Министерство внутренних дел Российской Федерации
Барнаульский юридический институт МВД России

Р.Р. Валюлин, В.В. Козлов

РАССЛЕДОВАНИЕ ТЕЛЕФОННЫХ МОШЕННИЧЕСТВ

Учебное пособие

Барнаул
2023

УДК 343.13(075.8)
ББК 67.410.212я73
В 159

Рецензенты:
врио начальника отдела СУ УМВД России
по г. Барнаулу *А.А. Фельк*;
заместитель начальника КМО ГСУ ГУ МВД России
по Алтайскому краю *М.В. Дитятева*.

Валюлин, Руслан Рашитович.

В 159 Расследование телефонных мошенничеств : учебное пособие / Р.Р. Валюлин, В.В. Козлов. – Барнаул : Барнаульский юридический институт МВД России, 2023. – 56 с.

ISBN 978-5-94552-559-7

В учебном пособии исследованы отдельные способы совершения преступлений в сфере информационно-телекоммуникационных технологий, рассмотрен алгоритм их расследования, проанализирована специфика производства следственных и процессуальных действий.

Пособие предназначено для сотрудников органов предварительного расследования и участников образовательного процесса вузов системы МВД России.

УДК 343.13(075.8)
ББК 67.410.212я73

ISBN 978-5-94552-559-7

Введение

Телефонное мошенничество – один из самых распространённых видов преступной деятельности на современном этапе развития общества. Это обусловлено ускоряющимися темпами развития информационно-телекоммуникационных технологий[1], компьютеризации, развитием кредитно-финансовой отрасли. Происходит повсеместное внедрение в повседневную жизнь дистанционных способов оказания различных услуг, купли-продажи товаров, денежных перечислений, что, безусловно, активно используют преступники, совершая посягательства на имущество граждан и организаций на принципиально новой (высокотехнологичной) основе.

Развитие цифровых технологий постоянно порождает все новые виды преступлений и способы их совершения и сокрытия. В связи с массовым распространением средств мобильной коммуникации возникли новые виды преступлений, такие как создание и распространение вредоносных программ для мобильных телефонов, использование мобильных средств связи для совершения мошенничеств, вымогательств, поджогов, взрывов, террористических актов и пр. В данном пособии указанная категория преступлений будет объединена понятием «телефонные мошенничества».

В последние несколько лет наблюдается ежегодный рост количества совершенных телефонных мошенничеств. В связи с изложенным остро стоит вопрос об ответных мерах реагирования со стороны правоохранительных органов.

[1] Совокупность программных и аппаратных средств, позволяющих устанавливать связь без использования проводов и передавать пакеты информации, включающие также аудио- и видеоинформацию.

1. Общая характеристика телефонных мошенничеств

Уголовно-правовая характеристика

Мошенничество представляет собой хищение чужого имущества либо приобретение права на чужое имущество путем обмана или злоупотребления доверием[1], которые и характеризуют качественные особенности данной формы хищения.

Признаками преступления в сфере мошенничества являются:

Субъект – физическое лицо, возраст которого достигает на момент совершения преступления не менее 16 лет. Также субъектом может быть признано лицо, занимающее определенную должность, которое совершило деяние с использованием служебного положения.

Субъективная сторона мошенничества – вина в виде прямого умысла и корыстная цель.

Объект – чужое имущество или недвижимое имущество, право на чужое движимое имущество. Общественные отношения, на которые посягает преступник.

Объективная сторона мошенничества состоит в хищении чужого имущества или приобретении права на чужое имущество путем обмана или злоупотребления доверием.

Согласно примечанию 1 к ст. 158 УК РФ ***под хищением понимаются*** совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

Обман как способ совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях (например, в предоставлении фальсифицированного товара или иного предмета сделки, использовании различных обманных приемов при расчетах за товары или услуги или при игре в азартные игры, в имитации кассовых расчетов и т.д.), направленных на введение владельца имущества или иного лица в заблуждение. Обман может осуществляться различными способами и на разных этапах прохождения информации, при этом намеренному искажению может подвергаться как сама информация, так и сознание жертвы обмана. Иными словами, обман можно расценивать как манипуляцию с информационным потоком, получаемым гражданином. Способами манипулирования информацией являются: умолчание, селек-

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

ция, передергивание, искажение, переворачивание, конструирование, которые нередко используются в совокупности друг с другом.

Злоупотребление доверием при мошенничестве заключается в использовании с корыстной целью доверительных отношений с владельцем имущества или иным лицом, уполномоченным принимать решения о передаче этого имущества третьим лицам. Доверие может быть обусловлено различными обстоятельствами, например служебным положением лица либо его личными отношениями с потерпевшим[1].

В связи с развитием способов мошенничества в Уголовный кодекс РФ были введены такие квалифицированные виды данного преступления, как:

- мошенничество в сфере кредитования (ст. 159.1);
- мошенничество при получении выплат (ст. 159.2);
- мошенничество с использованием электронных средств платежа (ст. 159.3);
- мошенничество в сфере страхования (ст. 159.5);
- мошенничество в сфере компьютерной информации (ст. 159.6).

В связи с распространившимися случаями хищения денежных средств с платежных банковских карт потерпевших Пленум Верховного Суда Российской Федерации разъяснил, что в случае, когда хищение имущества осуществлялось с использованием поддельной или принадлежащей другому лицу кредитной[2], расчетной[3] или иной платежной карты, путем сообщения уполномоченному работнику кредитной, торговой или иной организации заведомо ложных сведений о принадлежности указанному лицу такой карты, преступление должно квалифицироваться как мошенничество.

В случаях, когда лицо похитило безналичные денежные средства, воспользовавшись необходимой для получения доступа к ним конфиденциальной информацией держателя платежной карты (например, персональными данными владельца, данными платежной карты, контрольной информацией, паролями), переданной злоумышленнику самим держате-

---

[1] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021). Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Кредитная карта – банковская платёжная карта, предназначенная для совершения операций, расчёты по которым осуществляются за счёт денежных средств, предоставленных банком клиенту в пределах установленного лимита в соответствии с условиями кредитного договора (положение ЦБ РФ № 266П).

[3] Расчётная карта – платёжная карта, дающая своему владельцу право на приобретение товаров в кредит в пределах оговорённой суммы. От схожего термина «кредитная карта» отличается высоким кредитом и полным погашением баланса за короткий (как правило, месяц) срок относительно овердрафта по кредитной карте, предоставляющего более длительный срок погашения.

лем платежной карты под воздействием обмана или злоупотребления доверием, действия виновного квалифицируются как ***кража***[1]**.**

Именно способ совершения преступления лежит в основе разграничения данных составов преступлений. Например, поскольку денежные средства изымаются из банкомата тайно, не образует состава мошенничества хищение чужих денежных средств путем использования заранее похищенной или поддельной платежной карты, если выдача наличных денежных средств была произведена посредством банкомата без участия уполномоченного работника кредитной организации. В этом случае содеянное следует квалифицировать как кражу.

Как тайное хищение следует квалифицировать действия и тогда, когда виновным потерпевший введен в заблуждение или обманут, под воздействием чего он сам передает злоумышленнику свою карту или сообщает персональный идентификационный номер – ПИН-код, а снятие денег с банкомата происходит без потерпевшего.

Криминалистическая характеристика телефонного мошенничества

Криминалистическая характеристика телефонного мошенничества включает следующие структурные элементы:

- ***Особенности способов приготовления, совершения и сокрытия телефонных мошенничеств.*** Подготовкой является сбор данных о жертвах, их банковских счетах, социальном положении и т.д. Опираясь на способ совершения преступления, можно констатировать наличие у злоумышленника и использование им соответствующей аппаратуры, куда входят не только сотовые телефоны, но и иные гаджеты с выходом в интернет, и, конечно, наличие у злоумышленника банковского счета, электронного кошелька или иного счета, куда потерпевший, находясь под влиянием обмана, переводит денежные средства. Расследование телефонных мошенничеств представляет объективную сложность в связи с тем, что, как правило, исключается непосредственный личный контакт с мошенником, преступник может находиться в любом месте на территории страны и за ее пределами, регистрировать доменные имена за границей, в короткий промежуток времени совершить значительное число хищений, а установление его личности в данном случае крайне затруднительно. Как способ сокрытия следов совершения телефонного мошенничества можно рассматривать активное вовлечение потерпевшего в его совершение, когда действия, направленные на хищение принадлежащих потерпевшему де-

[1] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 29.06.2021). Доступ из справ.-правовой системы «КонсультантПлюс».

нежных средств, совершаются самим потерпевшим под руководством преступников. Потерпевшему сообщается о необходимости снятия всех денежных средств и временного зачисления их на так называемые «резервные счета», данные о которых сообщают преступники. Сами преступники определенное вмешательство в процесс совершения хищения осуществляют дистанционно, во-первых, на стадии телефонных переговоров, пользуясь функцией подмены номера телефона. С целью сокрытия следов преступления используются такие анонимайзеры, как VPN, TOR, Proxy. Использование данных программ предполагает не только шифрование передаваемых и получаемых сведений, но и серверов, неподконтрольных российским правоохранительным органам. Во-вторых, на стадии получения денежных средств, когда мошенники, не участвуя в процессе лично, используют современные технологии, позволяющие получить деньги. Следы совершения преступления в этом случае блокируются за счет возможности анонимного обналичивания денежных средств либо их иного использования, например, для оплаты товаров, заказываемых из-за рубежа, когда идентификация покупателя не осуществляется либо крайне затруднена, потому что покупатель и мошенник – не одно и то же лицо[1].

Способы телефонных мошенничеств достаточно разнообразны и зависят от изобретательности и интеллектуальных способностей преступника, более подробно они будут рассмотрены во втором параграфе данного пособия.

- ***Особенности средств и орудий совершения телефонных мошенничеств.*** Орудиями указанных деяний выступают мобильные телефоны, принадлежащие потерпевшему и (или) обвиняемому, ноутбуки, сим-карты, электронные кошельки, платежные карты и пр.
- ***Особенности предмета преступного посягательства телефонных мошенничеств.*** Для расследования телефонных мошенничеств важное значение имеет форма предмета, которая выступает в виде безналичных денежных средств.
- ***Особенности оставляемых следов.*** Средство связи сохраняет введенные номера телефонов, в приложении интернет-банка сохраняются виды транзакций с передачей денежных средств. Цифровой след начинается с момента поступления телефонного звонка потенциальной жертве, затем имеет место вход в приложение банка злоумышленника, перевод денег в платежных системах WebMoney, E-Gold, StormPay, RuPay, RBKMoney, QIWI, «Яндекс.Деньги», «Монета.ру» и др., на серверах платежных систем остаются данные об операциях с интересующими нас счетами, данные пользователей, конкретное время проведения операций со

[1] Колчевский И.Б., Журавлев В.М., Кузнецов А.Г. и др. Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ: аналитический обзор. М.: ФГКУ «ВНИИ МВД России», 2018.

счетами, следы от дистанционного управления мошенниками своими счетами, их открытия и закрытия, а также многие другие сведения; реквизиты счетов, на которые осуществлен перевод денежных средств[1]. Кроме того, с помощью фоноскопической экспертизы возможна идентификация человека по голосу из записей телефонных переговоров, если такие записи производились.

- ***Особенности личности лица, совершившего преступление, и потерпевшего.*** Личность преступника является одной из процессуальных фигур в уголовном деле, познание которой имеет важное значение для правильного разрешения уголовного дела. Практика показывает, что рассматриваемые преступления преимущественно совершаются мужчинами (63%). При этом немаловажным является тот факт, что доля женщин, совершающих мошенничество (37%), значительно выше доли женщин, совершающих все преступления в целом (16%).

Возрастную характеристику личности мошенников изучил И.В. Ильин, на основе его исследований можно составить своеобразный возрастной рейтинг рассматриваемых преступлений[2]. Возрастная структура обусловлена в первую очередь психофизиологическими характеристиками личности. В этой связи следует отметить, что именно в среднем возрасте преступникам присущи обдуманные преступления, требующие подготовки и тщательного планирования. Указанный возраст характерен для лица с высокими запросами для удовлетворения своих потребностей. Большое значение при составлении криминалистической характеристики личности мошенника имеет оценка морально-нравственных качеств личности. Такого рода преступления чаще всего совершают лица с достаточно сформированными ценностными ориентациями, взглядами, установками, сознательно ориентирующиеся на выбор преступного поведения как средства обеспечения образа жизни с высоким уровнем достатка. Лица, которые занимаются мошенничеством, обладают рядом специфических характеристик. В отличие от воров, грабителей и других преступников корыстной направленности мошенники более «интеллектуальны», подозрительны, недоверчивы, имеют гибкость и вероятностность мышления, его альтернативность и вариативность. Как правило, они хорошие психологи, обладают элементами своеобразного «артистизма», имеют более высокий образовательный уровень, эгоистические нравственные принципы, доведенные до степени искусства навыки обмана в своей сфере мошенничества. Такие люди готовы идти на значительный риск, т.к. уверены в себе и склонны к гедонизму (стремлению к удовлетворению как высшему бла-

[1] Полещук О.В. Шаповалова Г.М. Криминалистическое исследование следов при расследовании компьютерных преступлений: монография. Владивосток, 2006. 161 с.

[2] Ильин И.В. Социально-демографические признаки личности экономического мошенника. М., 2010. С. 71-77.

гу)[1]. По отношению к «классическим» мошенникам «телефонные» мошенники часто обладают специальными познаниями в области техники и компьютерной информации. Совершение мошенничества, например, с использованием услуги «Мобильный банк» свидетельствует о том, что злоумышленник как минимум на потребительском уровне может пользоваться данной услугой и, понимая механизм ее работы, осуществляет свою корыстную цель путем совершения противоправных действий. Лицо совсем не обязательно должно быть компьютерным гением, основная ставка делается на психологический аспект в части убеждения потерпевшего в совершении тех или иных действий по указанию виновного лица. Сложность механизма совершения таких преступлений говорит о том, что осуществить их в одиночку практически невозможно, и совершаются они, как правило, в составе преступных групп. Отличительной особенностью таких преступных групп является то, что их члены, выполняя конкретные функции, могут быть незнакомы друг с другом или знакомы только с кем-то из других участников.

В афере всегда есть две стороны, и портрет мошенника был бы неполным без портрета жертвы. Немаловажную роль играет и виктимологический аспект. Можно выявить два основных типа потерпевших по мошенничествам. Первые – это те, кто стремятся обогатиться, но в результате преступных действий становятся жертвами преступления. В обманутом всегда есть что-то, что роднит его с преступником: например, жажда наживы. Аферист играет на том, что человек хочет что-то получить дешево или вообще бесплатно, быстро и не прикладывая сил. Лень – одна из основных причин, почему люди становятся жертвами. Лень узнавать подробности, лень куда-то идти, лень спрашивать. Плюс любопытство и любознательность – мошенники интригуют, завораживают, они говорят так, что потерпевшему интересно, чем это закончится. Дешево, быстро, легко и престижно – эти слова привлекают пострадавшего, а если у него есть тяга к авантюрам, минимум самоконтроля, он доверчив, инфантилен и недальновиден, то вскоре еще одно дело ложится на стол следователя. К другому типу жертв относятся те, кто стремится якобы предотвратить какое-либо посягательство на свои собственные права, например разблокировать банковскую карту. То есть они хотят защитить лишь то, что им принадлежит на законных основаниях, однако, веря мошеннику на слово, попадаются на очередной его обман.

[1] Дьячков А.М. Психологические аспекты личности современного мошенника и приемы, используемые им для обмана граждан. М., 2005.

Мошенники стали имитировать кол-центры[1] банка. Злоумышленники достаточно правдоподобно воспроизводят работу настоящих банковских кол-центров, часто детально знают банковские продукты, услуги и форматы их работы, используют аналогичные сценарии разговора, музыку и другие атрибуты, которые вводят клиента в заблуждение. Мошеннические кол-центры стали логическим развитием формата социальной инженерии.

Широко распространены случаи совершения телефонных мошенничеств осужденными, отбывающими уголовное наказание в виде лишения свободы в исправительных учреждениях. И это связано, прежде всего, с тем, что мошеннические действия можно осуществлять в отношении неограниченного количества граждан, никак не связанных с исправительным учреждением. При этом осужденные рассчитывают на невысокую вероятность наступления неблагоприятных для них последствий в виде уголовного преследования, полагаясь на свое преступное мастерство и низкий уровень правового сознания большинства граждан, обусловливающий латентность преступлений.

2. Основные способы совершения телефонных мошенничеств

Новые виды телефонных мошенничеств появляются довольно часто. Но и давно существующие схемы обмана до сих пор действуют на удивление успешно. Стать жертвой такого преступления, как телефонное мошенничество, может даже самый осторожный владелец мобильного телефона. Рассмотрим самые распространенные и известные на сегодня виды телефонного мошенничества.

Схема 1. Мошенничества через сайты объявлений. Мошенник-продавец.

Мошенник размещает на сайтах объявлений («Авито», «Юла», «Циан» и др.) информацию о продаже какого-либо товара, сдаче в аренду жилых помещений или же оказании тех или иных услуг. Цена, как правило, в объявлениях указывается ниже рыночной, чтобы заинтересовать как можно больше будущих жертв преступной деятельности мошенника. На самом деле у мошенника нет никакого товара и никаких услуг он оказывать не собирается, в объявлении размещаются фотографии, скачанные из сети Интернет. Будущий потерпевший звонит мошеннику по номеру телефона, указанному в объявлении, либо обращается через сообщение в чате на сайте объявлений, чтобы

[1] Кол-центр (от англ. call – звонок) – это подразделение компании или отдельная организация, предоставляющая услуги обработки входящих и исходящих вызовов клиентов.

договориться о будущей сделке. В ходе общения мошенник предлагает внести предоплату за будущую услугу, товар или аренду, сообщает реквизиты банковской карты, на которую потерпевшие переводят предоплату. В последующем никакие услуги, естественно, не предоставляются, товары не поступают. Предоплата, как правило, составляет от 1000 до 5000 руб., но в связи с заманчивой ценой объявление вызывает повышенный спрос, и на уловки мошенника попадается значительное количество потерпевших.

Схема 2. Мошенничества через сайты объявлений. Мошенник-покупатель.

Мошенник звонит по объявлению потерпевшего, размещенному на сайте («Авито», «Юла», «Циан» и др.), говорит, что якобы желает приобрести его товар, и предлагает внести задаток. Для внесения задатка мошенник просит продиктовать контрольные данные по банковской карте. Будущий потерпевший, не подозревая о преступных намерениях звонящего, сообщает номер своей банковской карты, срок ее действия и CVV-код, расположенный на оборотной стороне карты. Получив данные сведения, мошенник от имени потерпевшего через онлайн-сервисы делает заявку о покупке какого-либо товара или о переводе денежных средств с банковской карты потерпевшего. После этого мошеннику остается только узнать код подтверждения операции, высланный по номеру телефона потерпевшего. Мошенник под каким-либо обманным предлогом выясняет у потерпевшего текст поступившего СМС-сообщения, после чего вводит этот код в онлайн-сервис, подтверждая тем самым покупку или перевод денежных средств потерпевшего. Или же мошенник просит подойти к банкомату и выполнить ряд комбинаций, подключая мобильный банк и в последующем похищая денежные средства.

Схема 3. Подделка чеков о переводе денег.

Мошенник обращается по объявлению, размещенному на сайте («Авито», «Юла», «Циан» и др.), с просьбой продать ему какой-то небольшой объем товара, продажей которого занимается будущий потерпевший. Мошенник выясняет у продавца для оплаты номер банковской карты или телефона, к которому привязана эта карта. Продавец, ничего не подозревая, предоставляет, как обычно, запрашиваемые данные, и мошенник реально оплачивает свою первую покупку. Далее мошенник входит в доверие, совершая несколько настоящих небольших платежей, после чего делает крупный, дорогостоящий заказ. Часто продавец не имеет возможности своевременно проверить поступление оплаты на свой счет, и в качестве доказательства оплаты покупки или денежного перевода принимает электронный чек, к примеру, из

приложения «Сбербанк Онлайн» покупателя. С помощью чат-бота[1] за небольшую плату в мессенджере Telegram, по образцу первых чеков, генерируется поддельный чек за последнюю покупку, после чего мошенник предоставляет его продавцу в подтверждение оплаты, которая на самом деле не осуществлялась. Продавец, будучи уверенным, что товар оплачен, на самом деле передает его мошеннику безвозмездно.

Схема 4. Мошенничества со взломом страниц социальных сетей.

Мошенник с помощью третьих лиц за определенную сумму приобретает в сети Интернет взлом страницы[2] социальной сети («ВКонтакте», «Одноклассники», «ДругВокруг» и др.) или осуществляет его самостоятельно, как правило, с помощью специальных вирусов, которые собирают на зараженных компьютерах всю вводимую информацию. Получив доступ к аккаунту, мошенник действует по одному из двух сценариев. По первому мошенник рассылает всем друзьям из списка контактов сообщения мошеннического характера с просьбой занять денежные средства под различными предлогами (заболел родственник, не хватает на срочную покупку и т.д.). В этом же сообщении мошенник указывает реквизиты для перевода денег. Получатель данного сообщения, не подозревая, что страница друга взломана, и желая помочь последнему, перечисляет деньги на указанные в сообщении реквизиты. По второму сценарию мошенник также рассылает сообщения всем друзьям из списка контактов, но при этом вместо просьб сообщения содержат ссылки на порнографические, вредоносные или мошеннические ресурсы и приложения. Как правило, такие ссылки сопровождаются завлекающим текстом.

Пример 1: «Вот, наконец-то, вышла программа для просмотра гостей, которые заходят на твою страницу…».

Пример 2: «Видела твои фото, я такого не ожидала, посмотри сам!..».

Пример 3: «В этой базе данных есть вся информация на любого человека».

Отправлять спам-ссылки мошенники могут не только через сообщения, но и через публикацию соответствующих «статусов». Статусы отображаются в ленте новостей у «друзей» жертвы. Статусы могут быть не только текстовыми, но и в виде информационного сообщения самой соцсети о том, что «такому-то пользователю нравится видео XXX». В любом случае, если потерпевший переходит по присланной ссылке, его

[1] Чат-бот (англ. chatbot) – это программа, которая имитирует реальный разговор с пользователем. Чат-боты позволяют общаться с помощью текстовых или аудиосообщений на сайтах, в мессенджерах, мобильных приложениях или по телефону.

[2] Взлом сайта – несанкционированное подключение и получение доступа к файлам сайта или административной панели управления третьими лицами с целью последующего нанесения ущерба.

браузер может быть перенаправлен на совершенно другой ресурс, где на телефон загружается вирус (чаще всего используются вирусы Triada и Marcher), предоставляющий злоумышленнику доступ к СМС-командам. В дальнейшем мошенник похищает деньги путем направления сообщений на номер банка.

Схема 5. Мошенничество, совершенное с использованием вредоносных программ на ОС Android.

Потерпевшему на сотовый телефон с операционной системой Android с неизвестного номера приходят СМС-сообщения, например, с текстом: «Здравствуйте, я по Вашему объявлению. Не интересует обмен с доплатой? Ссылка: www.avit.o.ru/FriZksk», или СМС-сообщение с текстом: «Смотри, как мы здорово получились на этой фотографии. Ссылка: www.bit.ly/ZreizE1eAa». Потерпевший проходит по данной ссылке. После перехода по ссылке, так же как при мошенничестве со взломом страниц социальных сетей, на телефон загружается вирус, предоставляющий злоумышленнику доступ к СМС-командам. В дальнейшем мошенник похищает деньги путем направления сообщений на номер банка.

Схема 6. Мошенничество, совершенное под предлогом заказа банкета, товара, прочих услуг (или связь с курьером).

Мошенник звонит в организацию и говорит, что желает воспользоваться ее услугами по заказу крупной партии товара, банкета или прочих услуг. Далее мошенник назначает встречу с представителем компании, чтобы обговорить все условия предстоящего мероприятия, и называет место, где хотел бы встретиться с представителем компании. Для связи мошенник спрашивает телефон представителя компании. Незадолго до встречи, пока представитель компании следует в назначенное место, мошенник связывается с ним и просит по пути пополнить счет абонентского номера (или банковской карты) мошенника на неопределенную сумму, которую он (мошенник) отдаст при встрече. Никакой встречи после перевода денег не происходит, и деньги, естественно, не возвращаются. Также имеется разновидность подобной схемы, когда мошенники публикуют объявление о наличии высокооплачиваемой вакансии с хорошими условиями труда. На самом деле никакой вакансии нет, и объявление является обманом. Будущий потерпевший звонит по объявлению, желая устроиться на работу с хорошими условиями. По телефону лжеруководитель назначает кандидату время и место собеседования, а позже предлагает потерпевшему по дороге на собеседование приобрести продукты для банкета или цветы, а также срочно пополнить баланс телефона или одолжить до собеседования определенную сумму, которую ему вернут

при встрече. Никакого собеседования после перевода денег не происходит, и деньги, естественно, не возвращаются.

Схема 7. Мошенничество, совершенное под предлогом разблокировки банковской карты.

Мошенник осуществляет рассылку СМС-сообщений с текстом о блокировке банковской карты. В данном сообщении указывает абонентский номер (иногда виртуальный[1] – 8-800-..., 8-495-... и др.), по которому можно обратиться для консультации о произошедшем. Когда потерпевший звонит по данному номеру, в ходе разговора вначале мошенник представляется работником службы безопасности или какого-либо другого подразделения банка и сообщает, что существует угроза блокировки банковской карты потерпевшего. Под предлогом попытки сохранения денежных средств просит сообщить контрольные данные банковской карты либо подойти к банкомату. Паника отключает критическое мышление – таковы законы нейрофизиологии. Высока вероятность, что напуганный человек не будет тратить время на выяснение подробностей и сделает все, что ему говорят. Именно на это рассчитаны звонки из якобы службы безопасности банка, когда собеседник сообщает о происходящем – «вот прямо сейчас» – списании денег с карты. Сообщает номер своей банковской карты, срок ее действия и CVV-код, расположенный на оборотной стороне карты. Получив данные сведения, мошенник от имени потерпевшего через онлайн-сервисы делает заявку о покупке какого-либо товара или о переводе денежных средств с банковской карты потерпевшего. После этого мошеннику остается только узнать код подтверждения операции, высланный по номеру телефона потерпевшего. Пока владелец карты в панике соображает, что делать, «безопасник» предлагает простое решение: сообщить уже поступивший в СМС-сообщении трех-четырехзначный код, переслать эту СМС в «надежные руки». Получив код из СМС-сообщения, мошенник вводит его в онлайн-сервис, подтверждая тем самым покупку или перевод денежных средств потерпевшего.

Схема 8. Мошенничество, совершенное под предлогом предотвращения списания денежных средств.

Мошенник осуществляет рассылку СМС-сообщений с текстом о об угрозе списания с банковской карты денежных средств и абонентским номером для связи либо звонит самостоятельно и, представившись сотрудником безопасности ПАО «Сбербанк», сообщает об угрозе списания денежных средств в ходе разговора. Под предлогом попытки сохранения денежных средств мошенник просит временно перевести деньги с банков-

[1] Это основная услуга SIP-провайдера, которая работает через Интернет по принципу переадресации звонков.

ской карты на «безопасный счет», при этом заверяет, что потом деньги вернутся на обратно на карту. Мошенник диктует реквизиты одного или нескольких банковских счетов, куда необходимо перевести деньги, после чего жертва мошенничества либо через приложение, либо через банкомат переводит свои деньги.

Схема 9. Мошенничество, совершенное под предлогом компенсации за ранее приобретенные БАДы.

На стационарный или абонентский номер потерпевшего звонит мошенник, который представляется сотрудником прокуратуры или правоохранительных органов. Он сообщает, что в настоящий момент задержана группа мошенников, продававших некачественные БАДы либо какие-то другие товары, и что потерпевшему положена компенсация. Обманутому человеку обычно в глубине души хочется возмездия, восстановления справедливости. Тем более что органы правопорядка практически не в силах вернуть добровольно отправленные аферистам деньги, и жертва мошенничества остается со своими потерями один на один. И вот однажды объявляется «герой» и предлагает наказать виновных, а жертве – компенсировать все потери, конечно, не бесплатно, для получения компенсации необходимо оплатить государственную пошлину или налоговый сбор. Человек, пострадавший за веру в чудеса, соглашается: бесплатно ничего (хорошего) не бывает, – и готов оплатить восстановление справедливости. Обычно это выглядит как договор об оказании юридических услуг или оплата комиссии за перевод компенсации. Дотошные махинаторы ведут собственный учет обманутых граждан и время от времени возвращаются к ним с легендами о «помощи в возвращении украденного». Естественно, после оплаты потерпевшим вымышленных государственной пошлины или налогового сбора никакую компенсацию он не получает.

Схема 10. Мошенничество, совершенное под предлогом помощи родственнику, попавшему в беду.

На стационарный или абонентский номер потерпевшего звонит мошенник, который обращается под видом родственника («Привет, мама», «Привет, бабушка» и т.д.). Сообщает, что попал в ДТП и сбил человека или попал в полицию за хранение наркотиков, главное, что решение этого вопроса требует денег, причём очень срочно, и любое промедление может закончится арестом. Чаще всего аферисты работают в ночное время: так жертву проще всего застать врасплох. После сообщения о происшествии первый мошенник передает трубку второму – якобы сотруднику полиции. Представиться могут сотрудником ГИБДД или другим сотрудником ОВД, который, собственно, сам вошел в положение и готов помочь изменить обстоятельства ситуации в пользу задержанного за деньги. Мошенник может изначально представиться как самим

родственником, так и сотрудником организации, осуществившей задержание. В самом распространенном случае мошенник играет роль сына или дочери жертвы. В состоянии шока многим людям кажется, что по телефону они слышат голос действительно родственника. В конце разговора преступник называет точную сумму и способ передачи денег. Деньги просят перевести на номер телефона, на банковскую карту, или передать конверт с деньгами через курьера или водителя такси.

Схема 11. Мошенничество под предлогом романтического знакомства.

Мошенники регистрируются в социальных сетях или на сайтах знакомств, при этом характерно, что загружается очень мало фотографий, как правило, фотографии с гламурной или модельной внешностью, скачанные из интернета. В поле зрения мошенников попадают женщины средних лет и старше, брошенные, разведенные, потерявшие супруга, одинокие матери, которые пытаются найти детям отца, а также отчаявшиеся мужчины, мечтающие встретить любовь, непременно ослепительную красавицу. Восприимчивые люди, ведущие уединенный образ жизни, являются особо желанными целями, поскольку жаждут новых связей. После знакомства на сайте и непродолжительной переписки мошенники предлагают жертвам перенести общение из сайта знакомств в мессенджеры WhatsApp, Viber, Telegram и др. Заблаговременно мошенниками создаются фишинговые сайты[1] различных увеселительно-досуговых организаций (кафе, театров, кинотеатров и т.д.). По внешнему виду мошенники стараются делать данные сайты схожими с оригиналами сайтов указанных организаций. Таким образом, в ходе переписки мошенник предлагает жертве встретиться в кафе, театре, кинотеатре (для этого уже приготовлен соответствующий фишинговый сайт). Жертва может даже заподозрить, что это мошенничество и что ее попросят перевести деньги на билет для собеседника, но никаких денег мошенник не просит, а, наоборот, сообщает, что уже купил себе билет. Мошенник отправляет ссылку на фишинговый сайт, предлагая жертве приобрести билет на соседнее место. На сайте можно ознакомиться с услугами, предоставляемыми организацией (меню, расписание фильмов, спектаклей и т.д.). На сайтах есть опции выбора и покупки билетов, заказа меню. На самом деле, т.к. сайт является фишинговым, под видом приобретения билетов потерпевшие переводят свои деньги мошенникам, причем списание суммы, как правило, происходит неоднократно, до опустошения баланса карты либо блокировки карты системами банка ввиду подозрительной активности. После этого общение прекращается.

[1] Фишинговый сайт – поддельный сайт, который полностью копирует реальный веб-ресурс. Разница может быть всего лишь в одной букве или в символе URL-адреса площадки. Когда на таком сайте вводятся личные данные, например банковские реквизиты, мошенники получают эту конфиденциальную информацию.

Способы телефонных мошенничеств, перечисленные выше, относятся к одним из самых часто используемых. Но этот список далеко не исчерпывающий. Каждый день возникают все новые виды телефонного мошенничества.

3. Проверка сообщений о преступлениях, совершаемых с помощью абонентских устройств

Принятие решения о начале производства расследования совершенного преступления базируется на имеющихся у следователя (дознавателя) материалах проверки сообщения о преступлении.

Поводами для возбуждения уголовного дела по фактам телефонных мошенничеств в соответствии со ст. 140 УПК РФ служат:

- заявление о преступлении. Заявителями, как правило, являются лица, непосредственно пострадавшие от мошеннических действий, в т.ч. являющиеся законными держателями банковских карт. С заявлениями о преступлении нередко обращаются родственники указанных лиц;

- сообщение о совершенном или готовящемся преступлении, полученное из иных источников, оформленное рапортом об обнаружении признаков преступления, составленном в порядке ст. 143 УПК РФ, с прилагающимися к нему материалами. Такими источниками служат результаты ОРД, под которыми в соответствии с п. 36.1 ст. 5 УПК РФ понимаются сведения, полученные в соответствии с федеральным законом «Об оперативно-розыскной деятельности»[1], о признаках подготавливаемого, совершаемого или совершенного преступления, лицах, подготавливающих, совершающих или совершивших преступление и скрывшихся от органов дознания, следствия или суда и предоставленные в соответствии с Инструкцией о порядке предоставления результатов ОРД органу дознания, следователю или в суд[2]. Среди прочих источников стоит отметить выделенные в отдельное производство материалы уголовного дела, содержащие сведения о признаках нового факта мошенничества, выявленного в процессе расследования преступлений в сфере информационно-телекоммуникационных технологий и иных преступлений;

---

[1] Об оперативно-розыскной деятельности [Электронный ресурс]: федеральный закон от 12.08.1995 № 144-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд [Электронный ресурс]: 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. Доступ из справ.-правовой системы «КонсультантПлюс».

- постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании в случае совершения преступления, предусмотренного ст. 159.3 УК РФ, неустановленным лицом;

- явка с повинной.

В ходе проверки сообщения о телефонном мошенничестве сотрудник, которому поручено осуществление данной проверки, пользуется всем арсеналом средств, предусмотренных ч. 1 ст. 144 УПК РФ.

Особенности производства проверочных действий определяет специфика способов совершения рассматриваемой категории преступлений. На первоначальном этапе необходимо в кратчайшие сроки с учетом допустимых уголовно-процессуальным законом средств получить максимально возможный объем информации о наличии либо отсутствии оснований для возбуждения уголовного дела, обстоятельствах произошедшего.

Так, при получении объяснения от пострадавшего лица, контактировавшего с преступниками, следует оформить приложения к протоколу получения объяснения в виде копий необходимых документов, чеков, отпечатанных на бумаге снимков экрана мобильного телефона опрашиваемого (скриншоты) с номерами и временем входящих звонков, имеющейся переписки с преступниками, данных мобильного приложения банка о произведенных платежах, страниц мошеннических сайтов и т.п. При возможности следует приобщить истребованные самостоятельно владельцем телефона и банковских карт детализации звонков и выписки по счетам за интересующий период времени. Получение и фиксация подобным образом в материале проверки данной информации позволит сократить сроки проверки и оперативно принимать дальнейшие решения. Это обусловлено тем, что предусмотренная процедура истребования указанных сведений до возбуждения уголовного дела во многом носит длительный характер и имеет ряд проблемных особенностей.

К примеру, в соответствии со ст. 26 федерального закона «О банках и банковской деятельности» [1] предоставление кредитной организацией справок по операциям, счетам и вкладам до возбуждения уголовного дела осуществляется только должностным лицам, осуществляющим оперативно-розыскную деятельность, на основании судебного решения, полученного в порядке, предусмотренном ст. 9 федерального закона «Об оперативно-розыскной деятельности». Таким образом, следователь (дознаватель), которому поручено осуществить проверку сообщения о преступлении, для законного получения сведений об операциях, счетах и вкладах в кредитной организации может только направить поручение о проведении оперативно-розыскных мероприятий в соответствующий орган дозна-

[1] О банках и банковской деятельности [Электронный ресурс]: федеральный закон от 02.12.1990 № 395-1. Доступ из справ.-правовой системы «КонсультантПлюс».

ния в соответствии с ч. 1 ст. 144 УПК РФ. После этого оперативные работники обращаются в суд, который, в свою очередь, разрешает им проведение такого оперативно-розыскного мероприятия, как «наведение справок». Затем в ходе производства указанного оперативно-розыскного мероприятия банк предоставляет справки по операциям, счетам и вкладам своих клиентов, после чего необходимая информация в виде результатов оперативно-розыскных мероприятий направляется инициатору поручения[1].

В ходе проверки сообщения о телефонных мошенничествах для принятия итогового решения может возникать необходимость истребования информации, помимо операторов сотовой связи и кредитно-финансовых учреждений, у интернет-провайдеров, в IT-компаниях, у администраторов сайтов (в т.ч. сайтов объявлений) и пр. Содержание и оформление таких запросов подробно рассмотрены в параграфе 5 настоящего учебного пособия в разделе «Подготовка и направление запросов».

Основанием для возбуждения уголовного дела в соответствии с ч. 2 ст. 140 УПК РФ является наличие достаточных данных, указывающих на признаки соответствующего преступления, предусмотренного УК РФ. Фактических данных должно быть *достаточно* для вывода о существовании общественно опасного деяния, содержащего признаки преступления. Ключевым фактором при возбуждении уголовных дел по телефонным мошенничествам является установление в ходе проверки суммы похищенных денежных средств с целью отграничения преступления от деяния, не представляющего общественной опасности в силу малозначительности в соответствии с ч. 2 ст. 14 УК РФ.

4. Проблемы определения территориальной подследственности по уголовным делам о телефонных мошенничествах

При возбуждении уголовных дел и дальнейшем расследовании дистанционных мошенничеств особое внимание следует уделить определению подследственности.

Долгое время в практике органов предварительного расследования, прокуратуры и судов не складывается единообразная позиция относительно определения места совершения мошенничеств, связанных с использованием современных средств связи. Различные подходы к разреше-

[1] Козлов В.В. Истребование сведений, составляющих банковскую тайну, при проверке сообщения о преступлении // Особенности производства предварительного расследования на современном этапе развития уголовного процесса России: сб. матлов междунар. науч.-практ. конф-ции / под общ. ред. А.Ю. Терехова, Р.М. Исаевой. М., 2019. С. 62-65.

нию данного вопроса влекут необоснованную передачу материалов проверок и уголовных дел о мошенничествах между различными органами предварительного расследования.

Исследователями также высказаны различные мнения по существу данной проблемы. Некоторые авторы придерживаются позиции, что с целью избежания необоснованного перенаправления сообщений о мошенничествах между органами внутренних дел различных регионов России целесообразно возбуждать и расследовать уголовные дела по месту перечисления потерпевшим денежных средств[1]. Другие полагают, что местом совершения телефонного мошенничества, а следовательно, и местом предварительного расследования является место нахождения виновного[2].

Также в практике имеют место подходы к определению подследственности по месту нахождения (открытия) счета, с которого произошло списание денежных средств, по месту обналичивания денежных средств и по месту нахождения (открытия) счета, на который произошло их зачисление.

В пользу каждой из указанных позиций высказываются соответствующие обоснования, которые исходят из различных толкований требований ст. 152 УПК РФ.

В 2017 г. Пленум Верховного Суда РФ сформировал позицию относительно хищений, совершенных с использованием средств связи, согласно которой такие преступления следует считать оконченными с момента изъятия денежных средств с банковского счета их владельца или электронных денежных средств, в результате которого владельцу этих денежных средств причинен ущерб. Местом окончания мошенничества, состоящего в хищении безналичных денежных средств, согласно начальной редакции постановления Пленума Верховного Суда РФ, являлось место нахождения подразделения банка или иной организации, в котором владельцем денежных средств был открыт банковский счет или велся учет электронных денежных средств без открытия счета[3].

Однако ряд ученых небезосновательно указывают на то, что место открытия банковского счета, с которого изъяты денежные средства, нельзя связывать с местом совершения преступления, поскольку материальные активы, которые являются предметом преступления, не прибывают в конкретное место, при этом не происходит их физическое перемещение

---

[1] Фрост С., Федосов А. Проблемы определения места расследования мошенничества с использованием электронных форм платежей // Законность. 2015. № 1. С. 51-53.

[2] Лукинов А. Место расследования телефонного мошенничества // Законность. 2014. № 9. С. 43-44.

[3] О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

в пространстве, баланс банковского счета является единым для всей платежной системы кредитной организации, управление данным счетом и его обслуживание возможны из любого отделения банка, в котором он открыт, а с возможностями современных технологий – из любой точки мира при помощи сети Интернет[1].

Впоследствии Пленум Верховного Суда РФ в постановлении от 15 декабря 2022 г. № 37, исходя из особенностей предмета и способа рассматриваемого вида мошенничества, определил местом совершения хищения место совершения лицом действий, связанных с обманом или злоупотреблением доверием и направленных на незаконное изъятие безналичных денежных средств[2]. По такому же принципу определяется и территориальная подсудность уголовных дел по данным преступлениям.

Ввиду того, что в большинстве случаев при возбуждении уголовного дела личность преступника и его местонахождение в момент совершения преступления не известны, остающиеся открытыми на уровне федерального законодательства вопросы о территориальной подследственности в настоящее время урегулированы на ведомственном уровне.

Так, в соответствии с приказом МВД России от 3 апреля 2018 г. № 196 органам дознания и предварительного следствия по преступлениям, предусмотренным ст. 158, 159-159.3, 159.5, 159.6 УК РФ, совершенным с использованием платежных карт, средств мобильной связи и информационно-телекоммуникационной сети Интернет, надлежит проводить проверку и принимать решения о возбуждении уголовного дела в органе внутренних дел Российской Федерации, в который поступило сообщение о преступлении, при наличии достаточных данных, указывающих на признаки преступлений. При этом надлежит незамедлительно принимать исчерпывающие меры к раскрытию преступлений и установлению лиц, их совершивших, направлять в установленном порядке запросы в кредитные организации, операторам связи, оказывающим услуги связи, в т.ч. по передаче данных и предоставлению доступа к информационно-телекоммуникационной сети Интернет, и только после выполнения всех возможных процессуальных действий по месту возбуждения уголовного дела и получения достаточных доказательств о совершении преступления на территории обслуживания другого территориального органа МВД Рос-

[1] Багаутдинов Ф.Н., Журба С.М. Актуальные проблемы определения территориальной подследственности мошенничеств, совершаемых с использованием современных средств связи // Уголовное право. 2019. № 3. С. 96-100.

[2] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

сии направлять уголовные дела в порядке, предусмотренном ст. 152 УПК РФ[1].

Таким образом, при расследовании телефонных мошенничеств сложилась практика определения территориальной подследственности *по месту обращения потерпевшего в территориальный правоохранительный орган, уполномоченный принять сообщение о преступлении, возбудить уголовное дело и произвести расследование.*

В дальнейшем при доказанном установлении в ходе производства предварительного расследования места совершения преступления (территории другого административного района, области либо другого субъекта РФ), после выполнения всех необходимых следственных и процессуальных действий уголовные дела необходимо направлять в установленном ст. 152 УПК РФ порядке по территориальной подследственности с уведомлением об этом надзирающего прокурора, а также соответствующего прокурора по месту направления уголовного дела[2].

5. Особенности производства отдельных следственных и иных процессуальных действий при расследовании телефонных мошенничеств

Разнообразие имеющихся схем и методов совершения телефонных мошенничеств, постоянное появление их новых видов делает затруднительной разработку единых алгоритмов по расследованию преступлений рассматриваемой категории и, в частности, по производству следственных и иных процессуальных действий. Вместе с тем обобщение и анализ наработанной на сегодняшний день правоприменительной практики в сфере противодействия дистанционным мошенничествам позволяют выявлять определенные тенденции и закономерности, а также аккумулировать наиболее эффективные приемы и способы применения уголовно-процессуальных средств по данному направлению.

В настоящем учебном пособии рассмотрены ключевые особенности производства следственных и иных процессуальных действий, характерных для большинства видов телефонного мошенничества.

---

[1] О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений [Электронный ресурс]: приказ МВД России от 03.04.2018 № 196. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Наседкин В.А. Где эффективно расследовать телефонные мошенничества, или Еще раз о подследственности // Законность. 2018. № 10. С. 8-9.

Допрос потерпевшего

Отправной точкой в планировании организации расследования преступлений, совершенных в сфере информационно-телекоммуникационных технологий, помимо изучения материалов проверки сообщения о преступлении, является допрос потерпевшего.

Необходимо сразу обратить внимание на типичные ошибки следователя (дознавателя) при производстве допроса потерпевшего. Надзорные органы при изучении уголовных дел указывают, что допрос потерпевшего зачастую сводится к дословному отражению в протоколе информации, изложенной в первоначальном объяснении заявителя[1]. Между тем целью получения объяснений не является получение как можно большей информации для установления обстоятельств, подлежащих доказыванию, а лишь установление факта наличия или отсутствия признаков преступления. Во многих случаях качество получения объяснений оставляет желать лучшего. В итоге содержание допросов потерпевших носит формальный характер, что уже на первоначальной стадии производства по уголовному делу определяет и дальнейший формальный характер расследования.

После признания лица в качестве потерпевшего оно в соответствии со ст. 189 и 190 (191) УПК РФ допрашивается по обстоятельствам совершения мошенничества, при этом выясняются:

- дата, время поступления звонка (СМС-сообщения) с соответствующим содержанием, с какого номера поступил звонок (сообщение);
- абонентский номер потерпевшего, на который поступил звонок, СМС-сообщение (стационарный, мобильный телефон), на кого он зарегистрирован, как давно пользуется данной сим-картой;
- какие были его дальнейшие действия после поступления звонка (СМС-сообщения);
- дословное содержание разговора, кем представился звонивший, что пояснял, как обратился к потерпевшему, сколько человек разговаривали с ним, что предлагали сделать;
- описание голоса звонившего (дефекты речи – хрипота, картавость, шепелявость, заикание), какова была интонация голоса, разговаривал ли он шепотом или обычным голосом; какие особенности, странности в интонации, произношении звуков, в обращении заметил потерпевший, использование в разговоре специальных терминов, специфических речевых оборотов; может ли определить возраст звонившего, по каким приметам потерпевший сможет опознать голос звонившего;

[1] Островский С.А. Типичные нарушения, выявляемые в ходе надзора за расследованием уголовных дел о хищениях, совершенных с использованием средств мобильной связи // Законность. 2017. № 2. С. 23-26.

- качество связи (помехи, пропадала слышимость, разговор прерывался, хорошо или плохо был слышен голос и др.);

- что именно (по возможности дословно) сам заявитель сообщил неизвестному;

- как долго по времени длился телефонный разговор с неизвестным;

- подозревает ли кого-либо в совершении преступления;

- какова сумма материального ущерба, причиненного в результате совершения в отношении него преступления, является ли данный ущерб значительным, если да, то почему (состав его семьи, наличие иждивенцев, размер ежемесячного дохода, из чего он складывается, размер общего дохода всех членов семьи, расходы семьи);

- желает ли заявить гражданский иск о возмещении имущественного вреда, причиненного в результате совершения преступления (если да, то истребовать от потерпевшего заявление, в установленном законом порядке признать его гражданским истцом).

Если передача денежных средств происходила при личном контакте, у потерпевшего необходимо выяснить: обстоятельства передачи денежных средств неизвестному (описание внешности и голоса неизвестного лица (курьера, таксиста и т.д.), по каким приметам сможет его опознать; если передача денег осуществлялась в жилище, установить: когда неизвестный курьер (таксист и т.д.) зашел в квартиру, до каких предметов мебели, иных предметов дотрагивался, как себя вел, что сообщил, задавал ли какие-либо вопросы, задавал ли потерпевший ему какие-либо вопросы; сообщал ли потерпевший неизвестному точную сумму денег, которую передал ему, для каких целей он передает ему эти деньги; судя по поведению неизвестного, был ли тот осведомлен о содержимом, переданном ему, о причинах (целях) передачи ему денежных средств; как потерпевший упаковал деньги; звонил ли неизвестный в момент получения денег кому-либо, что говорил).

При осуществлении безадресного перевода необходимо выяснить полные установочные данные получателя, истребовать у заявителя квитанцию (чек) о переводе.

Если перевод был осуществлен на лицевой счет абонентского номера или счет банковской карты, у потерпевшего выясняются:

- абонентский номер телефона или номер банковской карты потерпевшего, с которой переведены денежные средства, когда, где, в каком отделении какого банка потерпевшим была получена банковская карта, ее реквизиты (номер карты, дата и место открытие счета, номер счета), пользуется ли в настоящее время данной банковской картой, блокировал ли её после совершения преступления;

- как давно пользуется банковскими картами, известны ли ему правила обращения с ними;

- подключена ли у него услуга «Мобильный банк», если да, то на какой абонентский номер телефона;

- почему, получив сообщение с неизвестного номера (телефонный звонок), сам лично не перезвонил в отдел по обслуживанию клиентов соответствующего банка, в котором открыт счет;

- какие именно операции были им проведены, каким образом, их последовательность (если операции проводились через банкомат – адрес банкомата, какие номера набирал в банкомате, желательно последовательность набора абонентских номеров, какие суммы перечислены на каждый номер, появлялись ли на дисплее банкомата сообщения о производимых им операциях, если да, то какие именно; осознавал ли он, что переводит денежные средства;

- абонентский номер телефона или номер банковской карты, на которые были переведены денежные средства;

В случае если хищение совершено с использованием информационно-телекоммуникационной сети Интернет, необходимо также установить:

- дату и время обнаружения объявления (получения ссылки на соответствующий интернет-ресурс);

- с использованием какого технического устройства потерпевший выходил на сайт с размещенным объявлением (переходил по интернет-ссылке): стационарного компьютера, мобильного устройства;

- какие характеристики продаваемого товара были указаны в объявлении о продаже;

- какие условия купли-продажи содержались в объявлении (условия о предоплате, оплате товара, сроках и видах его поставки, ответственности сторон);

- какие контактные данные продавца были указаны в объявлении о продаже;

- имелись ли отзывы, комментарии к объявлению о продаже;

- каким образом, когда (дата, время) потерпевший связался с продавцом;

- отразить подробное содержание разговора с продавцом, как продавец представился, что именно сообщил продавец о продаваемом товаре, об условиях оплаты товара, условиях, сроках и способах доставки покупателю товара;

- каким образом потерпевший известил продавца товара о перечислении денежных средств на указанную им банковскую карту (электронный кошелек);

- что именно потерпевшему сообщил после подтверждения оплаты (перечисления денег на банковскую карту преступника) продавец;

- в какой период времени, куда потерпевший прибыл для получения приобретенного товара;

- когда потерпевший осознал, что в отношении него было совершено мошенничество, в результате которого похищены принадлежащие ему денежные средства;

- сохранилась ли переписка с мошенником.

При допросе потерпевшего по возможности следует истребовать и приобщить к протоколу допроса копию его паспорта, справку о доходах потерпевшего и членов его семьи за последние 6 месяцев, детализацию телефонных переговоров абонентского номера потерпевшего за период переговоров с мошенником.

В настоящем учебном пособии предложен ***пример содержания и оформления протокола допроса потерпевшего*** (см. приложение 1) при получившей большое распространение схеме мошенничества, совершаемого под предлогом предотвращения списания денежных средств, сопровождаемого звонком преступников от имени сотрудников службы безопасности банка и сотрудников полиции.

Допрос свидетеля

При расследовании телефонных мошенничеств следователю (дознавателю) следует уделить должное внимание допросам свидетелей, определив их круг.

Свидетелями могут являться родственники потерпевших, лица, которые в силу наличия у них специальных знаний либо занимаемой должности в кредитной организации могут предоставить сведения, необходимые для создания объективной картины преступления (происшествия). Так, например, у сотрудников кредитных организаций необходимо устанавливать время выдачи карты клиенту, в т.ч. каким способом она передавалась (лично или посредством почтового отправления), ее вид (расчетная, кредитная, предоплаченная), каким образом законный держатель получил ПИН-код и через какое время после ее активации, круг обязанностей, процедуру осуществления платежей и переводов, наличие договора с потерпевшим как держателем платежной карты, имело ли место обращение о ее блокировке, о выписке по лицевому счету, о проверке правомерности списания денежных средств со счета, сумме причиненного ущерба и документах, это подтверждающих. Аналогично могут быть допрошены свидетелями сотрудники компаний сотовой связи, интернет-провайдеров и т.п.

Допрашиваются в качестве свидетелей подставные лица, на которых злоумышленники оформили банковские карты для дальнейшего использования их в преступных целях, если отсутствуют сведения о причастности таковых лиц к совершению преступления.

Свидетелями могут быть лица, занимающиеся скупкой и сбытом поддельных карт, не являющиеся соучастниками расследуемого преступления, лица, участвовавшие в процессе изготовления, приобретения, хране-

ния, транспортировки, сбыта поддельных банковских карт и распоряжений о переводе денежных средств. Помимо деталей участия в вышеуказанных процессах, у данных лиц выясняется в т.ч. осведомленность о преступных намерениях подозреваемого.

Предмет допроса каждой из названных групп свидетелей конкретизируется, исходя из обстоятельств уголовного дела.

Поскольку при телефонном мошенничестве, как правило, используются сим-карты, оформленные на подставных лиц, их установлению и допросу также следует уделить должное внимание. В ходе допроса таких свидетелей необходимо выяснить следующее:

- приобретал ли он на свое имя сим-карты с интересующими абонентскими номерами, если да, то когда и в каком офисе сотовой компании;
- где в настоящее время находятся сим-карты с интересующими абонентскими номерами (в случае, если сим-карта находится при нем, необходимо произвести ее выемку);
- кто пользовался сим-картой в интересующий период времени (когда было совершено преступление);
- какими сотовыми телефонами пользовались в период совершения преступления и пользуются в настоящее время (указать марку, модель и IMEI[1] телефонных аппаратов);
- имеются ли среди родственников и знакомых свидетеля лица, ранее судимые, отбывающие наказание в местах лишения свободы, если да, то указать их полные данные, места, где они отбывают наказание;
- если свидетель никогда не оформлял на свое имя сим-карту с абонентским номером, то терял ли свой паспорт, передавал ли его другим лицам, если да, то кому и с какой целью, кто мог использовать его паспортные данные для оформления сим-карт.

Допрос подозреваемого

При установлении лица, совершившего преступление, производится допрос подозреваемого. Перечень вопросов определяется следователем (дознавателем) в зависимости от вида мошенничества, в т.ч. могут быть выяснены следующие обстоятельства:

- место его постоянного и временного проживания, род деятельности по основной и дополнительной работе, уровень образования, в каких организациях и на каких должностях работал ранее;

[1] IMEI (сокращ. от англ. International Mobile Equipment Identity – международный идентификатор мобильного оборудования) – это номер, обычно уникальный, для идентификации мобильных телефонов.

- где и при каких обстоятельствах были оформлены интересующие следствие сим-карты, банковские карты и счета. Какие документы при этом предоставлялись;

- какие банкоматы либо устройства самообслуживания использовались для осуществления преступной деятельности. Указать адрес и место расположения;

- где хранятся денежные средства или иные материальные ценности, полученные в ходе совершения преступления;

- уровень владения электронно-вычислительной техникой, наличие навыков в сфере программирования;

- наименование сетевого ресурса, используемого для совершения преступления;

- каким способом осуществлялся доступ к сети Интернет (с использованием какой электронно-вычислительной техники, прямым подключением через кабель, с использованием Wi-Fi, беспроводного USB-модема, мобильного интернета и т.д.);

- при каких обстоятельствах был создан интернет-сайт либо учетная запись в сервисах электронной почты, электронных платежных системах, социальных сетях, мессенджерах. Каким образом осуществлялось администрирование указанных ресурсов, какой контент на них размещался;

- совершались ли им ранее подобные действия, если да, то где, когда, при каких обстоятельствах, в каких размерах, были ли у него соучастники;

- субъекты, которым в результате преступления причинен ущерб, его сумма;

- причины совершения преступления;

- наличие соучастников, виды осуществления коммуникации между ними в ходе совершения преступления (номера телефонов, электронные почтовые ящики, мессенджеры);

- иные вопросы, необходимость в выяснении которых может возникнуть в ходе предварительного расследования.

В случае если подозреваемый является участником организованной группы, выясняется количественный состав группы, ее организатор, роль каждого участника, время создания группы, обстоятельства, способствовавшие ее формированию, количество совершенных преступлений и другие вопросы.

При получении ответов подозреваемого лица на вышеуказанные основные вопросы следователь должен самостоятельно определить перечень дополнительных вопросов, исходя из полученной информации и имеющейся доказательственной базы.

Значимой при расследовании уголовных дел данной категории является организация действия по обеспечению возмещения гражданского иска. В связи с этим следователю (дознавателю) необходимо разъяснять по-

дозреваемому, что в соответствии с п. «к» ч. 1 ст. 61 УК РФ добровольное возмещение имущественного ущерба и морального вреда, причиненных в результате преступления, будет учитываться судом в качестве смягчающего обстоятельства при назначении наказания.

Подготовка и направление запросов

Важным этапом расследования преступлений, совершаемых в сфере информационно-телекоммуникационных технологий, является подготовка и направление запросов, а также анализ представленной по ним информации.

Учитывая специфику рассматриваемой категории преступлений, запросы направляются в офисы операторов сотовой связи, администраций интернет-ресурсов, интернет-провайдеров, кредитно-финансовые учреждения, иные организации.

Нормативной основой направления запросов для следователя (дознавателя) является часть 4 ст. 21 УПК РФ, согласно которой для учреждений, организаций, предприятий, должностных лиц и граждан такие запросы обязательны к исполнению. Однако следует учитывать, что процедура предоставления сведений, составляющих охраняемую законом тайну, отдельно регулируется федеральным законодательством.

Так, сведения по операциям и счетам можно получить из кредитных организаций в соответствии с требованиями ст. 26 федерального закона «О банках и банковской деятельности»[1] в рамках возбужденного уголовного дела на основании запроса следователя, согласованного с руководителем следственного органа. При этом стоит отметить, что указанный закон не предоставляет такой возможности дознавателю при расследовании уголовных дел[2]. Получение сведений, касающихся банковской тайны, в таком случае возможно только при производстве выемки данной информации в кредитной организации на основании судебного решения.

В ходе расследования уголовных дел рассматриваемой категории необходимо получать *сведения по банковскому счету*, открытому на имя потерпевшего, с которого были похищены денежные средства (за интересующий период времени), а также по банковским счетам, электронным кошелькам и счетам абонентских номеров, использовавшимся лицом при совершении преступления.

---

[1] О банках и банковской деятельности [Электронный ресурс]: федеральный закон от 02.12.1990 № 395-1. Доступ из справ.-правовой системы «КонсультантПлюс».

[2] Козлов В.В. Истребование сведений, составляющих охраняемую законом тайну, на стадии возбуждения уголовного дела // Евразийский юридический журнал. 2021. № 12 (163). С. 405-407.

В частности, при наличии банковской карты необходимо истребовать:

- информацию о владельце банковской карты (Ф.И.О., дата рождения, паспортные данные);
- дату и место (территориальный банк, внутреннее структурное подразделение банка) открытия счета, выдачи банковской карты;
- информацию о движении денежных средств по банковской карте и счету за интересующий период (включая дополнительный отчет по операциям перечисления с карты на карту и перечисления с карты на номер телефона);
- информацию об абонентском номере, к которому подключена услуга «Мобильный банк», где, когда и каким образом осуществлено подключение;
- информацию об IP-адресах, использованных для входа в онлайн-сервис по управлению данной банковской картой;
- по какой карте осуществляется вход в мобильное приложение банка;
- сведения из мобильного приложения банка: даты и IP-адреса[1] входов в мобильное приложение, способ подтверждения входа, дата и номер телефона регистрации мобильного приложения, наименование мобильного устройства.

Направляя соответствующий запрос, необходимо указать на необходимость сохранения видеозаписей с камер наблюдения в банкоматах за данный период с целью их дальнейшей выемки.

После получения сведений о лице, на чье имя открыта банковская карта, используемая преступником, необходимо направить новые запросы в банк для получения представляющей интерес информации.

По банковскому счету необходимо запрашивать аналогичную информацию, а также информацию о банковских картах, открытых для проведения операций по счету.

При использовании электронных кошельков («Яндекс.Деньги», QIWI и др.), необходимо истребовать информацию:

- о паспортных данных владельца электронного кошелька;
- способе и месте идентификации электронного кошелька;
- абонентском номере, с использованием которого был создан электронный кошелек;
- абонентских номерах, привязанных к электронному кошельку;
- виртуальных банковских картах, которые были выпущены по данному электронному кошельку;

[1] IP-адрес (сокращ. от англ. Internet Protocol Address) – это уникальный адрес, идентифицирующий устройство в интернете или локальной сети, означает набор правил, регулирующих формат данных, отправляемых через интернет или локальную сеть.

- пластиковых картах, выпущенных к данному кошельку, способ их получения (адрес почтового отправления);

- входящих и исходящих платежах по электронному кошельку с момента его регистрации;

- IP-адресах, использованных для совершения денежных транзакций, а также администрирования электронного кошелька.

Относительно использования услуги «Мобильный банк» можно получить следующую информацию:

- историю регистрации из программы «Мобильный банк» по карте (либо по телефону) за интересующий период. В предоставляемой информации указываются: номер карты, номер сотового телефона, даты подключения/отключения, номер банкомата или номер дополнительного офиса, где осуществлялось подключение;

- историю СМС-распоряжений и СМС-уведомлений из программы «Мобильный банк» по телефону за интересующий период. В предоставляемой информации содержатся: номер телефона, дата, время и тексты СМС-распоряжений, поступивших в банк с телефона, дата, время и тексты СМС-уведомлений, отправленных банком на номер телефона, в т.ч. пароли подтверждения и входов.

Обязательным пунктом в планировании расследования является *получение сведений у операторов сотовой связи,* а именно:

- детализация звонков по абонентскому номеру мошенника за последние три месяца – эти сведения позволяют определить, сколько у мошенника сотовых аппаратов (IMEI), как часто он меняет абонентские номера, а также избавляется ли он от сим-карты после совершения мошеннических действий или же использует повторно;

- использованные для связи IMEI за последние месяцы (период конкретизировать);

- использованные для связи базовые станции за последние месяцы с указанием следующих технических характеристик: количество секторов (антенных блоков в месте установки), азимут направленности использованных антенных блоков. Последний, как правило, представлен в числовом выражении и означает угол, под которым находилось абонентское устройство по отношению к базовой станции в момент фиксации его активности в сети;

- информация о входящих и исходящих платежах по лицевому счету абонентского номера;

- информация об IP-адресах, использованных для входа в личный кабинет сотового оператора по управлению данным номером (т.к. в большинстве случаев мошенник использует абонентские номера, зарегистрированные на подставных лиц, и все операции по управлению абонентским

номером проводит через личный кабинет, тем самым оставляя «след» в виде своего IP-адреса);

- паспортные данные владельца абонентского номера;
- копия регистрационной формы – документ, который заполняет продавец сим-карты при ее регистрации. Помимо установочных данных, в нем можно узнать данные об адресе торговой точки, где она была реализована, а также данные продавца с целью последующего его допроса по обстоятельствам приобретения карты.

При осуществлении расследования по ряду видов мошенничества необходимым является *запрос сведений у администраторов сайтов объявлений.* Если мошенник выступает как продавец, необходимо истребовать:

- информацию о лице, разместившем объявление о продаже товара с абонентского номера, его установочные данные;
- использованные преступником для регистрации абонентские номера и электронные почты;
- использованные для создания администрирования объявлений IP-адреса, аналогичную информацию об иных объявлениях данного лица;
- информацию о лицах, создававших объявления с использованием того же абонентского номера или электронной почты;
- аналогичную информацию о иных объявлениях данного лица, установленных при анализе cookie-файлов[1];
- имеющуюся переписку в объявлении.

В случае если мошенник является покупателем, необходимо истребовать информацию об IP-адресах пользователей сайта, просматривавших объявление потерпевшего, при этом в запросе необходимо указать номер объявления.

При расследовании мошенничеств, *совершенных посредством социальных сетей,* необходимо истребовать:

- информацию о пользователе страницы социальной сети (в запросе необходимо указать ссылку на страницу в социальной сети);
- установочные данные;
- использованные им для регистрации абонентские номера и электронные почты;
- IP-адреса, использованные для создания и доступа к странице за последние месяцы;
- аналогичную информацию по иным страницам социальной сети данного пользователя, установленной при анализе cookie-файлов (данный пункт не запрашивается в случае взлома страницы потерпевшего или страниц его друзей).

[1] Cookie-файлы – хранящиеся на компьютерах или мобильных устройствах небольшие файлы, с помощью которых сайт запоминает информацию о посещениях пользователя.

В случаях, когда при совершении преступления *мошенник использовал электронную почту*, в офисах соответствующих компаний («Яндекс», Mail.Ru Group и т.п.) необходимо запросить:

- информацию о паспортных данных владельца электронной почты;
- информацию об использованных для регистрации абонентских номерах;
- информацию об IP-адресах, использованных для доступа к электронной почте за максимально известный период;
- аналогичную информацию по иным электронным почтам, зарегистрированным данным пользователем, установленным при анализе cookie-файлов.

Отметим, что при необходимости получения переписки в социальной сети, переписки посредством электронной почты требуется судебное решение на выемку информации, содержащей охраняемую законом тайну.

При *создании сайтов, используемых мошенниками*, по доменному имени сайта необходимо запросить:

- информацию о паспортных данных регистратора доменного имени;
- информацию об использованных для регистрации абонентских номерах и электронных почтах;
- информацию о том, каким образом была произведена регистрация пользователя;
- информацию об IP-адресах, использованных для регистрации доменного имени;
- информацию об IP-адресах, использованных для входа в личный кабинет или панель управления для администрирования доменного имени;
- информацию об оплате услуг регистрации и аренды доменного имени с указанием полных реквизитов плательщика;
- аналогичную информацию по иным доменным именам, зарегистрированным данным пользователем, установленным при анализе cookie-файлов.

При *использовании мошенником сети Интернет* и установлении IP-адреса у интернет-провайдера необходимо запросить информацию о пользователе и адресе использованного оборудования, которому был выдан интересующий IP-адрес в необходимый промежуток времени.

Кроме того, следователю (дознавателю) в ходе расследования путем направления запросов необходимо организовать сбор характеризующего материала о личности преступника.

Помимо данных о личности подозреваемого (обвиняемого), с целью возмещения материального ущерба, причиненного преступлением, а также обеспечения гражданского иска или исполнения приговора в виде штрафа необходимо запросить и приобщить документы, характеризующие его материальное положение (о наличии счетов, вкладов – в кредитно-финансовых организациях, о наличии объектов недвижимости – в Росре-

естре, сведения о наличии автотранспорта – в ГИБДД МВД России по субъекту, о доходах – в УФНС России по субъекту, о наличии тракторов и дорожно-строительной техники – в Гостехнадзор и т.п.). После получения сведений необходимо принять меры к изъятию установленного имущества, иных активов с последующим наложением ареста.

Для быстрого и качественного получения интересующей органы предварительного расследования информации необходимо соблюдать определенные *требования в оформлении и содержании запросов*. Учреждения и организации, куда направляются запросы, нередко отказывают в их исполнении. Причины отказа в исполнении запросов:

- оформление запросов, которые по форме и содержанию не соответствуют формальным требованиям, предъявляемым к нормативным правовым актам;

- направление запросов за подписью неуполномоченных должностных лиц;

- направление запросов при отсутствии оснований и условий, установленных законодательством;

- несоблюдение порядка истребования сведений, составляющих охраняемую законом тайну;

- направление запросов субъектам, не обладающим искомой информацией.

В частности, причинами отказа в предоставлении сведений, составляющих банковскую тайну, являются:

- отсутствие в запросах исчерпывающих данных, позволяющих установить их обоснованность, в т.ч. сведений о возбужденном уголовном деле;

- отсутствие в запросах органов предварительного следствия по делам, находящимся в их производстве, сведений о согласии руководителя следственного органа;

- подписание запросов неуполномоченными должностными лицами;

- наличие технических ошибок, в частности, неточное указание реквизитов организаций, отсутствие гербовой печати в запросах[1].

В связи с этим необходимо обращать внимание на недопущение данных ошибок, правильность заполнения реквизитов инициирующей запрос стороны и адресата, в содержании указывать основания, причины, мотивы запроса сведений, информацию об уголовном деле, в рамках которого направлен запрос, соблюдать наличие необходимых штампов и печатей, подписей уполномоченных должностных лиц, в связи с чем предлагается примерный ***образец запроса в кредитно-финансовое учреждение*** (см. приложение 2).

[1] Сидоркин А.И. Практика применения органами внутренних дел законодательства в сфере охраняемой законом тайны // Российский следователь. 2015. № 21. С. 37-43.

Производство выемки

Одним из распространенных следственных действий при расследовании телефонных мошенничеств является выемка. Выемка производится в целях изъятия определенных предметов и документов, имеющих значение для уголовного дела, о месте нахождении которых известно органам расследования (ст. 183 УПК РФ).

Так, после производства допроса потерпевшего целесообразно на основании соответствующего постановления следователя (дознавателя) произвести у потерпевшего выемку имеющихся у него документов или материальных носителей, содержащих сведения о совершении преступления (в т.ч. платежных поручений, приходных кассовых ордеров, кассовых чеков, скриншотов, фиксирующих осуществление транзакций, мобильных телефонов, других устройств, содержащих переписку в социальных сетях, текстовые СМС-сообщения, детализацию соединений по его абонентскому номеру и пр.), а также документов, отражающих переписку потерпевшего с лицом, совершившим преступление.

Следует обратить внимание, что выемка предметов и документов, содержащих информацию, составляющую охраняемую законом тайну, в частности, банковскую тайну, тайну переписки, производится на основании судебного решения в порядке, предусмотренном ст. 165 УК РФ.

По уголовным делам о телефонных мошенничествах выемка производится у законных владельцев платежных карт, в банках-эмитентах (банках, выпускающих в обращение пластиковые карты), банках-эквайерах (обслуживающих банках), в кредитных, торговых, сервисных и иных организациях. У законного владельца платежной карты могут быть изъяты подлинная платежная карта, информация с которой использовалась при изготовлении поддельной карты, договор с банком на обслуживание, копии квитанций о совершенных им операциях с использованием карты. В банках-эмитентах выемке подлежат: стоп-листы с перечнем похищенных или утраченных платежных карт; документы, содержащие сведения о подлинном держателе карты (досье клиента); подлинники платежных квитанций или их заверенные копии; акты (или их заверенные копии) о сдаче торговыми, сервисными и иными организациями в банк квитанций для оплаты, копия договора между торговым предприятием и кредитной организацией об обслуживании держателей платежных карт, платежные документы о перечислении денежных средств на счета торговых предприятий и другие документы. В торговых (сервисных) организациях подлежат выемке: копии заявления в банк о заключении договора на обслуживание платежных карт при оплате товаров, работ, услуг; копия договора с банком о предоставлении такого права; квитанции, чеки на товары, приобретенные по принадлежащей другому лицу или поддельной карте; записи с камер видеонаблюдения, на которых зафиксирован факт предъявления

платежной карты к оплате; копии документов, подтверждающих стоимость оплаченных товаров, работ, услуг и другие документы.

При производстве выемки в учреждениях связи на основании судебного решения следует изымать сведения о входящих и исходящих сообщениях электронных почтовых ящиков, об абонентах, которым в указанный момент времени выдавался установленный IP-адрес, о MAC-адресах[1] как самой компьютерной техники, так и сетевого оборудования, с использованием которых осуществлялся доступ к сети Интернет. В зависимости от обстоятельств конкретного уголовного дела в учреждениях связи по судебному решению могут быть изъяты и иные сведения, которые с учетом требований федерального закона «О связи» также распространяют на себя положения об их тайне (ст. 53), однако действующая практика позволяет их получать и без судебного разрешения, на основе запроса о предоставлении сведений, не являющихся информацией ограниченного доступа. К таким сведениям следует относить данные:

- об абоненте с указанием его установочных данных;
- о номере и дате заключенного договора об оказании услуг с приложением заверенной копии договора;
- протоколы работы в сети Интернет (log-файлы);
- об IP-адресах, с которых осуществлялось создание и администрирование аккаунта.

В ходе выемки также осуществляется изъятие видеозаписей с камер видеонаблюдения, установленных вблизи или на банкоматах, с помощью которых похищенные денежные средства были обналичены. Проблемой в данном случае является недолгий срок хранения видеоматериалов. Следует отметить, что система видеонаблюдения банкомата состоит из нескольких камер, которые зачастую позволяют рассмотреть преступника, снявшего денежные средства.

Производство обыска

При наличии достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться орудия, оборудование или иные средства совершения преступления, предметы, документы и ценности, которые могут иметь значение для уголовного дела, в соответствии со ст. 182 УПК РФ необходимо производство обыска.

Обыск может проводиться в жилище подозреваемого, его родственников, предполагаемых соучастников преступления, загородных домах, гаражах, помещениях, оборудованных мошенниками под кол-центры, в офисах субъектов платежной системы при наличии информации об уча-

[1] MAC-адрес – уникальный код, присвоенный производителем сетевому устройству.

стии их сотрудников в хищении денежных средств или нахождении в них документов, материалов, которые могут быть использованы в ходе предварительного следствия в качестве доказательств, и иных местах, в которых, по имеющейся в уголовном деле информации, могут находиться документы, предметы, материальные ценности, имеющие значение для дела.

Обыск в жилище производится на основании судебного решения в порядке, предусмотренном ст. 165 УК РФ. При планировании обыска в помещении следователь (дознаватель), имея основания полагать, что обнаруженные и изъятые предметы и документы могут содержать охраняемые законом сведения, в т.ч. банковскую, коммерческую тайну, тайну переписки, также должен получить судебное решение на его производство с целью дальнейшего законного использования результатов обыска в доказывании. При этом следователю (дознавателю) в своем ходатайстве, а суду в судебном постановлении о разрешении производства обыска следует более конкретно указывать, с какой целью проводится следственное действие: например, «с целью обнаружения и изъятия электронных носителей информации и абонентских устройств, содержащих охраняемые законом сведения, и иных предметов, документов и ценностей, которые могут иметь значение для уголовного дела». В таком случае дополнительного разрешения суда для производства осмотра абонентского устройства не требуется, поскольку ранее суд уже ограничил права лица, в т.ч. и на тайну переписки[1].

При изъятии электронных носителей в ходе обыска должно быть обеспечено участие специалиста в области компьютерных технологий. Как правило, в качестве специалистов привлекаются сотрудники ЭКЦ, специализирующиеся на производстве компьютерных экспертиз, или сотрудники Центра информационных технологий, связи и защиты информации (ЦИТС и ЗИ) ГУ МВД России по субъектам Российской Федерации. В исключительных случаях привлекать к участию в обысках следует иных лиц, имеющих основное или дополнительное образование в сфере информационных технологий.

В ходе обыска обнаружению, фиксации и изъятию подлежат:

- оборудование, приспособления, инструменты, предметы, документы и материалы, которые могли быть использованы для изготовления поддельных платежных карт;

- квитанции на оплату товаров, работ, услуг с использованием поддельной (похищенной, утраченной) карты;

- документы, принадлежащие другим лицам или удостоверяющие личность держателя платежной карты;

[1] Клевцов К.К., Квык А.В. Изъятие и осмотр информации, находящейся в электронной памяти абонентских устройств // Законность. 2020. № 12. С. 56-60.

- материальные ценности, похищенные с использованием поддельных или принадлежащих другим лицам платежных карт, а также товарные ярлыки на них;

- ноутбуки, системные блоки компьютера с накопителями на жестких магнитных дисках (на них может содержаться информация о сайтах, которыми пользовался подозреваемый, его переписка);

- списки сайтов интернета, которые использовались для осуществления преступной деятельности;

- средства мобильной связи, сим-карты;

- записные книжки и другие документы, предметы и материалы, имеющие значение для расследования уголовного дела.

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

Характерным следственным действием при расследовании телефонных мошенничеств является получение информации о соединениях между абонентами и (или) абонентскими устройствами. Данное следственное действие производится в порядке, предусмотренном ст. 186.1 УПК РФ, на основании постановления суда о разрешении получения информации о соединениях между абонентами и (или) абонентскими устройствами.

В ходе расследования уголовного дела необходимо получать детализации соединений как по абонентскому номеру, используемому мошенником, так и по абонентскому номеру потерпевшего. Если для получения информации о соединениях по абонентскому номеру мошенника необходимо обязательно получить судебное решение и направить его для исполнения оператору связи, то детализацию по абонентскому номеру потерпевшего возможно получить от последнего в ходе выемки.

Необходимо учитывать, что согласно ст. 64 федерального закона «О связи»[1] информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи операторы связи на территории Российской Федерации обязаны хранить в течение трех лет с момента окончания осуществления таких действий, а текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщения пользователей услугами связи – до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

При установлении факта регистрации интересующего органы предварительного расследования абонента у того или иного оператора связи вы-

[1] О связи [Электронный ресурс]: федеральный закон от 07.07.2003 № 126-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

носится постановление о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами. Следователь (дознаватель) в постановлении указывает, какие именно сведения необходимы для уголовного дела (детализация вызовов, данные сим-карты, геолокация устройства, идентификационный номер IMEI либо иные). В постановлениях о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентским устройствами с привязкой к приемо-передающим базовым станциям необходимо конкретизировать запрашиваемую информацию, например: ходатайствовать перед судом о получении информации о соединениях между абонентами и (или) абонентским устройствами с привязкой к приемо-передающим базовым станциям, а именно: детализации телефонных переговоров с привязкой к приемо-передающим базовым станциям конкретного абонентского номера за конкретный (вплоть до минуты) период времени с обязательным указанием номеров приемо-передающих базовых станций (CID)[1], местах их расположения (адресе), информации о зоне с неповторяющимися частотами, на которых излучает каждая базовая станция (LAC)[2], азимутах и ширине направленности диаграммы антенны каждой базовой станции. Получение таких подробных сведений о номере приемо-передающей базовой станции, информации о зоне с неповторяющимися частотами, на которых излучает базовая станция, облегчает установление места расположения приемо-передающей базовой станции.

Постановление об указанном ходатайстве с согласия руководителя следственного органа (прокурора) направляется в суд (предложен ***образец постановления*** (см. приложение 3)). В случае принятия судом решения о необходимости получения информации о соединениях между абонентами и (или) абонентскими устройствами постановление и копия решения направляются следователем (дознавателем) в соответствующую организацию связи. Руководитель организации связи, куда они были направлены, обязан предоставить интересующую информацию.

Полученный носитель осматривается, при необходимости – с участием специалиста, при этом подробно описываются все технические действия, связанные с просмотром информации. При производстве следственного действия, предусмотренного ст. 186.1 УПК РФ, осмотр документов (либо предметов – носителей информации) выступает частью рабочего этапа получения информации о соединениях между абонентами и (или) абонентскими устройствами, что определяет комплексный характер

[1] CID – ID (идентификационный номер) базовой станции.

[2] LAC – известные параметры.

рассматриваемого следственного действия[1]. Изученные материалы приобщаются в полном объеме на основании постановления следователя (дознавателя) и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность.

Осмотр предметов и документов

После производства выемки, обыска, а также получения запрашиваемой информации необходимо произвести осмотр изъятых предметов и документов, а в ряде случаев – также носителей представленных по запросам сведений.

Так, при осмотре предметов – платежных карт – устанавливаются внешние характеристики: размеры карт или их заготовок, реквизиты, наличие и содержание эмбоссированной (рельефной) информации, наличие даты истечения срока действия, магнитной полосы, подписи на подписном поле и индивидуальных признаков, указывающих на подлинность или поддельность платежной карты.

При осмотре чеков – документов, являющихся доказательством совершения покупки или получения определенной услуги от торговой, сервисной организации или наличных денежных средств от банка с использованием платежной карты, и квитанций – документов, содержащих сведения о произведенных расчетах с использованием платежных карт, в ходе осмотра обращается внимание на номер платежной карты или иного платежного документа, код и координаты пункта обслуживания, стоимость товара (услуги), дату операции, подпись держателя карты и продавца (кассира).

При осмотре предоставленных банком по запросу выписок со счетов клиентов обращается внимание на дату совершения интересующих операций, суммы переводимых (снимаемых) денежных средств, номер счета и реквизиты контрагентов, назначение платежей, адреса банкоматов, наименования отделений банка.

При осмотре банкомата и платежного терминала (видом осмотра является, как правило, осмотр места происшествия) следует обратить внимание на целостность корпуса, проверяется наличие на корпусе марки-пломбы, идентификационного номера, который в дальнейшем может быть использован для направления запроса администратору платежной системы или оператору сотовой связи с целью получения подтверждающей информации о факте перевода (зачисления) денежных средств, наличие по-

[1] Демин Ю.В. Организационно-правовые основы выявления и раскрытия краж, совершаемых с банковского счета, а равно в отношении электронных денежных средств // Российский следователь. 2021. № 1. С. 64-68.

сторонних программно-аппаратных средств (скиммеров[1], накладных клавиатур и т.п.), следов рук. К осмотру необходимо привлекать соответствующих специалистов, в т.ч. поставщика данной техники или специалиста центра технического обслуживания. Кроме того, осуществляется осмотр записей камер видеонаблюдения, на которых содержится информация о событии преступления, лицах, подозреваемых в его совершении, их соучастниках, свидетелях мошенничества, об автотранспорте, находящемся около банкомата в момент совершения преступления и, возможно, принадлежащего злоумышленникам.

В зависимости от объекта осмотра к участию в его производстве следователь (дознаватель) может привлекать иных лиц. Так, осмотр изъятых у потерпевшего предметов и документов целесообразно произвести с участием потерпевшего и специалиста (при необходимости), в ходе которого зафиксировать сведения, имеющие доказательственное значение (переписка с лицом, совершившим преступление, сведения о переводе средств в электронных платежных системах, текст СМС-сообщений).

Следует оформлять приложения к протоколу осмотра в виде скриншотов экрана компьютера, мобильного телефона (с целью обеспечения наглядности). После чего предметы и документы, имеющие доказательственное значение для уголовного дела, необходимо признать и приобщить в качестве вещественных доказательств, определив их место хранения.

[1] Скиммер – инструмент, используемый преступниками для считывания данных банковской карты.

Заключение

В связи с массовым распространением средств мобильной коммуникации, развитием цифровых технологий и, как следствие, ростом количества совершаемых в данной сфере преступлений и изощренностью способов их совершения знание и владение спецификой расследования телефонных мошенничеств сотрудниками органов внутренних дел, осуществляющими предварительное расследование, имеет важнейшее значение в достижении успешных результатов в борьбе с преступностью.

Современный следователь, дознаватель, специализирующийся на расследовании рассматриваемой категории преступлений, должен постоянно совершенствовать свои познания в технической реализации различных способов мошенничества, учитывать нормативную основу предоставления организациями, предприятиями, учреждениями и должностными лицами той или иной информации, имеющей значение для расследования уголовного дела, учитывать указанные особенности при производстве следственных действий и собирании доказательств.

Выражаем надежду на то, что настоящее учебное пособие позволит дознавателям и следователям органов внутренних дел эффективно расследовать преступления, совершаемые в сфере информационно-телекоммуникационных технологий, и, в частности, телефонные мошенничества, а также заинтересует обучающихся и обеспечит возможность успешно подготовиться к занятиям по темам, связанным с расследованием преступлений.

Список литературы

I. Нормативные правовые акты

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.03.2020 № 1-ФКЗ) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 14.07.2022) [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 18.07.2022). [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

4. О банках и банковской деятельности [Электронный ресурс]: федеральный закон от 02.12.1990 № 395-1. Доступ из справ.-правовой системы «КонсультантПлюс».

5. О связи [Электронный ресурс]: федеральный закон от 07.07.2003 № 126-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

6. Об оперативно-розыскной деятельности [Электронный ресурс]: федеральный закон от 12.08.1995 № 144-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

7. О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений [Электронный ресурс]: приказ МВД России от 03.04.2018 № 196. Доступ из справ.-правовой системы «КонсультантПлюс».

8. Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд [Электронный ресурс]: 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. Доступ из справ.-правовой системы «КонсультантПлюс».

II. Материалы судебной практики

9. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48. Доступ из справ.-правовой системы «КонсультантПлюс».

10. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных пре-

ступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет» [Электронный ресурс]: постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. Доступ из справ.-правовой системы «КонсультантПлюс».

III. Специальная литература

11. Багаутдинов Ф.Н., Журба С.М. Актуальные проблемы определения территориальной подследственности мошенничеств, совершаемых с использованием современных средств связи // Уголовное право. 2019. № 3. С. 96-100.

12. Демин Ю.В. Организационно-правовые основы выявления и раскрытия краж, совершаемых с банковского счета, а равно в отношении электронных денежных средств // Российский следователь. 2021. № 1. С. 64-68.

13. Клевцов К.К., Квык А.В. Изъятие и осмотр информации, находящейся в электронной памяти абонентских устройств // Законность. 2020. № 12. С. 56-60.

14. Козлов В.В. Истребование сведений, составляющих охраняемую законом тайну, на стадии возбуждения уголовного дела // Евразийский юридический журнал. 2021. № 12 (163). С. 405-407.

15. Лукинов А. Место расследования телефонного мошенничества // Законность. 2014. № 9. С. 43-44.

16. Наседкин В.А. Где эффективно расследовать телефонные мошенничества, или Еще раз о подследственности // Законность. 2018. № 10. С. 8-9.

17. Островский С.А. Типичные нарушения, выявляемые в ходе надзора за расследованием уголовных дел о хищениях, совершенных с использованием средств мобильной связи // Законность. 2017. № 2. С. 23-26.

18. Сидоркин А.И. Практика применения органами внутренних дел законодательства в сфере охраняемой законом тайны // Российский следователь. 2015. № 21. С. 37-43.

19. Фрост С., Федосов А. Проблемы определения места расследования мошенничества с использованием электронных форм платежей // Законность. 2015. № 1. С. 51-53.

Приложение 1

ПРОТОКОЛ
допроса потерпевшего

г. Энск (место составления) «*26*» *апреля* 20*22* г. (дата составления)

Допрос начат в 16 ч 30 мин
Допрос окончен в 18 ч 05 мин

Следователь отдела по организации расследований на территории, обслуживаемой ОП по Центральному району УМВД России по г. Энску, старший лейтенант полиции А.А. Сидоров
в помещении *служебного кабинета № 205 ОП по Центральному району УМВД России по г. Энску*, расположенном по адресу *г. Энск, ул. Интернациональная, 121*
в соответствии со ст. 189 и 190 (191) УПК РФ допросил по уголовному делу № *** в качестве потерпевшего:
1. Фамилия, имя, отчество: *Иванова Таисия Антоновна*
2. Дата рождения: *25 мая 1986 г.*
3. Место рождения: *г. Энск Энской области*
4. Место жительства и (или) регистрации: *Энская область, г. Энск, пр-т Красноармейский, д. 51, кв. 15*
телефон: *8-961-***-11-11*
5. Гражданство: *РФ*
6. Образование: *среднее специальное*
7. Семейное положение, состав семьи: *не замужем, сын Иванов А.В., 2016 г.р.*
8. Место работы или учебы, род занятий или должность: *менеджер по продажам, ООО «Профит», г. Энск, пр-т Ленина, 2*
телефон: *8-***-2-398-225*
9. Отношение к воинской обязанности: *невоеннообязанная, на воинском учете не состоит*
10. Наличие судимости: *не судима*

Потерпевшая *Иванова* (подпись)

11. Паспорт или иной документ, удостоверяющий личность потерпевшего: *паспорт серии 0101 № 73**74, выдан 12.12.2012 ТП УФМС России по Алтайскому краю*
12. Иные данные о личности потерпевшего: *не имеется*

Иные участвующие лица *не участвовали*

Потерпевшая *Иванова* (подпись)

Лица, участвующие в следственном действии, были заранее предупреждены о применении при его производстве технических средств *не применялись*

Потерпевшая *Иванова*
(подпись)

Перед началом допроса мне разъяснены права и обязанности потерпевшего, предусмотренные частью второй ст. 42 УПК РФ. Согласно ст. 18 УПК РФ мне разъяснено право давать показания на родном языке или на том языке, которым я владею, а также пользоваться помощью переводчика бесплатно. Мне также разъяснено, что в соответствии со ст. 51 Конституции Российской Федерации я не обязан(а) свидетельствовать против самого себя, своего супруга (своей супруги) и других близких родственников, круг которых определен п. 4 ст. 5 УПК РФ. При согласии дать показания я предупрежден(а) о том, что мои показания могут быть использованы в качестве доказательств по уголовному делу, в том числе и в случае моего последующего отказа от этих показаний.

Об уголовной ответственности за отказ от дачи показаний по ст. 308 УК РФ и за дачу заведомо ложных показаний по ст. 307 УК РФ предупрежден(а)

Потерпевшая *Иванова*
(подпись)

По существу уголовного дела могу показать следующее[1]: 22 апреля 2022 г. в отношении меня были совершены мошеннические действия. Неизвестные мне лица, представившиеся сотрудниками банка и полиции, по мобильному телефону сообщили мне, что мой банковский счет находится под угрозой. Я, ничего не подозревая, выполнила по их указанию определенные действия по переводу с моего счета денежных средств. В результате чего у меня были похищены принадлежащие мне денежные средства в общей сумме 50 000 рублей, о чем от меня поступило заявление в полицию.

Потерпевшая *Иванова*
(подпись)

[1] Предмет допроса может быть различным в зависимости от способа/схемы хищения денежных средств граждан посредством телефонного мошенничества. Порядок изложения информации в описательной части протокола допроса также может быть различен: в виде свободного рассказа или в виде «вопрос – ответ». В данном случае в образовательных целях предложен второй вариант, чтобы наглядно отразить перечень вопросов, ответы на которые необходимо получить в ходе расследования преступления рассматриваемого вида.

Вопрос следователя: ***Где, когда и при каких обстоятельствах произошло событие, по поводу которого Вы обратились в полицию в связи с хищением денежных средств с Вашей банковской карты?***

Ответ Ивановой Т.А.: 22 апреля 2022 г. около 15 часов я находилась на работе в г. Энске по адресу пр-т Ленина, 2, когда мне на сотовый телефон поступил звонок. В ходе телефонного разговора со мной беседовал мужчина, который представился Сергеем Викторовичем Захаровым, сотрудником безопасности ПАО «Сбербанк». Он пояснил, что у меня имеются банковские карты, назвал первые и последние цифры карт, какие именно, я сейчас не помню, и также сказал, что на меня в Читинской области пытались оформить кредит. Далее он пояснил, что во избежание списания денежных средств мне нужно зайти в приложение «Сбербанк Онлайн» и отменить заявку. Я сказала, что такая программа у меня есть, однако в настоящее время у меня отсутствует мобильный интернет. Человек, представившийся сотрудником безопасности банка, сказал, что надо подключить интернет, для того чтобы совершить определенные действия. Но у меня в тот момент не было возможности это сделать. Тогда он сказал, что перезвонит позже.

После этого с незнакомого номера мне позвонил мужчина, представился сотрудником полиции, свои данные не называл. Он спросил, разговаривала ли я с Сергеем Викторовичем. Я ответила, что разговаривала. Мужчина сказал мне, что в отношении моего банковского счета совершались незаконные действия с целью похитить денежные средства. При этом он заверил меня, что действия сотрудника безопасности банка правомерны и что для предотвращения хищения моих денежных средств мне необходимо выполнить то, что скажет мне Сергей Викторович. Он говорил убедительно, и я ему поверила. Затем мне снова позвонил Сергей Викторович, сказав, что денежные средства, которые находятся на моей карте, необходимо временно перевести на безопасный счет, при этом заверив меня, что потом деньги вернутся на мою карту. Сразу после этого я, доверившись людям, мне звонившим, будучи уверенной, что разговариваю с сотрудниками банка и полиции, пошла в торговый центр «Пассаж», расположенный в г. Энске на пр-те Ленина, к банкомату ПАО «Сбербанк», находящемуся на втором этаже названного здания. При этом сотрудник безопасности банка был на связи и говорил, как мне действовать. Он продиктовал мне номера, на которые я перевела со своей карты разными суммами денежные средства в общем размере 50 000 рублей. Мужчина, называвший себя Сергеем Викторовичем, сказал, что теперь мне надо ждать и что он свяжется со мной потом. На следующий день я позвонила по тому номеру, с которого мне звонил Сергей Викторович, но абонент был недоступен. После этого я поняла, что меня обманули, и обратилась в полицию.

Иванова

Вопрос следователя: ***Подавали ли ранее заявки на кредиты, когда и где, были ли одобрены?***

Ответ Ивановой Т.А.: 21 января 2022 г. я решила оформить кредит в одном из банков, для чего осуществила вход в сеть Интернет, где и оставила заявку на одном из сайтов: m.kovalut.ru. На данном сайте я указала следующую информацию о себе: свои фамилию, имя, отчество, дату рождения, паспортные данные, номер телефона, место проживания, место работы, стаж работы, размер заработной платы, сумму предполагаемого кредита, возможно, вводила в анкету и другие данные о себе, в настоящее время не помню. Одобрение кредита мне так и не пришло.

Иванова

Вопрос следователя: ***Сколько у Вас имеется банковских счетов и банковских карт? Когда, в каких банках и по какому адресу были открыты счета, с которых были похищены денежные средства?***

Ответ Ивановой Т.А.: Согласно имеющимся при мне документам на открытие счета, у меня в пользовании имеется счёт в ПАО «Сбербанк», к которому привязана банковская карта № 2202 2002 *** 8626. Счет был открыт 19.02.2015 в дополнительном офисе банка № 8644/0172 по адресу г. Энск, пр-т Красноармейский, 58а/1. На указанную карту я получаю заработную плату. Больше никаких счетов на мое имя не открыто. Именно с этой карты были похищены денежные средства.

Иванова

Вопрос следователя: ***Какая сумма находилась на счете, с которого были похищены денежные средства?***

Ответ Ивановой Т.А.: 20 апреля 2021 г. на данную карту я получила заработную плату и премию в размере 40 000 рублей, вместе с остатком в 11 000 рублей общий баланс составлял 51 000 рублей.

Иванова

Вопрос следователя: ***С каких телефонов Вы вели разговоры с лицами, инструктирующими Вас о переводе денежных средств? На кого зарегистрированы эти номера?***

Ответ Ивановой Т.А.: Я пользуюсь мобильным телефоном с абонентским номером 8-961-***-11-11 с 2010 г., сотовый оператор «Билайн». Сим-карта зарегистрирована на мое имя. Больше мобильных номеров на мне не зарегистрировано. Другими номерами я не пользуюсь. Все разговоры осуществлялись с данного номера.

Иванова

Вопрос следователя: ***Можете ли Вы сказать точно, в какое время и с каких номеров телефонов Вам звонили лица, представившиеся сотрудником банка и сотрудником полиции?***

Ответ Ивановой Т.А.: Да, я могу сказать точно, поскольку журнал звонков сохранен в моем мобильном телефоне, к тому же я сделала скриншоты журнала звонков за 22 апреля 2022 г.

Так, человек, представившийся сотрудником безопасности ПАО «Сбербанк», звонил мне в 15:28 и в 16:47 с незнакомого мне номера +7-495-400-55-55. Мужчина, представившийся сотрудником полиции, звонил мне в 15:35 с незнакомого мне номера +7-385-2-397-130.

Иванова

Вопрос следователя: ***Велась ли переписка с данными лицами посредством СМС-сообщений или интернет-мессенджеров?***

Ответ Ивановой Т.А.: Нет, переписка не осуществлялась.

Иванова

Вопрос следователя: ***Имеются ли записи телефонных разговоров с лицами, по просьбе которых Вы перечислили с Вашей банковской карты принадлежащие Вам денежные средства?***

Ответ Ивановой Т.А.: Нет, разговоры я не записывала.

Иванова

Вопрос следователя*: Сохранились ли чеки произведенных Вами операций по рассматриваемому перечислению денежных средств?*

Ответ Ивановой Т.А.: Нет, данные чеки у меня не сохранились.

Иванова

Вопрос следователя: ***Можете ли Вы сказать, когда точно, какими суммами и на какие номера зачислялись Вами денежные средства?***

Ответ Ивановой Т.А.: Да, согласно данным мобильного приложения «Сбербанк Онлайн», которое установлено на моем телефоне, 22 апреля 2022 г. мною были осуществлены следующие денежные переводы: в 16:52 я перевела денежные средства в сумме 14 634,15 рубля на номер 8-953-365-76-02 (комиссия составила 365,85 рубля); 18.01.2022 в 16:55 я перевела денежные средства в сумме 14 634,15 рубля на номер 8-953-365-76-02 (комиссия составила 365,85 рубля); 18.01.2022 в 16:57 я перевела денежные средства в сумме 14 634,15 рубля на номер 8-953-156-88-95 (комиссия составила 365,85 рубля); 18.01.2022 в 16:58 я перевела денежные средства в сумме 4878,05 рубля на номер 8-953-156-88-95 (комиссия составила 121,95 рубля). С учетом комиссии я перевела денежные средства на общую сумму 50 000 рублей.

Кроме того, я истребовала в ПАО «Сбербанк» выписку по счету за 22 апреля 2022 г., которая находится при мне.

Иванова

Вопрос следователя: ***Является ли причиненный Вам ущерб для Вас значительным?***

Ответ Ивановой Т.А.: Да, причиненный мне ущерб в сумме 50 000 рублей является для меня значительным, поскольку моя ежемесячная заработная плата составляет 28 000 рублей, иного источника дохода у меня не имеется, а расходы на продукты питания и коммунальные платежи составляют более 20 000 рублей в месяц. Кроме того, у меня на иждивении находится сын Иванов А.В., 2016 г.р., алиментов не получаю.

Иванова

Вопрос следователя: ***Запомнили ли Вы голоса звонивших Вам мужчин? Если да, то по каким признакам, и сможете ли их опознать?***

Ответ Ивановой Т.А.: Голос мужчины, представившегося сотрудником полиции, я не запомнила и опознать не смогу. Голос мужчины, представившегося сотрудником безопасности банка, я запомнила хорошо и смогу опознать по манере разговора, быстрой речи, высокому тембру, интонации, специфическому произношению звука «г».

Иванова

Вопрос следователя: ***Звонили ли Вы на горячую линию банка, чтобы проверить информацию о попытке хищения Ваших денежных средств со счета?***

Ответ Ивановой Т.А.: Нет, так как я была уверена, что по телефону общаюсь с сотрудником банка.

Иванова

Вопрос следователя: ***Звонили ли Вы в банк с целью заблокировать перевод денежных средств, после того как поняли, что в отношении Вас совершено мошенничество?***

Ответ Ивановой Т.А.: Да, звонила, мне ответили, что моя карта была заблокирована, а также что возвратить денежные средства они уже не могут и сказали, чтобы я обращалась в полицию.

Иванова

Вопрос следователя: ***Знали ли Вы о дистанционных хищениях денежных средств?***

Ответ Ивановой Т.А.: Да, слышала про это из средств массовой информации и памяток правоохранительных органов, но не думала, что это случится со мной.

Потерпевшая *Иванова*

(подпись)

К протоколу прилагаются: копия паспорта Ивановой Т.А. на 1 листе; справка о доходах Ивановой Т.А. за 6 месяцев на 1 листе.

Потерпевшая Иванова
(подпись)

Перед началом, в ходе либо по окончании допроса потерпевшего от *потерпевшей Т.А. Ивановой* заявления *не поступили.*

Потерпевшая Иванова
(подпись)

По окончании допроса протокол предъявлен для ознакомления *Т.А. Ивановой*, которой разъяснено её право делать подлежащие внесению в протокол оговоренные и удостоверенные её подписью замечания о его дополнении и уточнении.

Ознакомившись с протоколом путем *личного прочтения*, *Т.А. Иванова* замечания о его дополнении и уточнении *не сделала*.

Потерпевшая Иванова
(подпись)

Следователь Сидоров А.А. Сидоров

Приложение 2

М В Д Р о с с и и

Г Л А В Н О Е У П Р А В Л Е Н И Е
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО ЭНСКОЙ ОБЛАСТИ
(ГУ МВД России по Энской области)

пр-т Ленина, 80, Энск, 756000
_____ № _____
на №_____ от _____

ПАО «Сбербанк России»

Москва, 117997, ул. Вавилова, д. 19

В производстве СЧ СУ УМВД России по г. Энску находится уголовное дело № 12201010000000000, возбужденное 15.11.2022 по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ.

Расследованием уголовного дела установлено, что неизвестное лицо, используя мобильный телефон, путем обмана похитило денежные средства потерпевших. Похищенные денежные средства были зачислены на счет банковской карты № 4276 8090 1280 0000.

Наряду с вышеуказанным, на основании ч. 4 ст. 21 УПК РФ и ст. 26 Федерального закона от 02.12.1990 № 395-1-ФЗ «О банках и банковской деятельности», прошу Вас предоставить следующую информацию:

- установочные данные лица, на чье имя оформлена банковская карта № 4276 8090 1280 6876,
- о счете данной карты, дате и месте его открытия;
- выписку о движении денежных средств по счету (отчет по карте и дополнительный отчет по операциям перечисления);
- информацию об абонентском номере, к которому подключена услуга «Мобильный банк», где и каким образом он был подключен;
- информацию об IP-адресах, использованных для входа в онлайн-сервис по управлению данной банковской картой;
- по какой карте осуществляется вход в «Сбербанк Онлайн»;
- сведения из программы «Сбербанк Онлайн»: даты и IP-адреса входов в «Сбербанк Онлайн», способ подтверждения входа, дата и номер телефона регистрации мобильного приложения «Сбербанк Онлайн», наименование мобильного устройства.

Следователь *Иванов* И.И. Иванов

Руководитель СО *Сидоров* С.С. Сидоров

(подпись, гербовая печать)

Приложение 3

Согласен

Руководитель следственного органа –
начальник СО МО МВД России ***

подполковник юстиции
Фролов А.А. Фролов
«21» января 2022 г.

П О С Т А Н О В Л Е Н И Е
о возбуждении перед судом ходатайства
о разрешении получения информации о соединениях
между абонентами и (или) абонентскими устройствами

г. Барнаул 21 января 2022 г.

Следователь СО МО МВД России *** старший лейтенант юстиции В.В. Петров, рассмотрев материалы уголовного дела № 22010100**000017,

У С Т А Н О В И Л:

Уголовное дело № 22010100**000017 возбуждено 16.01.2022 СО МО МВД России *** по признакам преступления, предусмотренного ч. 2 ст. 159 УК РФ.

Расследованием уголовного дела установлено, что 14.01.2022 потерпевшей Воропаевой М.А. на абонентский номер 8-961-237-01-01 поступили телефонные звонки с абонентских номеров 8-495-201-55-50, 8-962-348-45-48 от неустановленной женщины, представившейся сотрудником банка, которая пояснила, что неизвестные пытаются совершить перевод денежных средств с банковской карты Воропаевой М.А., для предотвращения перевода необходимо сообщить реквизиты карты и пароли из поступивших СМС-сообщений. После того как Воропаева М.А. выполнила данные требования, со счета её банковской карты № **** **** **** ****, открытого в ПАО «Сбербанк России», были списаны денежные средства в сумме 15 250 рублей и перечислены на открытый АО «Банк “Открытие”» счет № 4890****5138.

Кроме того, согласно ответу АО «Банк “Открытие”» установлено, что часть похищенных денежных средств в период с 14.01.2022 по 20.01.2022 была переведена на лицевой счет абонентского номера 8-962-348-45-48.

Для установления лиц, совершивших преступление, а также свидетелей и очевидцев, в целях полного и объективного расследования, в настоящее время необходимо получить в ПАО «ВымпелКом» по адресу Алтайский край, г. Барнаул, ул. Мало-Тобольская, 18, за период с 01.01.2022 до момента исполнения постановления следующую информацию:

- о лице (Ф.И.О., дата рождения, место регистрации, паспортные данные), на которое зарегистрирован абонентский номер 8-962-348-45-48, с указанием даты активации, блокировки и IMEI абонентских устройств, в которых он использовался;

- о входящих, исходящих звонках и СМС-сообщениях, с предоставлением текстов СМС-сообщений, голосовой информации, изображений, звука, видео- и иных сообщений, хранение которых регламентировано ч. 1 ст. 64 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», абонентского номера 8-962-348-45-48 с указанием сведений о месте расположения базовых станций операторов сотовой связи, через возможности которых обеспечивалось соединение указанного абонента с другими абонентами, с указанием IMEI абонентских устройств, посредством которых осуществлялись соединения;

- о движении денежных средств по счету абонентского номера 8-962-348-45-48 с указанием даты, времени, суммы, посредника – посредством какой платежной системы осуществлялось поступление или перечисление денежных средств, IP-адреса;

- об услугах «Переадресация» и «Переход от оператора к другому оператору связи с сохранением абонентского номера», подключенных на абонентский номер 8-962-348-45-48.

На основании изложенного, руководствуясь ч. 2 ст. 29, п. 3 ч. 2 ст. 38, ст. 165, ч. 3 ст. 186^1 УПК РФ, ст. 63 ФЗ «О связи»,

П О С Т А Н О В И Л:

Ходатайствовать перед *** районным судом Алтайского края о разрешении получить в ПАО «ВымпелКом» по адресу Алтайский край, г. Барнаул, ул. Мало-Тобольская, 18, за период с 01.01.2022 до момента исполнения постановления следующую информацию:

- о лице (Ф.И.О., дата рождения, место регистрации, паспортные данные), на которое зарегистрирован абонентский номер 8-962-348-45-48, с указанием даты активации, блокировки и IMEI абонентских устройств, в которых он использовался;

- о входящих, исходящих звонках и СМС-сообщениях, с предоставлением текстов СМС-сообщений, голосовой информации, изображений, звука, видео- и иных сообщений, хранение которых регламентировано ч. 1 ст. 64 Федерального закона от 07.07.2003 № 126-ФЗ «О связи», абонентского номера 8-962-348-45-48 с указанием сведений о месте расположения базовых станций операторов сотовой связи, через возможности которых обеспечивалось соединение указанного абонента с другими абонентами, с указанием номеров приемо-передающих базовых станций, информации о зоне с неповторяющимися частотами, на которых излучает каждая базовая станция, азимутах и ширине направленности диаграммы антенны каждой базовой станции, IMEI абонентских устройств, посредством которых осуществлялись соединения;

- о движении денежных средств по счету абонентского номера 8-962-348-45-48 с указанием даты, времени, суммы, посредника – посредством какой платежной системы осуществлялось поступление или перечисление денежных средств, IP-адреса;

- об услугах «Переадресация» и «Переход от оператора к другому оператору связи с сохранением абонентского номера», подключенных на абонентский номер 8-962-348-45-48.

Следователь *Петров* В.В. Петров

Содержание

Учебное издание

Валюлин Руслан Рашитович
Козлов Вячеслав Викторович

РАССЛЕДОВАНИЕ ТЕЛЕФОННЫХ МОШЕННИЧЕСТВ

Учебное пособие

Редактор С.В. Калинина
Корректура,
компьютерная верстка М.В. Егерь

Лицензия ЛР № 0221352 от 14.07.1999 г.
Лицензия Плр № 020109 от 15.07.1999 г.

Подписано в печать 04.12.2023. Формат 60х84/16.
Ризография. Усл. п.л. 3,5. Тираж 40 экз. Заказ 465.
Барнаульский юридический институт МВД России.
Научно-исследовательский и редакционно-издательский отдел.
656038, Барнаул, ул. Чкалова, 49; бюи.мвд.рф.