяется полнотой и качеством материалов, представленных в виде результатов оперативно-розыскной деятельности.

При принятии решения о возбуждении уголовного дела следователю (дознавателю) в первую очередь необходимо установить следующие обстоятельства:

– где, когда, кем и каким способом совершены противоправные действия, какие приемы маскировки при этом использованы;

– мотивы и цели совершения преступления:

– размер дохода, который был получен в результате хищения:

– наличие и характер обстоятельств, влияющих на характер и степень ответственности, а также обстоятельства, характеризующие личность преступника;

– причины и условия, которые способствовали совершению преступления.

Все поводы подлежат обязательной и тщательной проверке в соответствии с разработанными рекомендациями. Только после решения вопроса о достаточности оснований и наличии признаков преступления может быть принято решение о возбуждении уголовного дела.

Для возбуждения уголовного дела по факту хищения с использованием IT-технологий необходимо наличие повода и оснований (наличие признаков преступления), содержащихся в материалах доследственной проверки.

На первоначальном этапе расследования следователь анализирует складывающуюся следственную ситуацию. Следственная ситуация – это определенные условия, при которых осуществляется расследование. Анализируя правоприменительную практику, можно сделать вывод, что при расследовании указанных преступлений складываются сложные следственные ситуации. В условиях противодействия и его преодоления выдвигаются следующие следственные версии:

– имел место фишинг;

– имел место скимминг;

– преступление совершено:

- банковским работником,
- родственником или знакомым банковского работника;
- родственником или знакомым потерпевшего.

С целью установления обстоятельств, подлежащих доказыванию в соответствии со ст. 73 УПК РФ, необходимо провести определенные следственные и процессуальные действия.

Осмотр места происшествия по уголовным делам в сфере IT-технологий играет важную роль в ходе доследственной проверки. Так, при своевременной организации и проведении указанного следственного действия могут быть обнаружены и правильно зафиксированы материальные и цифровые следы.

На подготовительном этапе необходимо:

– установить, какие технические средства: компьютер, планшет, ноутбук, мобильный телефон – могут находиться в месте проведения следственного действия;

– предварительно изучить помещение, где будет проводиться осмотр, личность заподозренного лица, в том числе его профессиональные навыки пользования компьютером;

– организовать участие в следственном действии специалиста в области телекоммуникационного обеспечения с целью правильного обнаружения и изъятия цифровых следов;

– подготовить необходимые технические и программные средства, позволяющие осуществить просмотр, поиск, изъятие и последующее хранение компьютерной информации.

На обзорной стадии осмотра места происшествия необходимо:

– указать точное расположение осматриваемых технических средств;

– наличие локальной сети и места расположения серверов (на которых могут храниться различные образы памяти), и выходы в другие сети с помощью модема или выделенных линий;

– используемое системное и прикладное программное обеспечение;

– наличие систем защиты информации, их типы;

– возможность использования средств быстрого уничтожения компьютерной информации.

Осмотр средств сотовой связи состоит из нескольких этапов:

1. Внешний осмотр наружного строения и состояния аппарата, фиксация в протоколе таких характеристик, как марка, модель, тип, форма аппарата, цвет корпуса, размер, наличие объектива, сенсорных клавиш, разъема, повреждений, потертостей, сколов, чехла, шнурка, наклеек, надписей.

2. Конструктивный осмотр, т. е. осмотр конструкции телефона по частям: задней крышки телефона, аккумуляторной батареи, флэш-карты, сим-карты, идентификационных номеров.

3. Осмотр информационной среды, т. е. изучение и фиксация сведений, которые содержатся в памяти телефона, флэш-карты, сим-карты[1].

[1] См.: *Уханова Н. В., Иванов Д. А.* Указ соч. С. 137.

Согласно Определению Конституционного Суда Российской Федерации от 2 октября 2003 г. № 345-О[1] любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих звонках, составляют охраняемую законом тайну телефонных переговоров. В связи с этим осмотр информационной среды телефона необходимо производить только с согласия собственника телефона либо на основании решения суда. В связи с неотложностью осмотра следователь может произвести осмотр информационной среды телефона на основании ч. 5 ст. 165 УПК РФ[2].

При оказании противодействия лицом возможна такая ситуация, – и следователь должен знать об этом, – что при наличии соединения средств компьютерной техники с другим оборудованием, находящимся вне периметра зоны проводимого следственного действия (в другом помещении, удаленной территории, населенном пункте), существует реальная возможность непосредственного доступа к компьютерной информации и совершения любых действий (уничтожение, модификация, копирование либо блокирование информации). Для предотвращения этого необходимо временно или на длительный срок отключить компьютерную технику или локальную вычислительную сеть целиком от технических устройств, находящихся за периметром зоны осмотра. Отключение может быть произведено как на программном, так и аппаратном уровне.

Специалист может установить, что в ходе следственного действия на ином устройстве происходит уничтожение информации. Необходимо пресечь уничтожение информации и начать обследование с данного места.

Существует два основных способа изъятия компьютерной информации:

– изъятие обнаруженных средств компьютерной техники с последующим детальным изучением имеющейся на них компьютерной информации вне места изъятия (например, в служебном кабинете или экспертном учреждении);

– изучение всех средств компьютерной техники (содержащейся на них компьютерной информации) непосредственно во время следственного действия с последующим изъятием только той ее (компьютерной информации) части, которая представляет интерес для дела.

На наш взгляд, целесообразно детальный осмотр технических средств проводить в служебном кабинете или экспертном учреждении. Представляется, что в данном случае осмотр будет более полным и объективным.

---

[1] Определение Конституционного Суда Суда Российской Федерации от 02.10.2003 № 345-О. URL: www //http:garant.ru.

[2] Уголовно-процессуальный кодекс Российской Федерации.

По возможности необходимо изымать носитель информации, имеющейся на компьютерах, для дальнейшего детального осмотра, с привлечением специалистов.

Если изъять сам носитель информации не представляется возможным, но возможно выключение компьютера на некоторое время, то необходимо при проведении следственных действий копировать носитель (образ памяти) с помощью специальных программ. В дальнейшем копированный носитель не создает сложности и возможно работать так же, как с оригинальным носителем[1].

В ходе осмотра места происшествия необходимо изъять компьютер, планшет, ноутбук, мобильный телефон. Осмотреть данные технические устройства на предмет обнаружения цифровых следов (скиптов вредоносных вирусов, информации о процессах, происходящих в системе, информации о соединениях с интернет-ресурсами, скрытой информации, содержащейся в файле, данных о входящей и исходящей информации, технических характеристик поступившего письма).

Важное значение в ходе первоначального этапа расследования имеет опрос заявителя. В письменном объяснении должно быть отражено, какая сумма денежных средств списана со счета, необходимо указать дату и время, каким образом стало известно о списании денежных средств. У заявителя выясняется, кому последний разрешал пользоваться своей банковской картой, сообщал ПИН-код, CVC-код на ее обороте. Необходимо, чтобы заявитель истребовал из банка выписку о движении денежных средств в определенный период времени.

Объяснение заявителя, свидетеля преступлений, связанных с хищением денежных средств, совершенных с использованием компьютерной информации, должно включать ответы на перечень вопросов, подлежащих выяснению:

– каким способом произошло завладение компьютерной информацией;

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

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

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

– каким образом осуществляется защита компьютерной информации, каковы методы и средства;

– проверяются ли программы на наличие вирусов и как часто;

[1] См.: Организация расследования преступлений в сфере высоких технологий: учеб. пособие / П. В. Гридюшко и и др.; под общ. ред. И. Г. Мухина. Минск: Академия МВД, 2017. С. 33 (138).

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

– каков порядок работы с компьютерными программами, как информация обрабатывается и передается;

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

– имелись ли факты несанкционированного доступа к компьютерной информации ранее;

– кто является собственником или законным владельцем компьютерной информации.

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

– осмотр записей камер видеонаблюдения;

– проведение портретной экспертизы;

– проведение технико-криминалистической экспертизы с целью установления подлинности банковской карты;

– проведение компьютерной экспертизы;

– направление запросов.

Кроме того, особенности расследования мошенничества с использованием электронных средств платежа обуславливают необходимость отбирания объяснения от следующих лиц:

• разработчиков программного оборудования и поставщиков технического и программного обеспечения (о возможных средствах преодоления защиты, идентификационном номере законного пользователя, кодах и паролях доступа и т. п.);

• сотрудников кредитных организаций, в которых открыт банковский счет потерпевшего (о процедуре осуществления платежей, содержании договора с потерпевшим, операциях по счету потерпевшего, сумме списанных денежных средств и т. п.);

• сотрудников кредитных организаций, в которых открыты банковские счета, на которые переводились похищенные денежные средства (по каким документам данные счета открывались, характер действий данного лица, возможность фиксации его посредством установленных в зале камер наблюдения и т. д.);

• направление запросов операторам сотовой связи на получение информации о принадлежности номера сотового телефона, если переписка потерпевшего с преступником осуществлялась с его использованием;

• установление IP-адреса абонента технического устройства, с которого осуществлялся выход преступника в Интернет, если общение происходило в социальных сетях или на каких-либо сайтах;

• установление местоположения абонента, с которым осуществлялась переписка потерпевшего, если она происходила с использованием мобильных средств связи.

Кроме того, кредитные организации представляют выписки по банковским счетам на запросы правоохранительных органов. Как, например, ответ на запрос с исх. № SD0101385588 от 24.06.2019, согласно которому ПАО «Сбербанк России» предоставляет выписки по банковским счетам по движению денежных средств по счетам № 408… открытым А. 29.07.2017 в дополнительном офисе ПАО «Сбербанк России» № 7003/503, обслуживаемым в рамках выпущенной карты № 54… № 40… открытых 15.09.2017 А. в дополнительном офисе ПАО «Сбербанк России» № 7003/7770, обслуживаемым в рамках выпущенной карты № 22… согласно которым зафиксированы операции.

Или ответ на запрос, согласно которому ПАО «СКБ-банк» предоставлены сведения в отношении О. по счету № 40… открытому 10.04.2018, закрытому 18.06.2018, к которому выпущена банковская карта № 54……, обслуживаемая в ДО «Университетский» ПАО «СКБ-банк», с установленным лимитом снятия по карте 100 000 рублей в день.

По результатам доследственной проверки материалов сотрудник органа предварительного расследования должен получить четкое и полное представление о характере деятельности и структуре объекта, где было совершено хищение денежных средств с использованием компьютерных технологий, о технических характеристиках используемой компьютерной техники и программного обеспечения. Кроме того, следователь должен получить представление о том, каким законом или подзаконным нормативно-правовым актом охраняется компьютерная информация, ее вид. Выделяются два основных вида компьютерной информации: общего пользования – общедоступная – и охраняемая законом – конфиденциальная. Конфиденциальная информация должна быть задокументированной, т. е. зафиксированной на материальном носителе с реквизитами, которые позволяют эту информацию идентифицировать. Доступ к такой информации ограничивается в соответствии с законодательством Российской Федерации. Следователю необходимо изучить служебные обязанности лиц, имеющих санкционированный доступ к охраняемой законом компьютерной информации, а также установить, прямое или косвенное отношение они имеют к ценностям (имуществу), которые стали предметом правонарушения, преступления (или посягательства).

Для обеспечения эффективной борьбы с хищениями и своевременного пресечения преступных действий наркоторговцев необходимо более широ-

ко и тактически грамотно использовать все предусмотренные нормативно-правовой базой следственные действия и оперативно-розыскные мероприятия, а также возможности экспертных подразделений, технические средства для фиксации следов преступления. Важное условие успешного раскрытия и расследования хищений с использованием IT-технологий – тесное взаимодействие следователя с сотрудниками оперативно-розыскных и экспертных подразделений. Такое взаимодействие должно осуществляться с момента проведения доследственной проверки и в ходе расследования по уголовному делу.

Без осуществления оперативно-розыскной деятельности (далее – ОРД) выявление, раскрытие, пресечение и предупреждение хищений, совершенных с использованием IT-технологий, практически невозможно, т. к. преступления в сфере информационно-телекоммуникационных технологий – организованная и тщательно законспирированная деятельность. Разоблачение одного эпизода преступной деятельности еще не обеспечивает эффективной борьбы. В каждом отдельном случае должна быть прослежена вся преступная цепочка, выявлены все лица, причастные к общественно опасным деяниям. Решить эту задачу без ОРД невозможно, она создает условия и предпосылки для процессуального закрепления объективных данных, получающих после этого статус доказательств.

Основными формами взаимодействия оперативных и следственных подразделений являются: совместное обсуждение материалов, подготовленных сотрудниками оперативно-розыскных подразделений к реализации дел оперативного учета, планирование, подготовка и осуществление оперативно-розыскных мероприятий, а также оценка их результатов; реализация оперативных материалов; оперативное сопровождение расследования преступлений с момента возбуждения уголовного дела до завершения судебного разбирательства; обмен информацией о ходе предварительного следствия и результатах проведения оперативно-розыскных мероприятий; создание и функционирование следственно-оперативных групп (далее – СОГ); заслушивание членов СОГ о проделанной работе; своевременное исполнение поручений следователя.

Выполнение поручений следователя (дознавателя). Следователь (дознаватель) в ходе предварительной проверки вправе давать органу дознания обязательное для исполнения письменное поручение о проведении оперативно-розыскных мероприятий, о производстве отдельных следственных и иных процессуальных действий (п. 4 ч. 2 ст. 38, п. 1.1 ч. 3 ст. 41, ч. 1 ст. 144 УПК РФ). Поручение адресуется начальнику органа дознания, который, в свою очередь, дает конкретное задание подчиненному сотруднику оперативного подразделения. В поручении может быть указано о необходимости производства оперативно-розыскных мероприятий, направленных: на получение разрешения суда и направление запроса об истребовании у оператора

сотовой связи входящих и исходящих телефонных соединений абонентского номера, с которого звонили заявителю, с указанием места нахождения (адресов) базовых станций, а также получение информации, на чье имя зарегистрирован указанный абонентский номер; получение разрешения суда и направление запроса в кредитные организации для предоставления сведений: о номере счета, на который заявителем осуществлялся денежный перевод, лице, на чье имя (паспортные данные, адрес фактического проживания, контактные номера) зарегистрирован счет, о подключении услуги «Мобильный банк», с указанием номеров телефонов и периода действия; о подключении услуги «Сбербанк-онлайн» (или аналогичной услуги в других кредитных организациях), дате подключения и способе получения паролей; других подключенных услугах СМС-подтверждения операций с указанием номеров телефонов и периода действия; о снятии денежных средств в кредитных организациях и банкоматах; получение разрешения суда и направление запроса в кредитную организацию для предоставления сведений по банковской карте, на которую заявитель перевел денежные средства: о дате выпуска карты, когда и где она выпущена (номер и адрес дополнительно офиса) и получена, номер лицевого счета; имеются ли у лицевого счета другие карты, если имеются, то указать их номера, период действия; о держателе карты (паспортные данные, адрес фактического проживания, контактные номера); о подключении услуги «Мобильный банк» с указанием номеров телефонов и периода действия; о подключении услуги «Сбербанк-онлайн» (или аналогичной услуги в других кредитных организациях), дате подключения и способе получения паролей; других подключенных услугах СМС-подтверждения операций, с указанием номеров телефонов и периода действия; проверка абонентского номера телефона (банковской карты или счета) на совпадение по другим уголовным делам, преступления по которым совершены аналогичным способом и др.

Срок исполнения поручения в ходе предварительной проверки сообщения о преступлении не должен превышать 10 суток. Поручение о производстве оперативно-розыскных мероприятий исполняется в порядке, предусмотренном Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд. Приказ МВД России № 776, Минобороны России № 703, ФСБ России № 509, ФСО России № 507, ФТС России № 1820, СВР России № 42, ФСИН России № 535, ФСКН России № 398, СК России № 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд». Результаты выполнения поручения о проведении оперативно-розыскных мероприятий могут быть доложены начальнику органа дознания рапортом, после чего приобщаются следователем (дознавателем) к материалу проверки.

Сообщение о выполнении поручения должно носить конкретный информативный характер.

Как показывает практика, хорошо налаженное взаимодействие следственных, оперативных и экспертных подразделений обеспечивает качественное проведение доследственной проверки, обоснованное и своевременное возбуждение уголовного дела, наличие достаточных источников информации и доказательств для раскрытия преступления, а в последующем – и привлечения виновных к уголовной ответственности.

Организация расследования уголовного дела и тактика проведения первоначальных следственных действий, оперативно-розыскных мероприятий будет зависеть от сложившейся следственной ситуации.

Нельзя не согласиться с мнением ученых, что специфика производства следственных и иных процессуальных действий по уголовным делам о хищениях электронных денежных средств, совершенных в том числе с использованием информационно-телекоммуникационных технологий, является неоднородной по своему составу, соответственно, и специфика их расследования имеет некоторые отличия.

Вышеуказанные авторы выделяют следующие ситуации:

1. Преступник завладел банковской картой потерпевшего и при ее использовании совершил хищение денежных средств. По их мнению, данная группа преступлений представляется наименее сложной в доказывании, но при этом занимает немалую долю среди общего количества рассматриваемой категории хищений. Зачастую действия преступника в этих случаях сводятся либо к обналичиванию денежных средств через банкомат либо к оплате картой каких-либо товаров или услуг на кассе.

Ключевая информация при складывающейся ситуации появляется в первую очередь в рамках осуществления процессуальных действий с потерпевшим лицом.

1.1. При допросе потерпевшего выясняются следующие обстоятельства:

• сведения в отношении банковской карты и счета, с которого были похищены денежные средства (наименование банка, дата открытия счета по банковской карте, реквизиты данного счета, тип карты, ее номер, срок действия, остаток денежных средств на момент хищения, сведения об использовании услуг «Мобильный банк» и «Онлайн-Банк»; если потерпевший – пользователь системы электронных платежей (например, QIWI, Яндекс.Деньги и др.), необходимо указать реквизиты виртуальных электронных кошельков и карт, указать сведения о привязке их к банковским картам системы Visa, Mastercard и др., электронным почтовым ресурсам, телефонным номерам);

• сведения о местонахождении и владении банковской картой (место хранения, когда, кому и по каким причинам карта передавалась и др.);

• обстоятельства хищения (когда и каким образом стало известно о хищении, способ хищения, личность лица, похитившего денежные средства и др.);

• иные сведения? исходя из обстоятельств, сообщенных заявителем.

1.2. Сведения, сообщенные потерпевшим, являются идеальными следами преступления, ввиду чего целесообразно их закрепление соответствующими процессуальными действиями. В первую очередь следует получить их в распоряжение следствия, изучить и приобщить к материалам уголовного дела. Например, выписки по счету можно получить непосредственно от потерпевшего после того, как он их запросит в банке, либо получить от сотрудников оперативного аппарата. Кроме того, необходимо принимать безотлагательные меры, направленные на изъятие видеозаписи с камер наблюдения, установленных в местах списания денежных средств со счета потерпевшего (банкомат, магазин и др.).

1.3. К специфике данной группы преступлений следует также отнести необходимость установления обстоятельств распоряжения похищенным имуществом. При установлении данных обстоятельств необходимо:

• изымать приобретенные на похищенные денежные средства предметы, а также документы, подтверждающие их приобретение;

• запрашивать сведения о наличии похищенных денежных средств на банковских счетах, абонентских счетах иных лиц, в случае их наличия, предпринимать меры к наложению ареста на имущество.

2. Преступник завладел сведениями о банковской карте (номер, ФИО владельца, срок действия, CVV/CVN код) и при их использовании совершил хищение денежных средств потерпевшего.

В качестве примеров преступлений данной группы можно привести следующие. Мошенник обращается по объявлению, размещенному потерпевшим, например, на платформе «Авито», и под предлогом внесения предоплаты за товар выясняет указанные реквизиты карты, после чего похищает денежные средства путем их перевода на иные счета или оплаты товаров в интернет-магазинах. Или, например, мошенник под предлогом разблокировки банковского счета выманивает сведения о банковской карте у потерпевшего. В большинстве случаев при списании денежных средств при указанных обстоятельствах проходит двойная верификация платежа: реквизиты карты и код из СМС-сообщения, который также сообщается преступнику потерпевшим. Однако существуют интернет-магазины, осуществляющие платежи только при предоставлении реквизитов банковской карты.

Ключевая информация при складывающейся ситуации также появляется в рамках осуществления процессуальных действий с потерпевшим лицом.

2.1. Сведения, которые необходимо выяснить у потерпевшего, а также способы документального подтверждения события преступления. Ход расследования осуществляется по трем следовым направлениям.

2.2.1. Абонентский номер лица, при использовании которого связывались с потерпевшим. Необходимо провести следственное действие – получение информации о соединениях между абонентами и (или) абонентскими устройствами с целью выяснения следующей информации:

- персональные данные лица, на которое зарегистрирован абонентский номер, и сведения об IMEI-номерах абонентских устройств, в которых была установлена сим-карта с указанным абонентским номером, за интересующий следствие период;
- информация о соединениях между абонентскими устройствами с указанным абонентским номером и иными абонентами за интересующий следствие период, с указанием установочных данных абонентов оператора сотовой связи и адресов базовых станций, к которым происходило подключение указанных абонентских номеров, секторов их действия, азимута направленности использованных антенных блоков и угла охватываемой ими территории;
- информация о входящих и исходящих платежах по лицевому счету абонентского номера;
- информация об IP-адресах, предоставленных провайдером абоненту при выходе в Интернет;
- копия регистрационной формы при продаже и регистрации сим-карты.

В случае если абонентский номер относится к SIP-телефонии, необходимо также устанавливать следующие сведения:

- информация о том, каким образом была произведена регистрация номера и регистрационные данные абонента (иные абонентские номера, адреса электронной почты и др.);
- информация об IP-адресах, использованных для регистрации абонентского номера;
- информация об IP-адресах, использованных для входа в личный кабинет, панель управления по администрированию данным абонентским номером для осуществления звонков;
- информация об абонентских номерах, на которые шла переадресация звонков;
- статистика звонков за интересующий период;
- информацию об оплате услуг связи с указанием полных реквизитов плательщика.

Исходя из полученной в результате данного следственного действия информации необходимо производство следующих следственных и иных процессуальных действий:

- ориентировать оперативный аппарат на установление личности лица, на которое зарегистрирован конкретный абонентский номер или по уста-

новлению личности лиц по новым абонентским номерам, фигурирующим в исходной информации;

При установлении таких лиц – осуществить их допрос по обстоятельствам уголовного дела;

• по адресам электронной почты:

а) необходимо произвести выемку у провайдеров входящих и исходящих сообщений и произвести их последующий анализ с целью дальнейшего установления обстоятельств, имеющих значение для уголовного дела;

б) установить IP-адреса, с которых осуществлялось подключение к электронной почте;

• по IMEI-номерам необходимо установить марки и модели используемых телефонов и в дальнейшем ориентироваться на их изъятие в ходе дальнейшего расследования;

• по детализации соединений осуществить анализ места нахождения по базовым станциям и анализ круга абонентов, с которыми происходило соединение. В случае наличия звонков на горячие линии различных компаний – организовать изъятие аудиозаписи разговоров с целью получения образцов голоса подозреваемого;

• по лицевым счетам произвести анализ о движении денежных средств и направить дополнительные запросы в случае установления сомнительных переводов;

• по IP-адресам:

а) установить провайдера услуг и направить в его адрес запрос на установление лица или лиц, которым они предоставлялись;

б) провести обыска по месту предоставления IP-адресов;

в) осуществить допрос лиц, которым предоставлялись IP-адреса.

2.2.2. Счет, на который были переведены денежные средства потерпевшего. Необходимо направление запроса в соответствии со ст. 26 ФЗ «О банках и банковской деятельности» с согласия руководителя следственного органа о предоставлении следующей информации:

• персональные данные владельца счета (ФИО, привязанные абонентские номера и адреса электронных почт);

• движение денежных средств по счету за период с момента открытия по настоящее время с расшифровкой получателя и назначения платежа;

• сведения об IP-адресах, при использовании которых осуществлялось подключение к интернет-платформе по управлению счетом;

• сведения об IP-адресах и иных счетах, подключение к которым происходило при использовании одного интернет-браузера, полученные посредством анализа cookie-файлов.

По полученным данным владельца счета необходимо дальнейшее производство следственных действий в отношении данного лица в зависимости

от следственной ситуации (допрос, обыск в жилище, обыск по месту работы и др.). По сведениям о движении денежных средств необходимо проведение анализа и в случае их дальнейшего перевода – направление соответствующих аналогичных запросов, а в случае фактов обналичивания – установление банкоматов и принятие мер к изъятию видеозаписей с камер наблюдения (не только банкоматов, но и помещений, где они расположены, а также прилегающей территории). По IP-адресам необходимо установление провайдера и направление запроса на установление лица, которому представлялся данный IP-адрес, проведение обыска по месту представления IP-адресов и последующий допрос лиц, которым предоставлялся IP-адрес.

2.2.3. Третьим направлением расследования в случае звонка потерпевшему по объявлению на интернет-сервисе по размещению объявлений является данная организация. Необходимо направление запроса в организацию, владеющую указанным интернет-сайтом, о предоставлении сведений в отношении пользователей, просматривавших объявление потерпевшего за интересующий следствие период:

- информация об IP-адресах, с которых осуществлялся просмотр указанной страницы;
- в случае, если обращение к объявлению осуществлялось авторизованным пользователем – сведения в отношении его аккаунта (дата регистрации, регистрационные данные (ФИО, абонентский номер, адрес электронной почты и др.);
- сведения об иных IP-адресах и иных аккаунтах пользователя, подключение к которым происходило при использовании одного интернет-браузера, полученные посредством анализа cookie-файлов.

По полученным IP-адресам необходимо установление провайдера и направление запроса на установление лица, которому предоставлялся данный IP-адрес, последующие действия – в зависимости от следственной ситуации (допрос, обыск в жилище, обыск по месту работы и др.).

3. Преступник под различными предлогами путем введения потерпевшего в заблуждение уговорил его перевести со своего счета денежные средства. Примерами преступлений данной группы могут быть следующие: перевод денежных средств в качестве предоплаты за товар по объявлению на интернет-сервисе по размещению объявлений; перевод денежных средств в качестве оплаты товара при покупке через интернет-магазин; перевод денежных средств под предлогом передачи их в долг знакомому, аккаунт в социальной сети которого взломали и др.

3.1. Сведения, которые необходимо выяснить у потерпевшего, а также способы документального подтверждения события преступления.

3.2. Далее ход расследования осуществляется по трем следовым направлениям:

– абонентский номер, при использовании которого связывались с потерпевшим;

– счет, на который были переведены денежные средства потерпевшего;

– интернет-страница, с которой осуществлялось введение в заблуждение потерпевшего. Здесь распространенными являются три варианта: сайт интернет-магазина, страница пользователя или группы в социальной сети, страница на интернет-сервисе по размещению объявлений;

– сайт интернет-магазина. По средствам интернет-сервисов необходимо установить регистратора доменного имени сайта и организацию, предоставляющую услуги хостинга.

В данные организации направляются запросы о предоставлении следующих сведений:

• данные лица, на которое зарегистрировано доменное имя, которому предоставляются услуги хостинга (ФИО, наименование организации, абонентские номера, адреса электронных почт и др.);

• сведения об оплате услуг регистратора / хостинга (даты и способ оплаты, с указанием реквизитов);

• сведения об IP-адресах пользователя при регистрации доменного имени / при получении услуг хостинга.

По полученным персональным данным в зависимости от следственной ситуации необходимо производство следственных действий в отношении данного лица (допрос, обыск в жилище, обыск по месту работы и др.). По сведениям об оплате услуг необходимо направление запроса в отношении счета, с которого были переведены деньги. По полученным IP-адресам необходимо установление провайдера и направление запроса на установление лица, которому представлялся данный IP-адрес, последующие действия – в зависимости от следственной ситуации (допрос, обыск в жилище, обыск по месту работы и др.).

Страница пользователя или группы в социальной сети / страница на интернет-сервисе по размещению объявлений. Необходимо направление запроса в соответствующую организацию о предоставлении следующих сведений:

• дата регистрация аккаунта, регистрационные данные (ФИО, абонентские номера, адреса электронной почты и др.);

• сведения об IP-адресах, с которых осуществлялось подключение к аккаунту с момента регистрации по настоящее время;

• сведения об иных IP-адресах и иных аккаунтах пользователя, подключение к которым происходило при использовании одного интернет-браузера, полученные посредством анализа cookie-файлов.

По полученным персональным данным в зависимости от следственной ситуации необходимо производство следственных действий в отношении

данного лица (допрос, обыск в жилище, обыск по месту работы и др.). По полученным абонентским номерам и адресам электронной почты необходимо установление личности лиц. По полученным IP-адресам необходимо установление провайдера и направление запроса на установление лица, которому предоставлялся данный IP-адрес, последующие действия – в зависимости от следственной ситуации (допрос, обыск в жилище, обыск по месту работы и др.).

4. Хищение совершается при использовании вредоносных компьютерных программ или неправомерного доступа к компьютерной информации.

4.1. При допросе потерпевшего выясняются обстоятельства, отраженные в подп. 1.1., а также следующие сведения:

- адреса банкоматов, которые использовались для снятия наличных средств и осуществления транзакций (с целью выявления возможного скиммингового устройства);
- технические устройства, с помощью которых осуществлялся доступ в личный кабинет при пользовании услугой «интернет-банкинга», например ВТБ-онлайн, Сбербанк-онлайн и др. (указать тип, марку, IMEI, mac-адрес);
- сохранены ли сведения о реквизитах банковских карт и кошельков (номер карты, пароль, CVV2 / CVC2, сведения о держателе карты, срок ее действия) в интернет-браузере технического устройства;
- сохранены ли сведения о логинах и паролях для доступа в личный кабинет сервиса «интернет-банкинга» в интернет-браузере технического устройства;
- с какой организацией – интернет-провайдером заключен договор об оказании услуги доступа в сеть «Интернет» (договор об оказании услуг связи);
- периодичность выхода потерпевшего в Интернет, какие ресурсы при этом наиболее часто посещает, в том числе подозрительные ресурсы;
- каким интернет-браузером пользуется потерпевший во время выхода в сеть «Интернет», его настройки (сохраняются ли история посещений, cache-память, cookie-файлы и т. п.);
- какие лица имеют беспрепятственный доступ к работе с компьютером;
- имела ли место некорректная работа, сбои, неполадки в процессе работы компьютера, его программного обеспечения, электронных сетей, если таковые факты имели место, то выяснить, когда именно они случались и в чем именно это выражалось;
- установлено ли на компьютере (смартфоне) антивирусное программное обеспечение, если да, выяснить является ли оно лицензионным; с какой периодичностью проводится мониторинг на наличие либо отсутствие вредоносных файлов, программ, каковы результаты мониторинга за последнее время;

• как часто производится обновление операционной системы и каким именно образом;

• каким образом производится обслуживание и ремонт компьютерной техники (кем, где, как часто);

• каким образом устроено сетевое подключение компьютеров в организации, кто отвечает за работу сервера;

• переходил ли заявитель по подозрительным ссылкам в сети «Интернет».

При расследовании хищений с использованием IT-технологий следственные ситуации можно дифференцировать на следующие группы:

1. Известно лицо, совершившее хищение с использованием IT-технологий, установлен способ совершения преступления, имеются материальные и идеальные следы преступления.

2. Известно лицо, совершившее общественно опасное деяние, но не установлено его местонахождение.

3. Установлен факт хищения с использованием IT-технологий, но не установлено лицо, способ сокрытия.

В первой следственной ситуации необходимо тщательным образом исследовать полученные доказательства, выполнить комплекс следственных и процессуальных действий, направленных на закрепление доказательств причастности лица к совершенному преступлению:

– допрос потерпевшего, представителя (потерпевшего) по факту хищения денежных средств;

– осмотр места происшествия;

– выемка компьютерной техники, мобильных телефонов, планшетов, материалов и документов, находящихся на электронных носителях;

– допросы свидетелей (очевидцев);

– допрос подозреваемого (обвиняемого);

– обыски по месту жительства и работы подозреваемого (обвиняемого);

– назначение компьютерной, технико-криминалистической, бухгалтерской и иных экспертиз.

Вторая и третья следственные ситуации являются наиболее сложными. Кроме проведения следственных действий необходимо проведение оперативно-розыскных мероприятий в целях установления личности преступника, причин и условий совершения преступления, установления свидетелей (очевидцев), обнаружения следов и других вещественных доказательств.

Важное значение в ходе расследования уголовного дела имеет допрос потерпевшего:

– когда и где был открыт расчетный счет;

– при открытии расчетного счета был или нет к счету подключен абонентский номер;

– пользовался ли потерпевший интернет-банком для отправки платежных поручений в банк;

– блокировался ли по инициативе банка расчетный счет;

– какими денежными суммами пополнялся расчетный счет.

Допросы свидетелей. Необходимо отметить, что такие преступления чаще всего осуществляются в отсутствие идеальных следов; показания свидетелей носят косвенный характер и сводятся к общим данным. Свидетелями, как правило, становятся так называемые сведущие лица, которые имеют определенные знания о произошедшем событии либо могли находиться рядом с потерпевшим в момент обнаружения им сторонних воздействий на программные и (или) программно-аппаратные средства, компьютеры, в том числе ноутбуки, планшетные компьютеры, смартфоны, которые сам потерпевший не осуществлял. В случае мошенничества в отношении физических лиц, как правило, свидетелями являются родные или близкие потерпевшего, а также коллеги по работе. Как уже отмечалось, если потерпевший – юридическое лицо, то свидетелями могут являться сотрудники, занимающие должность директора, системного администратора, техника, бухгалтера, менеджера и т. п. В условиях бесконфликтной ситуации у свидетелей выясняются вопросы, которые касаются их осведомленности о совершенном мошенничестве, и устанавливаются все сведения, которые могут быть полезными для расследования. В условиях конфликтной ситуации необходимо использовать большинство тактических приемов, которые применяются при производстве допроса подозреваемого.

Допросы подозреваемых (обвиняемых). При расследовании уголовных дел по мошенничеству в сфере компьютерной информации целесообразно наладить постоянное, непрерывное взаимодействие со специалистами в области компьютерной информации; они могут привлекаться к проведению многих следственных действий, таких как осмотр места происшествия; выемка и обыск, допросы подозреваемых, следственный эксперимент и, конечно, проведение судебных экспертиз.

В своем диссертационном исследовании В. В. Коломинов на основе изученных уголовных дел, а также анкетирования следователей, выявил неоднозначное отношение следователей к привлечению специалистов к непосредственному проведению допроса: 45 % опрошенных респондентов указали, что необходимо привлекать специалиста для участия в допросе; 50 % опрошенных указали, что присутствие специалиста негативно повлияло на ход допроса; 5 % затруднились ответить на данный вопрос[1]. Данные цифры свидетельствуют о том, что 50 % опрошенных следователей предпочитают

[1] См.: *Коломинов В. В.* Расследование мошенничества в сфере компьютерной информации: научно-теоретическая основа и прикладные аспекты первоначального этапа: дис. … канд. юрид. наук. Краснодар, 2017. С. 112.

привлекать специалиста во время подготовки к допросу, заранее получив консультацию, и тем самым быть готовым к допросу. Еще необходимо учитывать тот факт, что многие следователи предпочитают не показывать подозреваемым свою некомпетентность по некоторым вопросам, а присутствие специалиста будет прямо указывать на это.

Здесь необходимо отметить, что, несмотря на консультации со стороны специалистов, следователь является должностным лицом, уполномоченным осуществлять предварительное следствие, и от его знаний, опыта и профессионализма зависит ход и результат расследования. Поэтому до проведения вышеуказанных следственных действий должна осуществляться тщательная предварительная подготовка.

Хотелось бы подробнее остановиться на тактических особенностях проведения такого следственного действия, как допрос подозреваемых, в связи с тем что именно данное следственное действие проводится в 100 % случаев при расследовании мошенничеств в сфере компьютерной информации, и от качества его проведения зависит объем полученной информации. Кроме того, от уровня проведения допроса подозреваемого лица во многом зависит ход дальнейшего расследования: если следователь во время первого допроса покажет свою некомпетентность, то подозреваемый займет конфликтную позицию и не будет давать правдивых показаний, что отрицательно повлияет на ход всего расследования.

Вышесказанное свидетельствует о том, что по данным уголовным делам вне зависимости от процессуального положения допрашиваемого лица следователю необходимо тщательно подготовиться к проведению допроса. До начала допроса необходимо проконсультироваться с оперативным сотрудником отдела «К», который может помочь в выяснении следующих вопросов: каков характер предмета преступного посягательства; посредством чего осуществлялся неправомерный доступ к информации; какое именно воздействие или вмешательство было осуществлено преступником; каковы последствия преступных действий; каков уровень специальных знаний у предполагаемого преступника; один человек или группа лиц могла совершить мошенничество. Данный круг вопросов не является исчерпывающим, носит ориентировочный характер и варьируется в зависимости от конкретного преступления[1].

Точный ответ на ряд перечисленных вопросов требует производства длительных исследований, однако специалист, ознакомившись с имеющейся информацией, может высказать свои предположения, которые помогут выдвинуть следственные версии и спланировать тактику допроса[2].

---

[1] См.: *Бердникова О. П.* Указ. соч. С. 29.

[2] См.: *Грибунов О. П., Старичков М. В.* Указ. соч. С. 97.

Подозреваемые, как правило, занимают конфликтующую сторону и пытаются оказать пассивное или активное противодействие следователю. Так, в большинстве случаев подозреваемые обладают углубленными знаниями в области высоких информационных технологий. Они имеют специализированное образование или самообразование, особые криминальные навыки работы с компьютерной техникой, которые постоянно совершенствуются[1].

Контрольные вопросы

1. Назовите особенности возбуждения уголовного дела по факту хищения, с использованием IT-технологий.
2. Какие обстоятельства подлежат установлению при расследовании указанных преступлений?
3. Какие типичные следственные ситуации возникают на первоначальном этапе расследования?
4. Перечислите тактические особенности осмотра технических средств.
5. Каковы особенности взаимодействия следователя с органом дознания в процессе раскрытия и расследования хищений?

Практические задачи

1. С 13.04.2021 по 23.04.2021 С., П., действуя группой лиц по предварительному сговору, находясь в дополнительном офисе «Ритм» ПАО КБ «УБРиР», расположенном по адресу: ул. Сухоложская, д. 8, в Чкаловском административном районе г. Екатеринбурга, путем обмана похитили денежные средства с расчетного счета ООО «РИТМ» в размере более 1000 000 рублей.

Охарактеризуйте сложившуюся следственную ситуацию. Определите алгоритм действий следователя.

2. Инженер-программист П. с помощью созданной компьютерной программы совершил доступ к файлу начисления заработной платы сотрудникам… В результате работы данной программы со всех сотрудников списывались денежные средства от 100 до 500 рублей. Полученная сумма в размере 25400 рублей зачислялась на личный счет его знакомой В. В тот же день под вымышленным предлогом П. взял у гражданки В. принадлежащую ей кредитную карту и обналичил похищенные денежные средства.

Охарактеризуйте сложившуюся следственную ситуацию. Составьте план расследования. Составьте план допроса подозреваемого и потерпевшего.

3. М. в период с 08.11.2016 по 18.07.2018 в силу исполнения своих должностных обязанностей, являясь лицом, выполняющим организационно-распорядительные функции в коммерческой организации, имела доступ

[1] См.: *Поляков В. В.* Региональные особенности криминалистической характеристики преступлений в сфере компьютерной информации // Вестник криминалистики. 2016. № 2 (58). С. 47.

к досье клиентов и информации о состоянии счетов, вкладов и банковских операциях по счетам клиентов ПАО «УБРиР» посредством доступа к Централизованной Автоматизированной Банковской Системе «Банк XXI Век», а также программе «SAPCRM», в которой хранятся персональные данные клиентов банка, при этом для выполнения операций в указанных программах М. была наделена персональным логином и паролем. Воспользовавшись своим служебным положением, М. осуществила хищение денежных средств со счетов клиентов ПАО «УБРиР».

Составьте план расследования. Составьте план и фрагмент допроса подозреваемой. Какие следственные действия должны быть проведены в данном случае?

Глава 3. Судебно-экспертное обеспечение расследования хищений, совершенных с использованием IT-технологий

Как отмечалось ранее, в первой главе, раскрывающей криминалистическую характеристику хищений, совершаемых с использованием IT-технологий данный вид преступлений приобрел огромные масштабы и распространился на все слои населения. Это, безусловно, связано с повсеместным распространением средств мобильной связи, компьютеров, сети «Интернет», самых разнообразных приложений и программного обеспечения, что является одной из особенностей современного развития общества и государства.

При расследовании хищений с использованием IT-технологий следователи и дознаватели сталкиваются с рядом трудностей, начиная с проведения проверочных мероприятий, которые по данным уголовным делам включают осмотры места происшествия, назначение судебных экспертиз (традиционные экспертизы, компьютерно-технические, судебно-бухгалтерские и иные), осмотры предметов и документов, выемки различных технических носителей информации и проведение других следственных действий. Поэтому на данной стадии проведения проверочных мероприятий эффективность и быстрота принятия решений во многом требует участия специалистов. Отметим, что использование помощи специалиста может осуществляться как в процессуальной, так и в непроцессуальной форме. Непроцессуальными формами взаимодействия в первую очередь являются консультации, получаемые от специалистов до проведения допросов подозреваемых, вынесения постановления о назначении компьютерно-технической экспертизы, производства обыска и выемки и других следственных действий.

Таким образом, для успешного расследования уголовного дела и установления по нему истины одной из первостепенных задач следователя при расследовании уголовных дел о хищении электронных денежных средств, в том числе совершенных посредством информационно-телекоммуникационных сетей, является установление местонахождения электронно-вычислительной техники, которая выступает в качестве средства совершения преступления, и последующее ее изъятие в установленном законом порядке с целью дальнейшего осмотра и назначения компьютерной экспертизы.

Однако для осуществления целей, обозначенных выше, следователю необходимо обладать минимальными познаниями в области компьютерной информации, непосредственно связанными с процедурой выхода в сеть «Интернет», и в частности, владеть основными терминами и понятиями, применяемыми в ходе расследования всех уголовных дел, о преступлениях, совершенных с использованием информационно-телекоммуникационной сети «Интернет».

Рассмотрим некоторые из них:

1. Интернет-сайт (website, web – «паутина, сеть», site – «место») – это интернет-ресурс, который включает в себя объединенные ссылками и общей структурой документы (веб-страницы). Также применимы названия «интернет-сайт», «веб-сайт», «сайт».

Веб-сайты располагаются на специальных серверах, предоставляемых хостинговыми компаниями (также хостинг-провайдеры), как на платной основе, так и на бесплатной; соответственно, услуга по предоставлению ресурса для размещения информации на сервере называется хостингом. В свою очередь наименование сайта (его символьное имя, которое следует за обозначением всемирной сети «www.») называется доменным адресом (также домен, доменное имя), например, instagram.com, facebook.com, rt.ru и т. д.

2. Интернет-браузер (или webbrowser) – это прикладная программа, предназначенная для загрузки и просмотра страниц, скачивания файлов, управления приложениями и решения других задач в сети «Интернет», например, Yandex.browser, Firefox, Internet Explorer и др.

Интернет-браузер, при определенных настройках сохраняет историю посещений сайтов, а также cookie-файлы и cache-файлы, запоминает пароли и логины к определенным сайтам, а кроме того, предоставляет много иных возможностей, например, создание личного кабинета, который открывает доступ к пользованию всеми ресурсами и службами, например, Яндекс.Деньги, Яндекс.Музыка, Яндекс.Почта и т. д.

3. IP-адрес (Internet Protocol Address) – уникальный сетевой адрес узла в компьютерной сети. Для выхода в сеть «Интернет» устройство (компьютер, планшет, мобильный телефон и др.) использует IP-адрес, предоставленный интернет-провайдером. Существует несколько версий IP-адресов, в частности IPv4 и IPv6. В настоящее время наиболее распространенной является версия IPv4, которая представляет 32-битное число, записанное в виде четырех десятичных чисел со значением от 0 до 255, разделенных между собой точками, например, 172.13.235.2.

IP-адреса условно делятся:

- на внешние (публичные, глобальные) – используются для выхода в сеть «Интернет»;
- внутренние (локальные, частные) – используются для работы в локальной сети;
- динамические – выдаются из свободного в конкретный момент диапазона адресов. Меняются при каждом новом выходе в сеть;
- статистические – данный вид адресов неизменен, привязывается к каждому устройству автоматически либо вручную и сохраняется в дальнейшем за ним.

Таким образом, органы предварительного следствия, располагая данными об IP-адресе, имеют возможность установления точного местонахожде-

ния технического устройства, с помощью которого было совершено преступление, что повышает вероятность установления местонахождения и самого лица, совершившего хищение.

Однако при запросе необходимой информации об IP-адресах у администрации интернет-сайта либо интернет-провайдера стоит учитывать некоторые нюансы адресации в сети «Интернет», такие как NAT и VPN, краткий принцип действия которых мы рассмотрим ниже.

4. NAT (Network Address Translation – «преобразование сетевых адресов») – это специальный механизм, реализованный в сетях TCP/IP, который позволяет изменять IP-адреса пересылаемых пакетов (внутренних или частных IP, которые присылаются на сетевой шлюз) во внешние (глобальные) с последующей отправкой в сеть «Интернет». Такие пакеты нередко называют транзитными.

Данная технология возникла в связи с критической нехваткой IP-адресов версии IPv4, в которой максимальное количество адресов может достигать 4,3 миллиардов. В целях устранения проблемы нехватки адресов еще до создания адресов версии IPv6 была разработана технология NAT.

С технической точки зрения, данная технология довольно-таки сложна для полного понимания, особенно без имеющихся минимальных познаний об устройстве адресации в сети «Интернет». Однако если говорить максимально просто, то одним из достоинств NAT является расширение диапазона IP-адресов, в том числе вплоть до предоставления одного IP-адреса нескольким пользователям одновременно. Логично предположить, что применение данной технологии может создать существенные препятствия в расследовании уголовных дел.

В связи с этим следователь истребует сведения об абоненте у интернет-провайдера, которому был предоставлены в пользование конкретные IP-адреса, должен указать точное время обращения и конкретное наименование ресурса. В противном случае интернет-провайдер может дать ответ о том, что интересующий IP-адрес в определенный момент времени был предоставлен сразу нескольким десяткам, а может быть и сотням лиц. Таким образом, конкретизация запрашиваемых сведений существенно сужает круг лиц, которым предоставлялся интересующий следствие IP-адрес, что позволит в короткие сроки провести анализ полученного ответа и скоординировать дальнейшие действия.

К сожалению, проблема, возникающая в результате использования технологии NAT, не единственная. Преступники, совершая хищения, зачастую используют способы анонимизации, самым популярным из которых являются технологии VPN.

5. VPN (Virtual Private Network – «виртуальная частная сеть») – общее наименование технологий, которые позволяют обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети.

Упрощенный принцип действия VPN выглядит следующим образом: в сети каждому пользователю интернет-провайдером предоставляется IP-адрес, а, в свою очередь, VPN-сервис предоставляет подменный IP-адрес, принадлежащий в подавляющем большинстве случаев иностранному интернет-провайдеру, который физически может находиться в любой части города, страны, а в большинстве случаев – на территории иностранных государств. Очевидно, что данный факт значительно осложняет расследование уголовного дела, как с процессуальной точки зрения, так и с технической, что, как итог, заводит следствие в тупик. На сегодняшний день гарантированных способов деанонимизации VPN не существует. Однако все же существуют способы, которые могут быть эффективны в данном отношении. Так, весьма полезными могут быть используемые многими сайтами cookie-файлы.

6. Cookie-файлы – небольшие фрагменты текстовых файлов, отправляемых веб-сервером браузеру и хранящиеся в памяти компьютера либо иного технического устройства. Интернет-браузер при открытии страницы сайта пересылает фрагменты текстовых файлов веб-серверу в составе HTTP-запроса. В дальнейшем при повторном обращении к данному сайту он уже будет узнавать пользователя и располагать пакетом информации о нем. Другими словами, сервер обменивается с браузером различного рода данными о веб-сайтах, посещаемых пользователем. Например, данные файлы могут содержать сведения о статистике посещений сайтов, логинах и паролях от личных кабинетов пользователей сайтов или сервисов, сведения о регионе, а также о запросах, сделанных пользователем в поисковой строке браузера. Данная информация анализируется сервером и в последующем пользователю не приходится каждый раз вводить логин и пароль при обращении к конкретному ресурсу, также при работе в сети периодически могут появляться всплывающие рекламные окна с предложениями о покупке того или иного товара, сделанными на основе запросов пользователя, и часто посещаемых интернет-страниц, или, например, при посещении каких-либо онлайн-кинотеатров пользователю предлагаются к просмотру подборки фильмов, сделанные на основе его личных предпочтений и т.д., все вышеперечисленное основано на анализе cookie-файлов, получаемых сервером.

Необходимо отметить, что cookie-файлы не подвержены изменениям, в том числе в случаях, когда соединение происходит с использованием VPN. Из этого следует, что при истребовании информации у администрации сайтов о предоставлении IP-адресов, необходимо также истребовать сведения о cookie-файлах и их анализе, что поможет идентифицировать устройство, с которого осуществлялся выход в сеть, а также в некоторых случаях – его местонахождение. Кроме того, результаты анализа полученных cookie-файлов могут быть эффективно применены при проверке лица на причаст-

ность к совершению иных аналогичных преступлений, совершенных именно с данного интернет-браузера и технического устройства.

Рассматриваемый вид преступлений отличается вариативностью и неординарностью, в связи с чем и расследование таких преступлений нельзя описать каким-то единым алгоритмом. Эффективность предварительного следствия зависит во многом от инициативности следователя, творческого подхода и отсутствия шаблонного мышления. Ниже нами будут приведены рекомендации по производству отдельных следственных и иных процессуальных действий, но следует понимать, что в большей степени они являются ориентирующими и в зависимости от следственной ситуации должны модифицироваться. Говоря о специфике производства следственных и иных процессуальных действий по уголовным делам о хищениях электронных денежных средств, совершенных в том числе с использованием информационно-телекоммуникационных технологий, следует заметить, что указанная категория преступлений является неоднородной по своему составу, соответственно, и специфика их расследования имеет некоторые отличия. В связи с этими обстоятельствами целесообразно объединить данные хищения в четыре агрегированные группы, которые также имеют свои подгруппы.

Более подробно рассмотрим особенности проведения отдельных процессуальных и следственных действий, где чаще всего следователи и дознаватели прибегают к помощи специалиста.

Осмотр места происшествия. Специфика осмотра места происшествия при расследовании хищений с использованием компьютерной информации, в отличие, например, от кражи в жилище, заключается в том, что осматривается не только помещение, но и, самое главное, устройство, с которого осуществлялся неправомерный доступ.

В связи с этим при работе на месте происшествия, где обнаружен стационарный компьютер, ноутбук и другая техника, следственно-оперативной группе и иным участникам необходимо соблюдать ряд рекомендаций и правил:

– категорически запрещается совершать с обнаруженными на месте происшествия компьютерами и иными техническими устройствами любые действия, в результате которых могут наступить не известные заранее последствия;

– необходимо ограничить использование в ходе следственного действия или отказаться от использования технических средств, которые могут повредить компьютерную информацию, например, техники, работа которой основана на действии электромагнитного излучения, магнитного поля, рентгеновского излучения и т. п.;

– специалист должен соблюдать осторожность при работе не только с техническими средствами, но и с порошками и химическими реактивами.

Кроме того, в целях проведения качественного осмотра места происшествия, помимо вышеуказанных правил, необходимо соблюдать организационно-тактические основы производства осмотра места происшествия.

После принятия решения о проведении осмотра места происшествия необходимо произвести следующие действия:

а) принять меры по обеспечению охраны места происшествия до своего приезда (например, крайне негативным моментом в расследовании преступлений данной категории будет приглашение пострадавшей стороной специалистов в области информационных технологий для аварийного восстановления компьютерных систем до прибытия СОГ, т. к. могут быть по неосторожности или незнанию уничтожены важные данные, которые имеют доказательственное значение;

б) обеспечить присутствие специалистов на инструктаже СОГ. При этом особое внимание следует уделить совместному инструктажу участвующих в осмотре места происшествия лиц и поручить специалистам проверить готовность программно-технических средств;

в) проконсультироваться со специалистами самому и обязать специалистов проинструктировать всех лиц, участвующих в осмотре места происшествия, о порядке осмотра места происшествия;

г) обеспечить участие понятых. При расследовании преступлений в сфере компьютерной информации в следственных действиях, связанных с осмотром, изъятием компьютерного оборудования, машинных носителей, программного оборудования, с иными манипуляциями с программным оборудованием, компьютерным оборудованием, необходимо к понятым предъявлять дополнительные требования – владение минимальными знаниями в той сфере, которую затрагивает следственное действие.

Правильное закрепление криминалистически значимых следов преступной деятельности, находящихся на технических устройствах, требует от следователя глубоких знаний и навыков по поиску, изъятию и дальнейшей работе с носителями такой информации.

Рабочий этап осмотра начинается со сбора традиционных доказательств: следов пальцев рук, следов обуви, возможных орудий взлома, рукописных записей и т. д.

При осмотре места происшествия следует применять концентрический способ осмотра, под которым понимается порядок осмотра от периферии к центру, где находится самый важный объект (объекты) – сетевой сервер (серверы).

Проведение детального осмотра компьютерных систем, их сетей и периферийного оборудования либо осуществление исследования указанных устройств непосредственно на месте происшествия возможно следующим образом. Специалистом в присутствии понятых производится подключение своего ноутбука к сети или машинному носителю для проведения антиви-

русного тестирования системы. Осуществив указанное подключение, специалист проводит тестирование персональных компьютеров и сети на предмет обнаружения вредоносных (либо поврежденных вирусом) программ. Для их обнаружения используется соответствующее антивирусное и вирусодетектирующее программное обеспечение.

Следует выделить основополагающие принципы работы с компьютерной информацией при производстве осмотра места происшествия:

– обеспечивается сохранность обнаруженных следов на месте преступления (исключение посторонних лиц, контроль за бесперебойной работой компьютерного оборудования);

– не допускается поиск файлов и работа с ними на включенном компьютерном устройстве без участия соответствующего специалиста;

– в случае необходимости изъятия компьютерного оборудования осуществляется правильное завершение работы, отключается роутер или модем;

– если есть угроза несанкционированного уничтожения электронно-цифровых следов преступления вредоносным программным обеспечением, принимаются меры к экстренному отключению компьютера от сети электропитания;

– в случае осуществления работы с устройством, работающим от аккумуляторной батареи, например, ноутбуком, принимаются меры к ее отсоединению;

– осуществляется тщательный контроль за упаковкой и транспортировкой изъятого оборудования;

– производство осмотра компьютера сопровождается фотофиксацией его внешнего вида, отображения экрана монитора и подключенных к нему устройств;

– производится фотофиксация и подробное описание обстановки около компьютерного устройства;

– запрещается приводить в рабочее состояние выключенный компьютер;

– каждый изымаемый объект (кабель, flesh-накопитель и т. д.) подлежит индивидуальной маркировке;

– упаковка должна исключать возможность повреждения изъятых предметов;

– обеспечивается транспортировка и дальнейшее хранение в условиях, исключающих контакт с магнитами и другими потенциально опасными устройствами;

– любая документация на изымаемое оборудование, например записи с логинами / паролями и иная криминалистически значимая информация, подлежит обязательному изъятию;

– при работе с включенным мобильным телефоном или планшетом недопустимо выключать или блокировать экран. Повторное включение может привести к запросу пароля, что осложнит работу с данными. При этом не-

обходимо обеспечить заряд аккумуляторной батареи в оптимальном состоянии;

– если по каким-либо причинам устройство не может длительное время поддерживать автономную работу без дополнительного заряда батареи, а зарядное устройство отсутствует, то необходимо незамедлительно организовать работу с данным устройством с участием специалиста до того, как оно разрядится;

– осуществляется детальное документирование всех произведенных действий в соответствующем протоколе осмотра места происшествия.

С целью получения образцов для последующего сравнительного исследования (файлов), успешного проведения данного и последующих действий и недопущения нанесения вреда системе необходимо произвести полное резервное копирование файлов сетевой среды на внешние носители информации либо на ноутбук специалиста.

Последовательность осмотра переносных компьютерных устройств, планшетов, мобильных телефонов и т. п. можно разделить на три стадии: внешний осмотр, в рамках которого следователь изучает и фиксирует общие признаки (тип и состояние устройства); конструктивный, где осматривается сама конструкция аппарата (корпус, аккумуляторная батарея, флешкарта, SIM-карта); осмотр информационной среды, при котором изучаются и фиксируются сведения, содержащиеся в памяти устройства, на флешкарте или SIM-карте. Добавим, что в протоколе осмотра предмета отмечаются не только сведения об обнаруженном устройстве (IMEI, номер SIM-карты, марка, модель, форма, конструктивные особенности, серийный номер, номер IP и т. п.), но и все манипуляции, проводимые с устройством (включение, просмотр содержимого карт памяти, телефонной книги, открываемых файлов, папок, локальных дисков и т. п.) с подробным описанием и наименованием открываемых файлов.

В качестве некоторых тактико-криминалистических рекомендаций следует добавить, что нередко возникают ситуации, когда в распоряжении следователя при производстве первоначальных следственных действий изымается сразу несколько устройств (планшетов, мобильных телефонов, ноутбуков) во включенном состоянии. В данной ситуации до осмотра нецелесообразно производить их отключение, изымать батарею, SIM-карту, так как при последующем включении могут потребоваться коды блокировки, защитные пароли, PIN-коды. Подчеркнем, что в данном случае конструктивный осмотр следует проводить только после изучения его информационной среды.

В рамках осмотра места происшествия следователем (дознавателем) с письменного согласия заявителя может быть произведен осмотр его мобильного телефона с целью отыскания и закрепления следующей информации: IMEI телефонного аппарата заявителя; наличия SIM-карт с абонент-

скими номерами заявителя; информации, содержащейся в журнале вызовов мобильного устройства, в банке СМС-сообщений, в записной книжке (или «контактах») внутренней памяти мобильного устройства или SIM-карты; информации в виде сохраненных текстов переписки между соответствующими абонентскими устройствами посредством СМС-сообщений или других мессенджеров, например «WhatsApp», «Viber», об истории посещения интернет-сайтов, поиске через установленный на устройстве браузер в Интернете сведений, имеющих отношение к исследуемому событию, использовании соответствующих интернет-сервисов, позволяющих осуществлять виртуальный оборот денежных средств (различные электронные кошельки), регистрации в качестве пользователя в социальной сети, на личной странице которого могут содержаться данные, представляющие интерес для расследования (социальные сети «Вконтакте», «Одноклассники» и пр.); в виде сохраненных логинов и паролей (например, некоторые установленные на мобильное средство связи утилиты (программы) позволяют сохранять информацию о логинах и паролях всех когда-либо посещенных сайтов); типе программного обеспечения мобильного устройства заявителя, наличии в нем собственной антивирусной программы и ее активности. Такой осмотр целесообразно проводить с участием специалиста.

В среде Windows – клавиша на клавиатуре «PrtSc» делает снимок экрана (screenshot) и сохраняет его в оперативной памяти компьютера (буфере обмена). Для его сохранения в файл необходимо открыть графический редактор, например, «Paint» и нажать одновременно сочетание клавиш «Ctrl» и «v». В рамках осмотра необходимо детально исследовать соответствующие разделы приложения «Мобильный банк» («История платежей», «Последние операции» и пр.), в которых зафиксировано движение денежных средств по счету (банковской карте), сделать снимки экрана мобильного устройства, запечатлевающие данную информацию с помощью самого устройства (если позволяет его аппаратно-программное обеспечение), либо сфотографировать экран любым устройством, позволяющим получить фотографическое изображение. Обнаружению и закреплению (фотографированию) также подлежит информация, находящаяся в памяти мобильного устройства, отражающая переписку с виновным лицом, с помощью СМС-сообщений, переписки в Viber, WatsApp и пр., сохраненные страницы в мобильном браузере из социальных сетей, электронных торговых площадок (и их мобильных приложений) и пр.

Информация, полученная в ходе осмотра мобильного устройства, подлежит занесению в протокол, а фотоматериалы необходимо приобщить фототаблицей. При хищениях денежных средств, совершенных при помощи вредоносного программного обеспечения (ВПО), жертвами такого рода преступлений становятся владельцы мобильных устройств на базе платформы Android. Вирус позволяет удаленно управлять отправкой СМС-

сообщений с телефона и перехватывать ответные сообщения, не уведомляя владельца телефона. Пропажа денежных средств обнаруживается заявителем при проверке баланса карты или проведении операций по обналичиванию. По этой причине осмотр самого телефона на предмет сохраненных сообщений не дает результата. Признаками противоправного деяния при наличии в мобильном устройстве ВПО будут служить СМС-сообщения, направляемые на сервисные номера банка с абонентского номера заявителя, которые будут видны только при получении детализации соединений его абонентского номера. Осмотр мобильного телефонного аппарата заявителя может быть произведен и в качестве самостоятельного следственного действия – осмотр предметов, если для этого требуется, например, длительное время, применение специальных знаний и технических средств. В этом случае в ходе осмотра места происшествия возможно изъятие мобильного телефона и его содержимого. При осмотре жилого помещения заявителя возможно изъятие полученных им самостоятельно документов и сведений, относящихся к событию хищения: детализации входящих и исходящих соединений абонентского номера, по которому заявитель общался с виновным, с целью установления абонентского номера последнего; выписки движения денежных средств по банковской карте (счету), с которого были переведены денежные средства; договор банковского счета (банковского обслуживания) и документов об оформлении банковской карты (заявления на открытие банковского счета и предоставление банковской расчетной карты) и др. При получении сообщения о мошенничестве необходимо провести осмотр места передачи (наличных денежных средств), перевода, а при установлении – места зачисления денежных средств. При этом денежные средства заявителем могут быть зачислены на указанный ему номер телефона (лицевой счет абонентского номера), на счет электронного кошелька, на банковский счет (карту).

Представляется особо значимым акцентировать внимание на том, что если для уголовного дела имеют значение данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи, то в случае отсутствия согласия законного владельца мобильного телефона следователь может осматривать подобного рода информацию только по решению суда. Обязательность исполнения этого положения корреспондируется с позицией Конституционного Суда Российской Федерации, выраженной в определении от 2 октября 2003 г. № 345-0: «…Информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным све-

дениям органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения. Иное означало бы несоблюдение требования статьи 23 (часть 2) Конституции Российской Федерации о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения»[1].

Считаем необходимым подробнее остановиться именно на осмотре информационной среды обнаруженного устройства связи, так как именно на этой стадии осмотра можно зафиксировать криминалистически значимые сведения. Осмотр информационной среды начинается с указания в протоколе процедуры разблокировки устройства, перечисления графических и текстовых элементов, которые отобразились на его экране после разблокировки. В случае осмотра мобильного телефона осуществляется проверка IMEI-номера мобильного телефона нажатием комбинации клавиш *#06# (пятнадцатизначный номер должен отобразиться на экране телефона) или в настройках мобильного телефона.

В случае если устройство не защищено паролем, то в протоколе осмотра последовательно указывается информационное содержимое – список контактов, сообщений, наличие изображений, фотографий, видеороликов, перечень папок и файлов рабочего стола, установленные программы и т. д.

В ходе осмотра информационной среды проводится поэтапная детальная фотосъемка экрана устройства с информацией, представляющей значение для уголовного дела. Для визуальной фиксации большого объема сведений, содержащихся в информационной среде, следует применять видеосъемку. При этом следователь в обязательном порядке комментирует все действия, которые направлены на получение той или иной информации с помощью манипуляций с оборудованием.

В правоохранительных органах наибольшую популярность обрели аппаратно-программные комплексы «Мобильный криминалист» и «UFED».

Аппаратно-программный комплекс отечественного производства «Мобильный криминалист» представляет собой программное обеспечение, предустанавливаемое на компьютерное устройство, с помощью которого происходит процесс поиска, обработки и изъятия криминалистически значимой информации (рис. 1).

[1] Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16.02.1995 «О связи»: определение Конституционного Суда РФ от 02.10.2003 № 345-0 // Вестник Конституционного Суда РФ. 2004. № 1. С. 51.

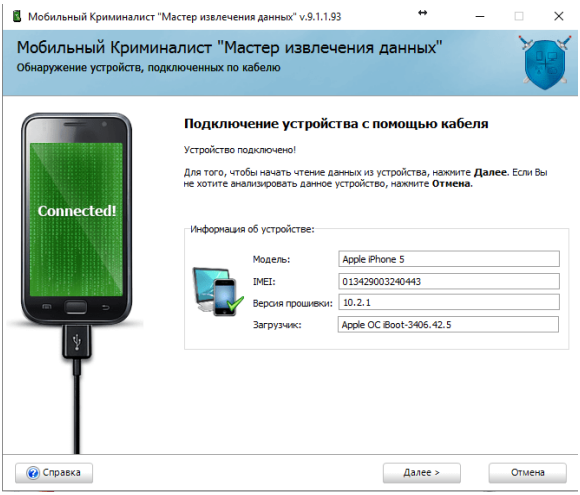


Рис. 1. Программное обеспечение «Мобильный криминалист»

Кроме того, к программному обеспечению «Мобильный криминалист» в комплекте прилагается специальный ключ в виде портативного устройства, оснащенного USB-портом (рис. 2). В случае отсутствия соединения данного ключа в момент запуска и работы с приложением в дальнейшей работе будет отказано.

Рис. 2. USB-ключ «Мобильный криминалист»

Аппаратно-программный комплекс «Мобильный криминалист» обладает возможностью изъятия информации, хранящейся в мобильном телефоне, компьютерном устройстве, а также в облачном хранилище (iCloud, Microsoft One Drive, Amazon Drive и др.), даже если устройство является заблокированным.

Программа позволяет извлекать данные из мобильных устройств и их резервных копий. Построение работы осуществляется за счет декодирования аппаратных ключей шифрования различных операционных систем, включая «Android» и «IOS». В результате чего программное обеспечение предоставляет полный образ исследуемого устройства, в том числе данные шифрованного приложения, которые извлекаются и расшифровываются в максимальном объеме и являются полностью идентичными данным приложения на устройстве.

Другая, не менее функциональная программа – «UFED» производства израильской компании «Cellbrite», также позволяет извлекать криминалистически значимую информацию с различных компьютерных устройств (рис. 3).

Рис. 3. Аппаратно-программный комплекс «UFED»

Данное программное обеспечение способно работать практически со всеми видами мобильных устройств и позволяет:

• полностью извлекать данные мобильного телефона, такие как телефонная книга, текстовые сообщения, фотографии, видеоизображения, журналы звонков (исходящих, входящих, пропущенных), звуковые файлы, ESN, IMEI, ICCID и IMSI и многое другое;

• клонировать идентификатор SIM-карты, производить анализ содержимого телефона без каких-либо сетевых операций и необходимости «взламывать» SIM-карту, заблокированную PIN-кодом;

• производить работу в условиях отсутствия сетевого питания (от аккумуляторной батареи).

В правоохранительных органах наибольшую популярность обрели аппаратно-программные комплексы «Мобильный криминалист» и «UFED».

Допросы подозреваемых. Участие специалиста необходимо в ходе проведения допроса отдельных видов подозреваемых. К ним относятся лица, обладающие высоким уровнем знаний в области высоких технологий, компьютерного программирования, и не желающих давать правдивые показания, а равно применяющие другие виды противодействия, в том числе с помощью ведения разъяснений, частично используя «компьютерный сленг», в том числе на английском языке. В данном случае участие специалиста в области компьютерных технологий обеспечит эффективность допроса и точность излагаемых объяснений подозреваемого.

Обыск. При подготовке к производству обыска следователю необходимо:

1) направить органу дознания поручение с целью установления:

– количества компьютерной техники, которая находится в помещении, где предполагается производство обыска;

– особенностей пропускного режима в организации (при его наличии);

– особенностей коммуникации для обмена информацией между компьютерами (наличие Wi-Fi-сети, локальной сети между компьютерами, местонахождение сервера);

– особенностей электропитания компьютерной техники и расположения мест обесточивания помещения;

– сведений о лицах, которые могут находиться в помещении, где предполагается производство обыска (правовой статус, образование, возраст, наличие профессиональных навыков);

2) уточнить конкретные места и помещения, в которых будет производиться обыск, время его проведения. Принять меры, связанные с безопасностью и конфиденциальностью, при производстве данного следственного действия, чтобы исключить возможность утечки информации;

3) в случае производства обыска в жилом помещении либо в помещениях, где могут находиться лица с особым правовым статусом, позаботиться о получении судебного решения для производства обыска;

4) в случаях проведения обысков в нескольких помещениях одновременно провести инструктаж участников следственной группы о порядке его производства и перечне объектов, подлежащих поиску и изъятию. Кроме того, организовать связь между следственными группами, находящимися по разным адресам;

5) привлечь специалистов для производства данного следственного действия, так как значительная часть объектов, подлежащих поиску, – это носители компьютерной информации. Чаще всего таковыми выступают эксперты Экспертно-криминалистического центра МВД России, которые спе-

циализируются на производстве компьютерных судебных экспертиз, и сотрудники Центра информационных технологий, связи и защиты информации.

Непосредственно при производстве обыска, помимо общих требований, предъявляемых законом к его производству, следователю необходимо обратить внимание на следующие особенности:

1) запретить лицам, находящимся в помещении, осуществлять какие-либо манипуляции с компьютерной техникой и источниками ее питания, даже под предлогом их добровольной выдачи;

2) установить наличие сети между компьютерами, выяснить принцип ее функционирования, местонахождение серверного оборудования;

3) изъять любые электронные носители, в первую очередь системные блоки, ноутбуки, моноблоки, видеокарты, жесткие диски, карты памяти различных форматов, твердотелые накопители и др.;

4) не использовать при производстве обыска устройства, которые могут создавать электромагнитное излучение, так как это может нанести вред или полностью уничтожить информацию;

5) изъятые технические устройства целесообразно упаковывать для недопущения дальнейшей работы с ними.

Напомним, что в соответствии с требованиями статьи 164.1 УПК Российской Федерации электронные носители информации подлежат изъятию с участием специалиста. Специалистом по ходатайству лица, которому принадлежат электронные носители, может быть произведено копирование информации с изъятых носителей. Если, по мнению специалиста, такое копирование может повлечь повреждение или уничтожение информации, то его можно не производить. О копировании информации и о передаче электронных носителей, на которых она содержится, законному владельцу изымаемых электронных носителей информации или обладателю содержащейся на них информации в протоколе следственного действия делается отметка.

В завершение рассмотрения особенностей проведения обыска при расследовании уголовных дел данной категории необходимо определить понятие электронного носителя информации.

Согласно ГОСТ 2.051-2013 «Единая система конструкторской документации. Электронные документы. Общие положения» электронным носителем информации является материальный носитель, используемый для записи, хранения и воспроизведения информации, обрабатываемой с помощью средств вычислительной техники. К таковым следует относить:

– оптические компакт-диски различных видов и форматов (CD-R, CD-RW, DVD-R, DVD-RW, BLU-RAY ит. д.);

– магнитные жесткие диски (винчестеры);

– карты памяти различных форматов (Compact Flash, Secure Digital, Multimedia Card, Memory Stick и др.);

– USB-флэш-накопители;

– оперативное запоминающее устройство периферийных устройств и др.

Таким образом, исходя из действующего уголовно-процессуального законодательства, можно сделать вывод о том, что к электронным носителям информации относится весь спектр технических устройств, указанный выше, поэтому их изъятие в любой форме необходимо производить с участием специалиста.

В связи с этим возникает вопрос о том, как следует производить изъятие таких технических устройств, которые находятся в каждодневном обиходе, но по сути своей тоже являются электронными носителями информации. Например, MP3-плееры в первую очередь служат для чтения аудио-файлов, сотовые телефоны – для звонков и передачи сообщений, цифровые фотоаппараты – для производства фотографий и видеозаписи, видеорегистраторы – для фиксации в видеоформате обстановки на дороге. Тем не менее, в каждом из перечисленных устройств присутствует один из видов памяти для сохранения той или иной информации.

Уголовно-процессуальный закон не регламентирует конкретного перечня электронных носителей информации, подлежащих изъятию с участием специалиста, поэтому их изъятие также должно проводиться с участием последнего.

Компьютерно-техническая экспертиза. Производство данного вида судебной экспертизы может поручаться как экспертным учреждениям МВД России и Минюста России, так и некоммерческим организациям, видом деятельности которых является производство судебных экспертиз и в штате которых состоят эксперты, имеющие допуски на производство соответствующего вида экспертиз. В ходе экспертизы могут исследоваться:

а) мобильный телефон (компьютер) потерпевшего;

б) мобильный телефон (компьютер), модем, роутер, компьютер с сетевой картой, изъятые по месту жительства лица, с IP-адреса которого произошел интересующий расследование удаленный доступ с последующим списанием средств потерпевшего;

в) log-файлы, полученные в ходе выемки из банка[1].

На разрешение экспертам предлагаются следующие типичные вопросы при назначении судебной компьютерной-технической экспертизы:

1. К какой марке и модели относится техническое устройство, предоставленное на исследование? Каковы его технические характеристики?

2. Какие функции возможно выполнять на представленном на исследование устройстве?

[1] Предоставление log-файлов на экспертизу осуществляется, как правило, тогда, когда они не читаемы либо когда защитник высказывает предположения о фактах фальсификации содержащейся в них информации. В отношении носителей с log-файлами может быть произведен осмотр с участием специалиста для обнаружения и фиксации необходимой информации.

3. Возможно ли выполнение определенных функций на представленном на исследование устройстве?

4. Пригодно ли к использованию техническое устройство, представленное на исследование?

5. В случае неисправности технического устройства каковы ее причины?

6. Какой марки и модели носитель электронной информации, представленный на исследование?

7. Для работы с помощью какого устройства предназначен представленный носитель информации, и каким способом к нему возможно подключение?

8. Какие параметры имеет носитель информации?

9. Какова общая характеристика и вид представленного программного обеспечения?

10. Каковы состав и параметры файлов, содержащихся на представленном аппаратном устройстве?

11. Установлены ли на представленном аппаратном устройстве программы, которые предназначены для внезапного уничтожения информации? Если да, то какие именно и каким образом они работают?

12. Имеются ли на представленном аппаратном устройстве какие-либо удаленные файлы, которые содержат информацию, относящуюся к планированию, совершению преступления или уничтожению его следов?

13. Имеются ли на представленном аппаратном устройстве установленные либо удаленные программы, предназначенные для быстрого обмена сообщениями, если да, то содержится ли в них информация, относящаяся к расследуемому преступлению?

14. Осуществлялось ли с представленного аппаратного устройства посещение сайтов, содержащих информацию о расследуемом преступлении, если да, то когда именно и какие сайты посещались?

15. Велась ли переписка с представленного аппаратного устройства в информационно-телекоммуникационной сети с иными лицами, если да, то с кем именно (электронные данные), когда, посредством каких информационно-телекоммуникационных сетей? Ели эта переписка была удалена, то возможно ли ее восстановить?

16. Каково содержание восстановленной информации? Какие данные на носителе информации имеют отношение к фактам и обстоятельствам конкретного дела или лица (в том числе юридического)?

17. Какие данные с представленных на экспертизу образцов и в каком виде находятся на носителе информации[1]?

[1] Компьютерная экспертиза. URL: https://studopedia.ru/17_7377_kompyuternayaekspertiza.html (дата обращения: 18.07.2021).

В отношении мобильного телефона (компьютера) потерпевшего могут быть поставлены следующие вопросы:

– имеются ли на аппаратных средствах представленного мобильного телефона (компьютера) файлы, детектируемые антивирусными программами (если соответствующая экспертиза и вопрос не назначались до возбуждения уголовного дела)?

– если на аппаратных средствах представленного мобильного телефона (компьютера) файлы, детектируемые антивирусными программами, каковы свойства этих программ и какие несанкционированные действия они выполняют: уничтожают, блокируют, модифицируют или копируют компьютерную информацию?

– можно ли установить, когда файлы, детектируемые антивирусными программами, были воспроизведены на аппаратных средствах представленного мобильного телефона (компьютера) и каким способом (из ресурсов сети «Интернет» или иное) они были загружены в них?

– имеются ли на аппаратных средствах представленного на исследование мобильного телефона (компьютера) средства защиты компьютерной информации от несанкционированного уничтожения, блокирования, модификации, копирования, если да, то какие?

– имеется ли на аппаратных средствах представленного на исследование мобильного телефона программа «Мобильный Банк («интернет-банк» и т. п.)» банка «указывается организационно-правовая форма и название банка»?

– имеется ли в истории посещений ресурсов сети «Интернет» на представленном мобильном телефоне (компьютере) информация о доступе к сайту «Мобильный Банк» («Интернет Банк» и т. п.) банка «указывается организационно-правовая форма и название банка», если да, то когда были осуществлены доступы?

Перечень представленных вопросов не окончательный и может меняться в зависимости от сложившейся ситуации и изъятых объектов. Кроме того, перед назначением экспертизы следователю желательно согласовать перечень вопросов, поставленных на исследование, с экспертами, так как некоторые из них могут оказаться нецелесообразными или неверно сформулированными.

Контрольные вопросы

1. Назовите основополагающие принципы работы с компьютерной информацией при производстве осмотра места происшествия.
2. Каковы особенности назначения компьютерно-технической экспертизы?
3. Опишите порядок действий следователя в ходе осмотра места происшествия.

4. Какие существуют формы взаимодействия следователя со специалистом?

5. Назовите цель получения образцов для сравнительного исследования.

Практические задачи

1. Инженер программист П. с помощью созданной компьютерной программы совершил доступ к файлу начисления заработной платы сотрудникам… В результате работы данной программы со всех сотрудников списывались денежные средства от 100 до 500 рублей. Полученная сумма в размере 25400 рублей зачислялась на личный счет знакомой В. В тот же день под вымышленным предлогом П. взял у гражданки В принадлежащую ей кредитную карту и обналичил похищенные денежные средства.

Необходимо ли в данном случае проводить экспертизу? Какую именно? Вынесите постановление о назначении экспертизы. Сформулируйте вопросы эксперту.

2. В течение декабря 2021 года З., являющийся студентом Института программирования, воспользовавшись специальными компьютерными программами для поиска свободных ресурсов в сети «Интернет», скопировал сведения о паролях и логинах для доступа к компьютерной сети «Интернет», а также информацию о пин-кодах Б. и М. Реализуя свой преступный замысел, З. похитил с банковских счетов Б. и М. деньги в сумме 7000 рублей и 3700 рублей.

Какие экспертизы могут быть назначены по данному уголовному делу. Назовите вид и цель экспертизы.

3. *Ситуация с вирусом-вымогателем (зловредная программа из семейства блокировщиков, с помощью которых злоумышленники блокируют доступ к компьютеру или отдельным файлам на нем и взамен требуют у пользователя выкуп за восстановление работоспособности устройства).*

В ДЧ поступило заявление от гражданина, который пояснил, что из-за действий злоумышленников лишился 30 тыс. рублей.

Из объяснения известно, что в 10 ч 20 мин 12 октября 2021 г. гражданину Е. на электронную почту erkonst79@mail.ru поступило письмо рекламного характера с эмблемой сети быстрого питания KFC со ссылкой и надписью, свидетельствующей о том, что после перехода по ссылке будет получен промокод для получения скидки в 40 %. Поскольку он является постоянным пользователем данной сети, то никаких подозрений относительно правдивости полученной информации у него не возникло.

После перехода по ссылке гражданин В. увидел, что система на ноутбуке перестала функционировать, после чего высветилось окно с текстом следующего содержания: «для разблокирования системы осуществите перевод 30 тыс. рублей по номеру телефона 8906…»

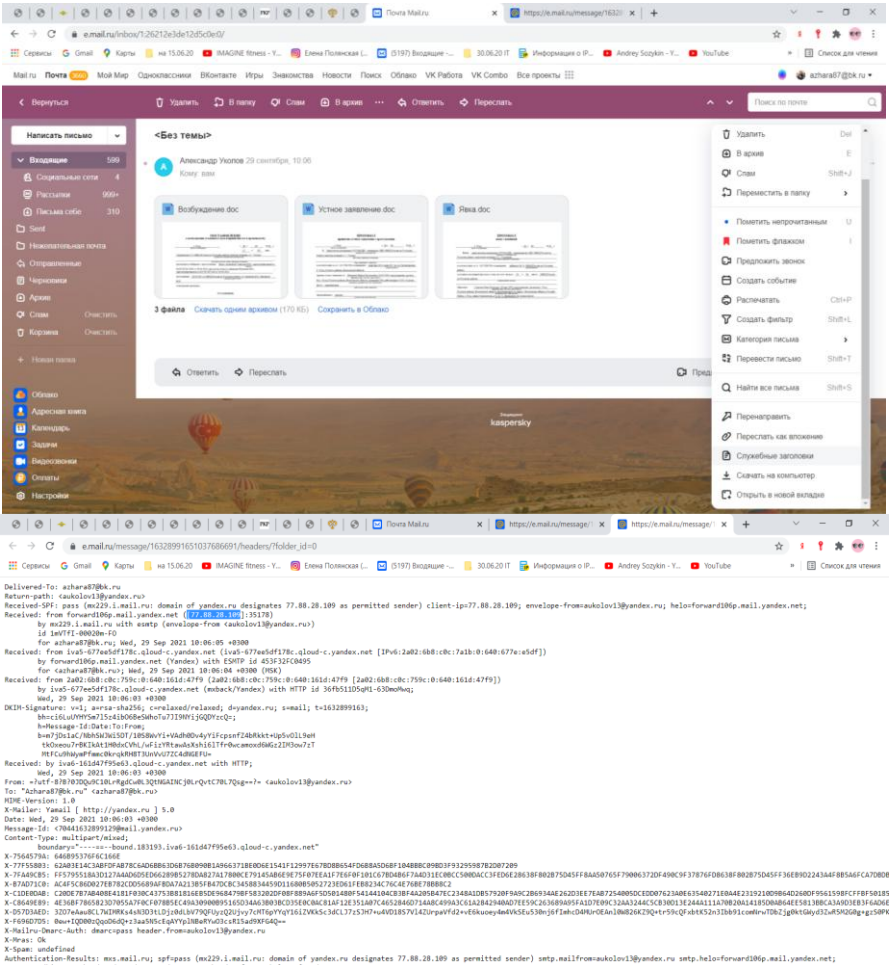
После перевода денежных средств по указанному номеру, спустя один час, система стала функционировать в прежнем режиме. Гражданин пони-

мал, что поймал вирус-блокировщик и лишился денежных средств, но боялся совсем потерять доступ к информации на ноутбуке.

В данном случае следует:

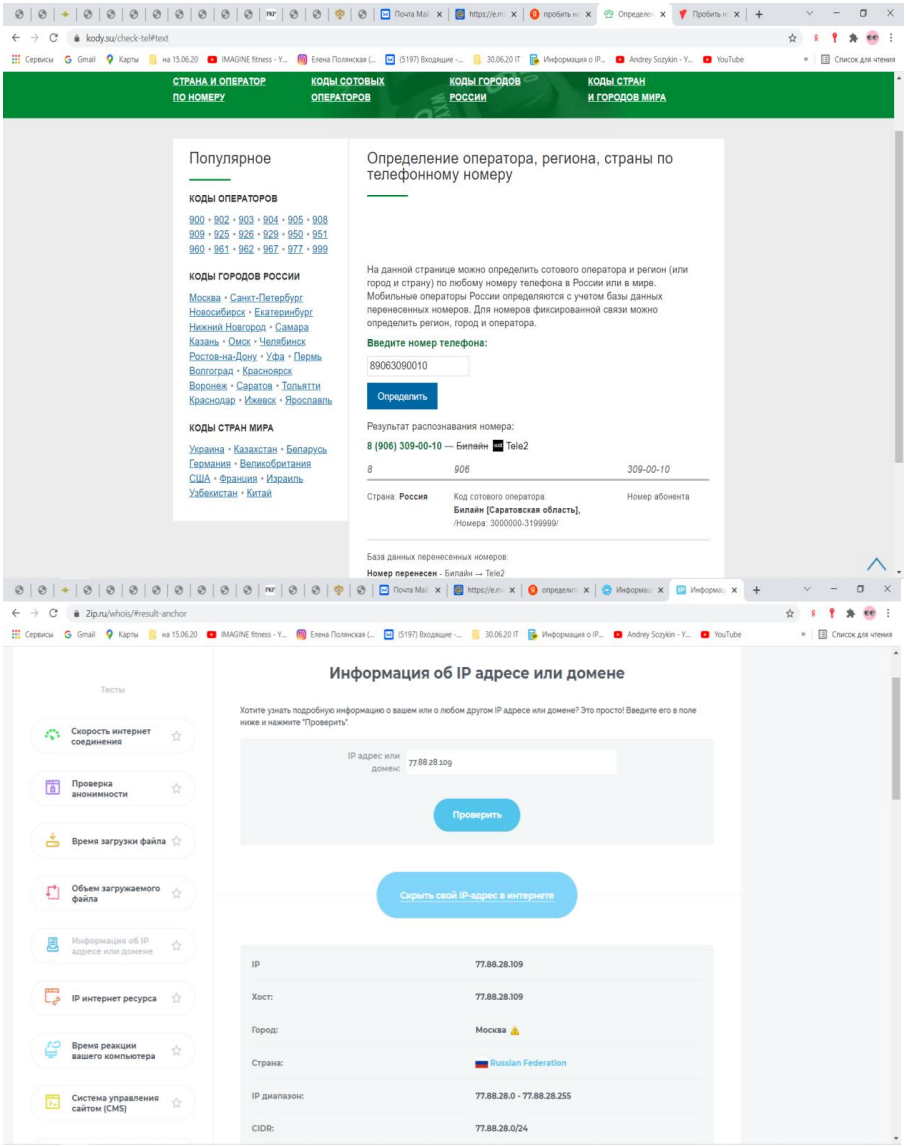
1. В максимально короткий срок получить всю значимую справочную информацию.

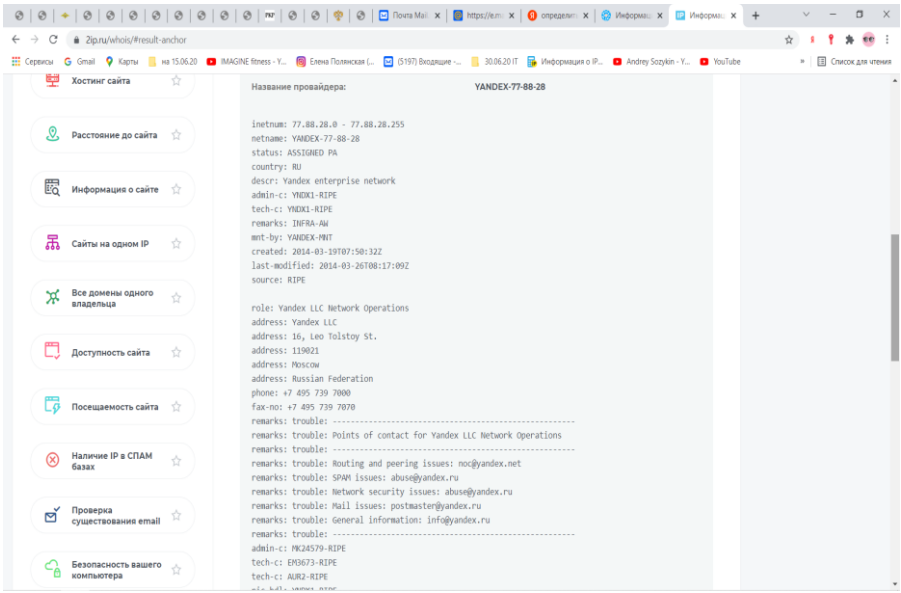
Ниже пример, где находится техническая информация по письму, там же будет IP-адрес, может быть несколько разных IP-адресов, тогда будет нужен только последний.



2. Произвести OSINT (интернет-разведку) по тем данным, которые были получены (номер телефона, карты, интернет-провайдера и т. д.).

Для примера ниже указана корректная информация по номеру, был осуществлен переход с «Билайна» на «Теле2» (код «Билайна»).





3. Произвести осмотр места происшествия, в ходе которого нужно детально осмотреть электронное письмо, компьютер, зафиксировать и скопировать значимую информацию.

4. Составить перечень, в какие компании будут направлены запросы и для получения какой информации (интернет-провайдеру, оператору сотовой связи, в банк, в mail.ru).

5. Назначить судебную компьютерно-техническую экспертизу по файловой системе, реестру для определения наличия скриптов вируса и по письму.

Заключение

В настоящее время во всем мире наблюдается рост преступности в сфере хищений с использованием IT-технологий. Данная категория преступлений в связи с развитием информационных технологий остается одной из высокодоходных видов преступной деятельности.

Преступления в сфере информационно-телекоммуникационных технологий – область, в которой масштабы развития преступности определяются степенью выявляемости органами внутренних дел преступлений данного вида, однако процент неочевидности данной категории преступлений достаточно высок. Это объясняется прежде всего тем, что зачастую системы ОВД разобщены в ведомственном плане, отчего в первую очередь страдает качество раскрываемости преступлений.

Полагаем, что главный упор должен делаться на выявление и пресечение наиболее опасных видов преступлений. Необходимо своевременно информировать граждан о возможных способах хищения через сеть «Интернет». В определенной степени именно правовая неграмотность населения влечет рост преступности в сфере информационно-телекоммуникационных технологий.

Представляется, что следует правильно применять уголовные, гражданские, уголовно-процессуальные нормы при расследовании указанных преступлений. Необходимо устранить нарушение установленных уголовно-процессуальным законом требований к сбору доказательств, небрежность при оформлении процессуальных документов и тактические ошибки в реализации оперативных материалов и следственной работе.

Требуется и консолидация в этом вопросе с зарубежными правоохранительными органами, сотрудничество в рамках универсальных международных организаций, обмен опытом решения этих проблем в рамках конференций, симпозиумов, семинаров. Важна правовая, консультативная и материально-техническая помощь по уголовным делам, а также обмен оперативной, справочной и криминалистической информацией.

В нашей стране это является проблемой, которая требует комплексного подхода к ее разрешению. Поэтому решить ее возможно, только совместив все усилия правоохранительных органов, которые призваны вести борьбу с хищениями в сфере IT-технологий.

Расследование уголовных дел указанной категории – трудоемкий процесс, требующий от следователя (дознавателя) творческого подхода в плане его организации и проведения следственных действий, глубоких знаний криминалистики, уголовного права, гражданского права и уголовного процесса, тактичного отношения к участникам процесса, соблюдения их законных прав и интересов.

Успешное расследование этих преступлений возможно лишь при правильной организации взаимодействия с оперативными службами. Четкое планирование, организация и проведение следственных действий в ходе всего расследования позволят следователю провести его всесторонне, объективно и в полном объеме. Противодействие преступности в сфере IT-технологий остается важной проблемой национальной безопасности.

СПИСОК ЛИТЕРАТУРЫ

Нормативные правовые акты и иные официальные документы

1. Уголовный кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 13.06.1996 № 63-ФЗ (действ. ред.). – URL: www //http:garant.ru.
2. Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 18.12.2021 № 174-ФЗ (действ. ред.). – URL: www //http:garant.ru.
3. Гражданский кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 30.11.1994 № 51-ФЗ (действ. ред.). – URL: www //http:garant.ru.
4. Федеральный закон «О валютном регулировании и валютном контроле» от 10.12.2003 № 173-ФЗ [Электронный ресурс]. – URL: www //http:garant.ru.
5. Постановление Пленума Верховного Суда Российской Федерации № 1 от 26.02.2019 «О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 7 июля 2015 г. № 32 “О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем”» [Электронный ресурс]. – URL: www //http:garant.ru.
6. Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» [Электронный ресурс]. – URL: www //http:garant.ru.
7. Федеральный закон от 23.09.92 № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных» [Электронный ресурс]. – URL: www //http:garant.ru.

Учебные, научные и иные публикации

1. *Андроник Н. А.* Расследование преступлений, связанных с незаконным оборотом наркотических средств и психотропных веществ: курс лекций / Н. А. Андроник, О. П. Виноградова. – Екатеринбург: Уральский юридический институт МВД России , 2018. – 80 с.

2. *Белкин Р. С.* Курс криминалистики / Р. С. Белкин. – Москва, 2001.

3. *Бердникова О. П.* Особенности первоначального и последующего этапов расследования мошенничества в сфере компьютерной информации: учеб. пособие / О. П. Бердникова. – Екатеринбург: Уральский юридический институт МВД России, 2019. – 56 с.

4. *Вехов В. Б.* Компьютерные преступления: Способы совершения и раскрытия / В. Б. Вехов; под ред. акад. Б. П. Смагоринского. – Москва: Право и Закон, 1996. – 182 с.

5. *Вехов В. Б.* Особенности расследования преступлений, совершаемых с использованием средств электронно-вычислительной техники: учеб.-метод. пособие / В. Б. Вехов. – Волгоград: Перемена, 1998. – 72 с.

6. *Воронцова С. В.* Киберпреступность: проблемы квалификации преступных деяний / С. В. Воронцова // Российская юстиция. – 2011. – № 2. – С. 14–15.

7. *Грибунов О. П.* Расследование преступлений в сфере компьютерной информации и высоких технологий: учебное пособие / О. П. Грибунов, М. В. Старичков. – Москва: ДГСК МВД России, 2017. – 160 с.

8. *Гросс Г.* Руководство для судебных следователей как система криминалистики: перепеч. с изд. 1908 г. / Г. Гросс. – Москва, 2002.

9. *Дуленко В. А.* Использование высоких технологий криминальной средой. Борьба с преступлениями в сфере компьютерной информации / В. А. Дуленко. – Уфа, 2017.

10. *Мазуров И. Е.* Методика расследования хищений, совершенных с использование интернет-технологий: дис. … канд. юридических наук / И. Е. Мазуров. – Казань. 2017. – 226 с.

11. Организация расследования преступлений в сфере высоких технологий учебное пособие / П. В. Гридюшко и др.; под общ, ред. И. Г. Мухина. – Минск: Академия МВД РБ, 2017. – 138 с.

12. *Уханова Н. В.* Расследование преступлений против собственности: учеб. пособие / Н. В. Уханова, Д. А. Иванов. – Москва: Московский университет МВД России имени В. Я. Кикотя, 2019. – 226 с.

13. *Ушаков А. Ю.* Особенности квалификации и расследования хищений электронных денежных средств, в том числе совершенных посредством использования информационно-телекоммуникационных сетей: метод. рекомендации / А. Ю. Ушаков, А. Г. Саакян, Р. С. Поздышев, М. А. Степанова. – Нижний Новгород: Нижегородская академия МВД России, 2020. – 56 с.

Эмпирические материалы

1. Приговор Миасского городского суда Челябинской области [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/vG70dKMsd6Yj/

2. Приговор Железнодорожного районного суда г. Барнаула Алтайского края [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/WO4C8QmPo7Z5/

2. Приговор Кировского районного суда г. Екатеринбурга в отношении М. по ч. 2 ст. 273, ч. 3 ст. 272 и ч. 4 ст. 159.6 УК Российской Федерации [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/YwQr7ZHgaQgR/

3. Приговор Фрунзенского районного суда г. Саратова в отношении М. по п. «а» ч. 3 ст. 159.6 УК Российской Федерации [Электронный ресурс]. – URL: https://sudact.ru/regular/doc/qtCZQWKOpk5x/t

4. Судебный департамент при Верховном Суде РФ [Электронный ресурс]. – URL: http//www.cdep.ru

5. Разновидности компьютерной техники [Электронный ресурс]. – URL: http://inphormatika.ru/comp_

Содержание

БЕРДНИКОВА Ольга Петровна
АНДРОНИК Наталья Ауреловна

Особенности расследования хищений, совершенных с использованием IT-технологий

Учебно-практическое пособие

Редактура и компьютерная верстка *И. Б. Бебих*

Подписано в печать 25.04.2022. Формат 60x84 1/16
Печать трафаретная. Бумага офисная
Усл. печ. л. 5,0. Уч.-изд. л. 4,5
Тираж 121 экз. Заказ № 19

Типография научно-исследовательского
и редакционно-издательского отдела
Уральского юридического института МВД России

620057, Екатеринбург, ул. Корепина, 66