ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
«ВСЕРОССИЙСКИЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

В. А. Рязанцев

ВОЗБУЖДЕНИЕ И РАССЛЕДОВАНИЕ УГОЛОВНЫХ ДЕЛ О ХИЩЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ, СЕТИ ИНТЕРНЕТ И СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

Практическое пособие

МОСКВА 2022

УДК 343.1

Рекомендовано к опубликованию
редакционно-издательским советом ФГКУ «ВНИИ МВД России»

Р е ц е н з е н т ы :
М. А. Стрекалов, кандидат юридических наук
(Следственный департамент МВД России);
Д. Н. Рудов, кандидат юридических наук, доцент
(Белгородский юридический институт МВД России имени И.Д. Путилина)

А в т о р :
В. А. Рязанцев, начальник 3 отдела НИЦ № 5,
кандидат юридических наук
(ФГКУ «ВНИИ МВД России»)

В. А. Рязанцев
Возбуждение и расследование уголовных дел о хищениях, совершенных с использованием банковских карт, сети Интернет и средств мобильной связи : практическое пособие / В. А. Рязанцев. – Москва : ФГКУ «ВНИИ МВД России», 2022. – 70 с.

В работе на основе анализа действующего законодательства, следственной практики раскрываются сущность, содержание и порядок рассмотрения сообщения о преступлении и производства предварительного следствия следователями органов внутренних дел Российской Федерации по уголовным делам о хищениях, совершенных с использованием банковских карт, сети Интернет и средств мобильной связи. Анализируются проблемы, возникающие при принятии решения о возбуждении уголовного дела. Исследуются особенности производства отдельных следственных и иных процессуальных действий, предусмотренных УПК РФ, аргументируется необходимость назначения и производства судебных экспертиз, которые отражают специфику рассматриваемой категории преступлений.

Для руководителей следственных органов, следователей органов внутренних дел, научных работников, преподавателей, аспирантов, адъюнктов и студентов юридических учебных заведений.

Практическое пособие подготовлено при информационной поддержке СПС КонсультантПлюс.

УДК 343.1

I. ОБЩИЕ ПОЛОЖЕНИЯ

Развитие информационно-коммуникационных технологий обусловило как процесс непрерывного роста их применения во всех сферах жизнедеятельности общества, так и открыло новые возможности для использования таких технологий в преступной деятельности, в том числе и в хищении денежных средств у граждан.

В последнее время все большее распространение получают хищения, совершаемые с использованием банковских карт, сети Интернет и средств мобильной связи.

Так, только в 2020 г. зарегистрировано 510 396 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в том числе 190 167 преступлений – с использованием расчетных (пластиковых) карт, 300 337 преступлений – сети Интернет, 218 739 преступлений – с использованием средств мобильной связи. При этом не раскрытыми осталось 379 830 преступлений[1].

В 2021 г. по сравнению с 2020 г. число зарегистрированных преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, выросло и составило 517 722 преступления, в том числе 165 658 преступлений – с использованием расчетных (пластиковых) карт, 351 463 преступления – сети Интернет, 217 552 преступления – с использованием средств мобильной связи. При этом по сравнению с 2020 г. количество не раскрытых преступлений в 2021 г. также увеличилось и составило 388 607 преступлений[2].

Анализ материалов, использованных при написании данной работы[3], свидетельствует об отсутствии у следователей необходимых знаний методики при проверке сообщений о таких преступлениях и их

[1] Состояние преступности в России за январь – декабрь 2020 г. ФКУ «ГИАЦ МВД России».

[2] Состояние преступности в России за январь – декабрь 2021 г. ФКУ «ГИАЦ МВД России».

[3] При подготовке работы были использованы: методические рекомендации «Особенности квалификации мошеннических действий по статьям 159.1–159.3, 159.5, 159.6 УК РФ и отграничение от деяний, подлежащих квалификации по статье 159 УК РФ», лекция «Расследование мошеннических действий, совершенных с использованием платежных карт», подготовленные авторскими коллективами ФГКУ «ВНИИ МВД России»; «Практическое пособие следователя по расследованию уголовных дел о хищениях, совершенных дистанционным способом, со сборником типовых запросов, направляемых при расследовании уголовных дел указанной категории», подготовленное Главным следственным управлением Главного управления МВД России по Кемеровской области; методические рекомендации по организации первоначальных оперативно-розыскных мероприятий при проведении доследственных проверок по фактам дистанционных мошенничеств, подготовленные Управлением МВД России по Ярославской области.

последующем расследовании, ложном стойком предубеждении о невозможности или крайней сложности раскрытия таких видов хищений, непонимании способов их совершения.

Вместе с тем с технической стороны процесс раскрытия данных преступлений каких-либо особых сложностей не представляет. При этом важное значение имеет деятельность следователя, как на стадии предварительного расследования, так и при рассмотрении сообщений о таких хищениях.

Представляется, что изложенная в данной работе методика расследования преступлений указанной направленности наиболее полным образом будет способствовать их раскрытию.

II. РАССМОТРЕНИЕ СЛЕДОВАТЕЛЕМ СООБЩЕНИЙ О ХИЩЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ, СЕТИ ИНТЕРНЕТ И СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

Статья 144 УПК РФ обязывает дознавателя, орган дознания, следователя и руководителя следственного органа принять, проверить сообщение о любом совершенном или готовящемся преступлении и, в пределах компетенции, принять по нему решение.

Проверка сообщения о преступлении осуществляется в срок до 3 суток, который может быть продлен руководителем следственного органа по мотивированному ходатайству следователя до 10 суток. Срок предварительной проверки сообщения в некоторых случаях может быть продлен руководителем следственного органа по мотивированному ходатайству следователя до 30 суток. Основаниями для этого является производство судебных экспертиз, исследований документов, предметов, а также проведение оперативно-розыскных мероприятий.

Следственные и иные процессуальные действия, которые могут проводиться в ходе предварительной проверки сообщения о преступлении, перечислены в ч. 1 ст. 144 УПК РФ. Применительно к проверке сообщения о рассматриваемых хищениях следователем могут быть получены объяснения от заявителя, очевидцев преступления, иных лиц, располагающих какой-либо информацией, имеющей значение для раскрытия преступления; истребованы документы и предметы; произведен осмотр места происшествия, изъятых или истребованных предметов и документов; назначена судебная экспертиза; дано письменное поручение органу дознания о проведении оперативно-розыскных мероприятий, а также проведены иные действия, предусмотренные ч. 1 ст. 144 УПК РФ.

Получение письменного объяснения от заявителя при проверке факта хищения, совершенного посредством телефонного звонка.

Наиболее распространенный способ совершения такого хищения заключается в сообщении заявителю посредством телефонного звонка (на стационарный или мобильный телефон) от лица родственника или знакомого (голос звонящего взволнованный, часто очень похож на известный заявителю) о том, что он задержан сотрудниками полиции за совершение того или иного преступления или правонарушения (ДТП,

хранение оружия или наркотиков, причинение вреда здоровью), но есть возможность за определенное вознаграждение «решить вопрос». Далее в разговор вступает другое лицо, которое представляется сотрудником правоохранительных органов и сообщает: какую сумму необходимо перечислить, каким образом и куда. Денежные средства могут быть переданы заявителем курьеру (таксисту), перечислены безадресным переводом, на банковский счет (электронный кошелек) или на лицевой счет абонентского номера телефона.

В ходе получения объяснения необходимо выяснить следующие обстоятельства:

дата, время поступления звонка с соответствующим содержанием;

абонентский номер заявителя, на который был осуществлен звонок (стационарный, мобильный телефон);

если звонок поступил на сотовый телефон или стационарный телефон с автоматическим определением номера, с какого номера телефона осуществлен звонок;

дословное содержание разговора, кем представился звонивший, о чем говорил, что предлагал сделать;

описание голоса звонившего (дефекты речи – хрипота, картавость, шепелявость, заикание), какова была интонация голоса, разговаривал ли он шепотом или обычным тембром; какие особенности, странности в интонации, произношении звуков, в обращении заметил заявитель, использование в разговоре специальных терминов, специфических речевых оборотов; по каким приметам заявитель сможет опознать голос звонившего;

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

что именно (по возможности дословно) сам заявитель сообщил неизвестному, представившемуся родственником, а также лицу, представившемуся сотрудником полиции;

как неизвестный узнал точный адрес места жительства заявителя: последний сам назвал его, либо неизвестный, представившийся сотрудником полиции, уже знал его место жительства;

как долго по времени длился телефонный разговор с неизвестным (сверить в последующем с данными детализации телефонных переговоров);

через какой период времени после окончания разговора подъехал звонивший неизвестный к дому заявителя;

описание голоса неизвестного лица (курьера, таксиста), какие особенности, странности в интонации, произношении звуков, в обращении к нему он заметил; по каким приметам заявитель сможет опознать его голос;

подробное описание его черт лица, рук, особенностей телосложения, походки, поведения, по которым заявитель сможет его опознать (составить композиционный портрет личности), одежды;

если передача денег осуществлялась в жилище заявителя, установить: когда неизвестный курьер (таксист) зашел в квартиру, то до каких предметов мебели, иных предметов дотрагивался, как себя вел, что сообщил, задавал ли какие-либо вопросы, задавал ли заявитель ему какие-либо вопросы, интересовался ли судьбой своего родственника, например, путем постановки вопроса, когда родственника «освободят» от уголовной ответственности и пр.;

сообщал ли заявитель 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;

пересчитывал ли заявитель, неизвестное лицо на месте передачи деньги;

как заявитель упаковал деньги;

звонил ли неизвестный в момент получения денег кому либо, что говорил;

провожал ли заявитель неизвестного, наблюдал ли за направлением, в котором неизвестный покинул место расположения его дома, передвигался ли неизвестный на автомобиле (какой модели);

какую сумму денег он хранит дома;

как часто его посещает родственник, якобы, «попавший в беду», как может охарактеризовать его, характер их взаимоотношений, чем родственник занимается, каков источник дохода родственника, есть ли среди круга общения родственника лица, ранее привлекавшиеся к уголовной ответственности, отбывавшие наказание, в частности, в местах лишения свободы;

кто из посторонних лиц посещает или посещал в последнее время заявителя (социальный работник, медицинский работник, представитель организации по вопросам пенсионного обеспечения и пр.), его полные анкетные данные, контактные номера телефонов, как может охарактеризовать его, когда последний раз тот посещал заявителя,

знаком ли социальный работник (медицинский работник) с его родственником, якобы «попавшем в беду», знает ли социальный работник, где проживает родственник, якобы «попавший в беду», как часто навещает заявителя.

При осуществлении безадресного перевода, необходимо выяснить, на чье имя переводились деньги, полные установочные данные получателя, истребовать у заявителя квитанцию о переводе. Если перевод был осуществлен на лицевой счет абонентского номера или счет банковской карты необходимо выяснить:

абонентский номер телефона или номер банковской карты, с которой переведены денежные средства (дата получения, срок действия, вид платежной системы, банк-эмитент карты, наличие договора банковского счета и документов об оформлении банковской карты), истребовать данные документы, чек или квитанцию о переводе;

абонентский номер телефона или номер банковской карты, на которую переведены денежные средства;

размер суммы перевода денежных средств;

предпринятые заявителем действия после обнаружения факта хищения;

является ли ущерб значительным для заявителя, если да, то обязательно отразить обстоятельства, подтверждающие это, каков состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

Получение письменного объяснения от заявителя при проверке факта хищения, совершенного с использованием информационно-телекоммуникационной сети Интернет.

В ходе получения объяснения необходимо установить:

дату и время обнаружения объявления (получения ссылки на соответствующий интернет-ресурс), если возможно – найти объявление в интернете и зафиксировать его адрес (еще раз пройти по интернет-ссылке), сделать снимок экрана, приобщить его к материалам проводимой проверки;

с использованием какого технического устройства заявитель 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;

сохранились ли у него данные объявления (№ объявления, ID-страницы);

каким образом, когда (дата, время) заявитель связался с «продавцом»;

как «продавец» представился;

где, со слов «продавца», он находился;

известно ли ему место нахождения товара;

отразить подробное содержание разговора с продавцом;

что именно сообщил «продавец» о продаваемом товаре, об условиях оплаты товара, условиях, сроках и способах доставки покупателю товара;

описание голоса «продавца», сможет или нет его опознать (по каким приметам);

когда (дата, период времени), каким образом (через банкомат, посредством услуги «Сбербанк Онлайн», «Мобильный банк»), в каком размере заявитель перечислил на какой счет (№ счета, либо банковской карты, открытые на чье имя) денежные средства в счет оплаты за якобы приобретаемый товар;

если заявитель осуществил перевод денежных средств со своей банковской карты на банковскую карту неизвестного посредством услуги «Сбербанк Онлайн», через «Личный кабинет», установить место входа потерпевшего в сеть Интернет (с какого компьютера, ноутбука, планшета, с использованием какого модема, wi-fi-роутера, их MAC-адреса, логины и пароли, какая компания-провайдер предоставляла в этот день заявителю услуги доступа в интернет);

дата и место открытия счета (банковской карты), с которой заявитель перечислил денежные средства;

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

что именно ему сообщил после подтверждения оплаты (перечисления денег на банковскую карту) «продавец»;

в какой период времени, куда прибыл для получения (как ему казалось) приобретенного товара;

когда он осознал, что в отношении него было совершено преступление, в результате которого похищены принадлежащие ему денежные средства;

предпринятые заявителем действия после обнаружения факта хищения;

является ли ущерб значительным для заявителя, если да, то обязательно отразить обстоятельства, подтверждающие это, каков состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

Получение письменного объяснения от заявителя при проверке факта хищения, совершенного с использованием вредоносного программного обеспечения.

В ходе опроса необходимо выяснить:

время, место и обстоятельства хищения денежных средств;

реквизиты банковской карты, с которой совершено хищение денежных средств, а также подключенной услуги «Мобильный банк» с указанием номеров телефонов, к которым она привязана;

если услуга подключена самим заявителем, то с какого времени и каким способом (посредством заявления о подключении в офисах банковских учреждений или посредством банкоматов);

с какого времени заявитель пользуется абонентским номером, к которому данная услуга подключена, т.к. не исключается перевыпуск номера оператором связи после истечения 6 месяцев неиспользования абонентского номера с оформлением номера на иное лицо;

модель телефона, подключенного к услуге «Мобильный банк», используемая операционная система в телефоне («Андроид», «IOS» (Apple) или иное);

наличие установленных антивирусных программ на мобильном устройстве;

какие мобильные приложения устанавливались в последнее время, способ установки (из официальных источников (сайтов) «AppStore» (Apple), «PlayMarket» (GooglePlay), с сайта банка-имитента банковской карты (банковского продукта, в случае, например, открытия банковского счета без выпуска банковской карты);

совершались ли операции через мобильное устройство (телефон, планшет) или компьютер, вводились ли иным способом данные карты или хранились сведения о ней в устройствах;

осуществлялся ли с данного устройства доступ в сеть Интернет, в том числе автоматически (например, при установке графика автоматического обновления приложений, то каких именно приложений и пр.);

осуществлял ли кто-либо с использованием данных банковской карты (номера, срока действия, данных владельца, CVC/CVV2-кода (три цифры, расположенные на обратной стороне банковской карты)) заявителя покупку товаров, заказ услуг через интернет;

поступали ли на мобильное устройство сообщения, содержащие ссылки на интернет-ресурсы, если да, то когда, от кого, содержание сообщений, осуществлялся ли переход по данным ссылкам, если да, то каков результат (было установлено приложение, установка приложения неожиданно прервалась, мобильное устройство «зависло», потребовалась перезагрузка, приложение «попросило» ввести определенные данные и пр.);

наблюдались ли какие-либо изменения в работе устройства, отличимые от повседневной, перед хищением денежных средств и в последующем, в чем они заключались, после каких действий (изменений в устройстве) проявились, как долго наблюдались и что с ними на момент проведения опроса;

ремонтировалось ли устройство до или после обнаружения факта хищения, где, кем;

поступали ли сообщения о снятии денежных средств, их содержание, номер с которого они были отправлены;

местонахождение мобильного телефона в настоящее время, а также желает ли заявитель добровольно предоставить его для производства компьютерной экспертизы с указанием необходимых паролей;

обращался ли заявитель в банк, имеются ли у него выписки о движении денежных средств по карте, ответы по обращениям (в случае наличия таковых приобщить их к материалам проводимой проверки);

является ли ущерб значительным для заявителя, если да, то обязательно отразить обстоятельства, подтверждающие это, каков состав семьи, близких родственников, лиц, находящихся на иждивении, размер доходов и расходов заявителя по состоянию на момент совершения в отношении него преступления.

Получение письменного объяснения от заявителя при проверке факта хищения, совершенного путем использования похищенной или поддельной кредитной либо расчетной карты.

В ходе получения объяснения от заявителя (держателя платежной карты) устанавливается:

кто имел доступ к карте или знал ПИН-код;

какими кредитными, торговыми, сервисными или иными организациями, банкоматами пользовался, какие расчетно-платежные операции проводил, кто при этом присутствовал;

производил ли оплату товаров, работ, услуг через сеть Интернет, какими сайтами пользовался;

получал ли СМС-сообщения о предоставлении продуктов и услуг банка с предложением нажать определенные клавиши на телефоне для подтверждения согласия в их приобретении, или СМС-сообщения о блокировке карты с номером телефона, по которому необходимо перезвонить, какие сведения в таких ситуациях он передавал, сообщал ли персональные данные платежных карт, какие именно;

имело ли место поступление на электронную почту сообщений от кредитных организаций, их содержание, перечень сведений, переданных им по просьбе банков;

время последнего использования карты, месторасположение сервисного предприятия или банкомата, где карта применялась в последний раз, перечень полученных услуг или приобретенных товаров (предметов);

обстоятельства утраты или похищения карты, если это имело место (или производится изъятие платежной карты и ее осмотр, если карта находится у потерпевшего);

иные сведения.

Объяснения также должны быть получены от свидетелей – очевидцев преступления, родственников заявителя, иных свидетелей, которые располагают какой-либо информацией, имеющей значение для раскрытия преступления. При необходимости следует направить их на составление композиционного портрета подозреваемого лица, предъявление фотокартотеки лиц, ранее судимых и состоящих на учете в органах внутренних дел. Объяснения могут быть получены и от лиц, обслуживающих платежные терминалы, работников банков о механизмах перевода денежных средств и др.

Истребование документов и предметов, в том числе получение справок от учреждений и организаций по запросу следователя.

В целях сокращения времени проведения проверки следователю необходимо истребовать у заявителя справки, выписки, чеки, договор на банковское обслуживание карты, со счета которого произошло списание денег или иных документов, подтверждающих факт перевода денежных средств на другие банковские карты (счета) или лицевой счет абонентского номера. Такие сведения держатель банковской карты может получить самостоятельно в кратчайшие сроки, возможно через личный кабинет или через определенный сервис, предоставляемый мобильным приложением. После возбуждения уголовного дела с согласия руководителя следственного органа следователю необходимо запросить полные сведения об осуществленном переводе по коду транзакции. Либо, получив судебное решение, следователь производит выемку документов, содержащих информацию о счетах граждан в банках и иных кредитных организациях.

В связи с этим дальнейшие действия следователя могут быть представлены в следующем порядке:

необходимо истребовать и получить от заявителя чеки, подтверждающие факт перевода денежных средств на другие банковские карты (счета) или лицевой счет абонентского номера, приобщить их к материалам проводимой проверки;

инициировать процедуру получения заявителем информации от кредитной организации о движении денежных средств по его банковской карте (счету), приобщить их к материалам проводимой проверки;

рекомендовать заявителю обратиться к оператору связи с предоставлением детализации соединений его абонентского номера телефона, приобщить данную выписку к материалам проводимой проверки;

с помощью сайта Федерального агентства связи «Россвязь» по ссылке: www.rossvyaz.ru/activity/num_resurs/registerNum/ или www.kody.su на вкладке «Коды сотовых операторов» и иных сайтах определить принадлежность оператору и региону абонентских номеров, использовавшихся при совершении преступления.

Для установления анкетных данных владельца абонентского номера, который использовался при совершении преступления, следователем[4] еще до возбуждения уголовного дела может быть направлен

[4] До возбуждения уголовного дела такой запрос направляется следователем соответствующему оператору связи на основании ч. 4 ст. 21, подп. 3 и 6 ч. 2 ст. 38 УПК РФ, ч. 5 ст. 64 Федер. закона от 7 июля 2003 г. № 126-ФЗ «О связи».

запрос соответствующему оператору связи о предоставлении необходимых сведений:

об абоненте, на которого зарегистрирован номер телефона, с указанием паспортных данных, даты активации SIM-карты и ее состоянии в текущий момент;

о точке продажи SIM-карты с интересующим абонентским номером, с указанием адреса и контактных данных организации;

о месте хранения оригинала договора об оказании услуг связи, заключенного при регистрации интересующего абонентского номера, с указанием адреса и контактных данных.

Запросы необходимо направлять операторам сотовой связи, обслуживающим именно тот регион, где зарегистрирована SIM-карта с интересующим следствие абонентским номером, кроме ПАО «ВымпелКом», так как данный оператор имеет единую базу данных по всей территории Российской Федерации.

Следует отметить, что информация о соединениях между абонентами и абонентскими устройствами, движении денежных средств по счету SIM-карты, IMEI номере устройства, в котором использовались SIM-карты с интересующими следствие абонентскими номерами, следователем может быть получена в установленном ст. 165 и 186.1 УПК РФ порядке только после возбуждения уголовного дела.

В соответствии с ч. 4 ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 (ред. от 30 декабря 2021 г.) «О банках и банковской деятельности»[5] справки по счетам и вкладам физических лиц могут быть выданы кредитной организацией без судебного решения по согласованным с руководителем следственного органа запросам следователя только по уголовным делам, находящимся в его производстве, но не при проведении проверки сообщения о преступлении.

Такой же порядок определен и при необходимости получения информации о движении денежных средств по лицевому счету абонентского номера, банковскому счету, посредством определенной платежной системы, о пользователях, совершивших соответствующие операции. Так, согласно ст. 26 Федерального закона от 27 июня 2011 г. № 161-ФЗ (ред. от 2 июля 2021 г.) «О национальной платежной системе»[6] операторы по переводу денежных средств, операторы платежных систем, операторы услуг платежной инфраструктуры и

[5] Собр. законодательства Рос. Федерации. 1996. № 6, ст. 492 // СПС КонсультантПлюс.

[6] Собр. законодательства Рос. Федерации. 2011. № 27, ст. 3872 // СПС КонсультантПлюс.

банковские платежные агенты (субагенты) обязаны гарантировать банковскую тайну в соответствии с законодательством Российской Федерации о банках и банковской деятельности[7].

Поэтому в случае необходимости получения вышеуказанных сведений от операторов сотовой связи, кредитной организации или администрации платежной системы при проверке сообщения о преступлении следователю следует использовать полномочия оперативных подразделений органов внутренних дел, предоставленные последним в соответствии с Федеральным законом от 12 августа 1995 г. № 144-ФЗ (ред. от 30 декабря 2021 г.) «Об оперативно-розыскной деятельности»[8] и Федеральным законом от 7 июля 2003 г. № 126-ФЗ (ред. от 30 декабря 2021 г.) «О связи»[9].

До возбуждения уголовного дела, а также в ходе предварительного следствия, следователь может направить запрос в организацию, обслуживающую интернет-ресурс, на котором лицом, подозреваемым в совершении преступления, размещено объявление о продаже товара (предоставлении услуг и пр.), с целью получения следующей информации:

о дате и времени регистрации, контактных данных при регистрации, а также после редактирования (если такое было) профиля пользователя, разместившего объявление;

о дате и времени внесения изменений в профиль пользователя;

точном наименовании интернет-ресурса;

полном содержании объявления, стоимости товара (услуги), указанном абонентском номере телефона;

---

[7] В соответствии со ст. 3 Федерального закона от 27 июня 2011 г. № 161-ФЗ (ред. от 2 июля 2021 г.) «О национальной платежной системе»: оператор по переводу денежных средств – организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств (п. 2); оператор платежной системы – организация, определяющая правила платежной системы, а также выполняющая иные обязанности, предусмотренные настоящим Федеральным законом (п. 6); оператор услуг платежной инфраструктуры – операционный центр, платежный клиринговый центр и расчетный центр (п. 7); банковский платежный агент – юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются кредитной организацией в целях осуществления отдельных банковских операций (п. 4); банковский платежный субагент – это юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые привлекаются банковским платежным агентом в целях осуществления отдельных банковских операций (п. 5).

[8] Собр. законодательства Рос. Федерации. 1995. № 33, ст. 3349 // СПС КонсультантПлюс.

[9] Собр. законодательства Рос. Федерации. 2003. № 28, ст. 2895 // СПС КонсультантПлюс.

об IP-адресе (адресах), с которого осуществлялся вход в учетную запись пользователем, разместившем объявление (внесшим изменения в профиль пользователя);

об IP-адресах пользователей, которые с момента регистрации данного объявления просматривали его;

об объявлениях, размещенных на сайте, в контактных данных пользователя которых указан такой же абонентский номер телефона (иные регистрационные данные) лица, разместившего интересующее объявление.

После получения от организации, обслуживающей интернет-ресурс, информации об IP-адресах следователю необходимо направить запросы провайдерам, которыми были присвоены такие IP-адреса для предоставления данных клиента, которому присвоен IP-адрес, адреса местонахождения оконечного оборудования (точки доступа в сеть Интернет) с приложением заверенной копии договора об оказании услуг связи.

При необходимости получения информации о владельце электронной почты следует учитывать, что сведения о регистрации и администрировании почтовых ящиков @gmail.com (@google.com), @hotmail.com, @yahoo.com (и прочие) находятся на оборудовании организаций, осуществляющих свою деятельность за пределами Российской Федерации. Получить вышеуказанные сведения возможно посредством направления запроса по линии НЦБ Интерпола[10] либо запроса о правовой помощи в соответствии со статьями 453 и 454 УПК РФ после возбуждения уголовного дела.

В случае поступления от оператора сотовой связи (организации, обслуживающей интернет-ресурс) информации об абонентах, достоверность паспортных данных которых вызывает сомнение, необходимо направить запрос в соответствующее территориальное подразделение Управления по вопросам миграции МВД России по субъекту РФ с целью проверки этих данных.

Рекомендуется получать данную информацию от исполнителей запросов сначала посредством электронной почты для организации

[10] Порядок направления запросов, сообщений, следственных поручений и ответов по линии Интерпола определен Инструкцией по организации информационного обеспечения сотрудничества по линии Интерпола, утвержденной приказом МВД РФ № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 от 6 окт. 2006 г. (ред. от 22 сент. 2009 г.) «Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола» // Бюллетень нормативных актов федеральных органов исполнительной власти. 2006. № 47; СПС КонсультантПлюс.

своевременного проведения необходимых процессуальных и следственных действий, а затем – оригинал получать почтой или иным способом.

При личном контакте заявителя с лицом, подозреваемым в совершении преступления, следователю необходимо направить ориентировки в территориальные подразделения органов внутренних дел с приметами последнего и в МРЭО ГИБДД, если имеются сведения о приметах и государственном регистрационном знаке автомобиля, на котором скрылось данное лицо.

При совершении операций по банковской карте через устройство самообслуживания (банкомат), следователю необходимо направить запрос в соответствующую организацию с просьбой осуществить архивацию видеозаписи с камер наблюдения, которую при проведении проверки сообщения о преступлении можно изъять в ходе осмотра места происшествия или после возбуждения уголовного дела в порядке, установленном ст. 183 УПК РФ.

Следователю следует незамедлительно принимать меры к сохранению и последующему изъятию видеозаписей с камер наружного видеонаблюдения в случае установления факта фиксации события преступления, пути следования предполагаемого преступника и его внешности.

Осмотр места происшествия (ст. 176 УПК РФ). При проверке заявления (сообщения) о преступлении осмотр места происшествия может проводиться до возбуждения уголовного дела. Это неотложное следственное действие, которое должно быть проведено незамедлительно после поступления сообщения о преступлении. Осмотр места происшествия проводится, если могут быть обнаружены следы преступления, выяснена обстановка происшествия и иные обстоятельства, имеющие значение для уголовного дела.

На момент получения сообщения о преступлении, как правило, может быть известно:

место нахождения заявителя в момент преступления;

место передачи денежных средств;

место перевода (зачисления и т.п.) денежных средств.

Если способ совершения преступления заключался в размещении на соответствующем интернет-ресурсе информации о продаже товаров (оказании услуг) без намерения выполнять свои обязательства, а заявитель просмотрел такое объявление с помощью компьютера, расположенного в занимаемом им жилом помещении, следует произве-

сти осмотр места происшествия: жилища заявителя с его согласия, в котором располагаются компьютерные устройства или их системы (компьютер, ноутбук, планшет, wi-fi-роутер, модем и пр.), подключенные к сетям телекоммуникационной связи и содержащие компьютерную информацию.

Осмотр места происшествия производится с целью фиксации обстановки, обнаружения и изъятия следов в виде электронной информации, предметов – носителей такой информации, иных предметов и документов, которые могут иметь значение для раскрытия и расследования преступления.

В протоколе осмотра места происшествия следует отразить:

расположение компьютера (стационарный компьютер, переносной ноутбук, планшетный компьютер, смартфон), устройств телекоммуникации (wi-fi-роутера, модема), порядок их соединения (сопряжения, связи) между собой (беспроводная связь, организованная компьютерная сеть);

назначение каждого устройства, его название, серийный номер, комплектацию (сетевые карты, соответствующие разъемы, наличие дисковода и др.), наличие соединения с сетями телекоммуникации, функциональное состояние устройств на момент осмотра;

содержание информации, отображаемой на мониторе.

В случае, если интернет-ресурс, с использованием которого совершены противоправные действия, продолжает функционировать на момент осмотра места происшествия (не удален, не заблокирован и т.п.), необходимо в протоколе указать представленную на сайте контактную информацию, род деятельности ресурса, наличие отзывов, приложить распечатки с интернет-сайта, экранную копию (снимок экрана) ресурса сети Интернет, на которой должны быть видны реквизиты – адресная строка страницы, идентификатор страницы и т.д.

В ходе осмотра места происшествия могут быть изъяты системные блоки персональных компьютеров или установленные в них накопители на жестких магнитных дисках, иные электронные носители информации, а также устройства телекоммуникации.

В рамках осмотра места происшествия следователем *с письменного согласия заявителя* может быть произведен осмотр его мобильного телефона с целью отыскания и закрепления следующей информации:

IMEI телефонного аппарата заявителя;

наличия SIM-карт с абонентскими номерами заявителя;

информации, содержащейся в журнале вызовов мобильного устройства, в банке СМС-сообщений, в записной книжке (или «контактах») внутренней памяти мобильного устройства или SIM-карты;

в виде сохраненных текстов переписки между соответствующими абонентскими устройствами посредством СМС-сообщений или других мессенджеров, например «WhatsApp», «Viber»;

об истории посещения интернет-сайтов;

о поиске через установленный на устройстве браузер в интернете сведений, имеющих отношение к исследуемому событию;

об использовании соответствующих интернет-сервисов, позволяющих осуществлять виртуальный оборот денежных средств (различные электронные кошельки);

о регистрации в качестве пользователя в социальной сети, на личной странице которого могут содержаться данные, представляющие интерес для расследования (социальные сети «Вконтакте», «Одноклассники» и пр.);

в виде сохраненных логинов и паролей (например, некоторые установленные на мобильное средство связи утилиты (программы) позволяют сохранять информацию о логинах и паролях всех, когда-либо посещенных сайтов);

о типе программного обеспечения мобильного устройства заявителя, наличия в нем собственной антивирусной программы и ее активности.

Такой осмотр целесообразно проводить с участием специалиста.

В рамках осмотра необходимо детально исследовать соответствующие разделы приложения «Мобильный банк» («История платежей», «Последние операции» и пр.), в которых зафиксировано движение денежных средств по счету (банковской карте), сделать снимки экрана мобильного устройства, запечатлевающие данную информацию с помощью самого устройства (если позволяет его аппаратно-программное обеспечение), либо сфотографировать экран любым устройством, позволяющим получить фотографическое изображение. Обнаружению и закреплению (фотографированию) также подлежит информация, находящаяся в памяти мобильного устройства, отражающая переписку с подозреваемым лицом, с помощью СМС-сообщений, переписки в Viber, WatsApp и пр., сохраненные страницы в мобильном браузере из социальных сетей, электронных торговых площадок (и их мобильных приложений) и пр.

Информация, полученная в ходе осмотра мобильного устройства, подлежит занесению в протокол, а фотоматериалы необходимо приобщить фототаблицей.

При хищениях денежных средств, совершенных при помощи вредоносного программного обеспечения (ВПО), жертвами такого рода преступлений становятся владельцы мобильных устройств на базе платформы Android. Вирус позволяет удаленно управлять отправкой СМС-сообщений с телефона и перехватывать ответные сообщения, не уведомляя владельца телефона. Пропажа денежных средств обнаруживается заявителем при проверке баланса карты или проведении операций по обналичиванию. По этой причине осмотр самого телефона на предмет сохраненных сообщений не дает результата.

Признаками противоправного деяния при наличии в мобильном устройстве ВПО будут служить СМС-сообщения, направляемые на сервисные номера банка с абонентского номера заявителя, которые будут видны только при получении детализации соединений его абонентского номера.

Осмотр мобильного телефонного аппарата заявителя может быть произведен и в качестве самостоятельного следственного действия – осмотр предметов, если для этого требуется, например, длительное время, применение специальных знаний и технических средств. В этом случае в ходе осмотра места происшествия возможно изъятие мобильного телефона и его содержимого.

При осмотре жилого помещения заявителя, возможно изъятие полученных им самостоятельно документов и сведений, относящихся к событию хищения: детализации входящих и исходящих соединений абонентского номера, по которому заявитель общался с подозреваемым лицом, с целью установления абонентского номера последнего; выписки движения денежных средств по банковской карте (счету), с которого были переведены денежные средства; договор банковского счета (банковского обслуживания) и документов об оформлении банковской карты (заявления на открытие банковского счета и предоставление банковской расчетной карты) и др.

При получении сообщения о преступлении необходимо провести осмотр места передачи (наличных денежных средств), перевода, а при установлении – места зачисления денежных средств. При этом, денежные средства заявителем могут быть зачислены на указанный ему номер телефона (лицевой счет абонентского номера), на счет электронного кошелька, на банковский счет (карту).

Для перевода денежных средств, как на лицевой счет абонентского номера телефона, так и на счет электронного кошелька заявителем может быть использован платежный терминал самообслуживания или банкомат, с помощью последнего возможно снятие заявителем наличных денежных средств, с последующей их передачей непосредственно подозреваемому либо его доверенному лицу.

В ходе осмотра места происшествия следует произвести осмотр помещения, в котором установлены данные устройства, с отражением в протоколе наличия или отсутствия камер наружного наблюдения, видеозаписи, дополнительно подтверждающих факт перевода (снятия) заявителем денежных средств, или содержащих иную информацию о событии преступления – лицах, подозреваемых в его совершении, их соучастниках, свидетелях, об автотранспорте, находящемся около банкомата в момент совершения преступления. При наличии видеозаписи с камер наружного наблюдения следователю необходимо в ходе осмотра места происшествия провести ее изъятие.

При осмотре банкомата или платежного терминала следует обратить внимание на наличие на его корпусе идентификационного номера, который в дальнейшем может быть использован следователем для направления запроса администратору платежной системы или оператору сотовой связи с целью получения подтверждающей информации о факте перевода (зачисления) денежных средств.

В случае необходимости к осмотру следует привлекать соответствующих специалистов, в том числе поставщика данной техники или специалиста центра технического обслуживания.

При передаче денежных средств непосредственно подозреваемому либо его доверенному лицу необходимо произвести осмотр не только места передачи, но и прилегающей территории с целью установления наличия и изучения записи видеокамер (видеодомофонов) в месте совершения преступления (расположенных на зданиях учреждений, организаций различных форм собственности), а также частных лиц.

В ходе осмотра места происшествия следователю необходимо составить план-схему: путей отхода лица, которому были переданы денежные средства, либо движение автомобиля, если денежные средства были переданы водителю (таксисту); возможных путей отхода лица, в случае если они не известны; ближайших мест расположения камер уличного видеонаблюдения.

Местом передачи денежных средств может быть квартира заявителя или лестничная площадка подъезда, в котором он проживает,

двор его дома и т.д. В этом случае осмотр места происшествия проводится следователем с участием специалиста для обнаружения:

следов пальцев рук, ладоней (например, на ручке входной двери квартиры заявителя);

следов обуви (в квартире, на лестничной площадке либо во дворе дома);

брошенных окурков;

следов протекторов шин автомобиля, на котором передвигался подозреваемый либо его доверенное лицо.

В ходе осмотра следователь является руководителем дежурной следственно-оперативной группы (СОГ), определяет порядок ее работы, обеспечивает ее согласованную деятельность, при необходимости дает указания обязательные для исполнения участникам СОГ. В зависимости от обстоятельств совершенного преступления решает вопрос о привлечении к осмотру необходимых (дополнительных) специалистов.

Прибыв на место происшествия в составе СОГ, следователь получает первичную информацию от прибывших первыми на место происшествия сотрудников органов внутренних дел, устанавливает, какие изменения внесены в обстановку места происшествия; определяет границы осмотра и порядок проведения. Получив общую исходную информацию, следователь определяет направление работы каждого участника группы, инструктирует их, формулируя конкретные задачи.

До начала работы на месте происшествия сотрудника экспертно-криминалистического подразделения в качестве специалиста, следователь принимает меры к недопущению совершения действий, влекущих нарушение или изменение целостности обстановки совершения преступления. Кроме того, он разъясняет всем участникам осмотра их права и обязанности. Особенно это важно делать в отношении понятых, которые могут быть допрошены в суде, об обстоятельствах их участия в следственном действии.

При осмотре места происшествия следователь несет персональную ответственность за качество, полноту и результативность осмотра, применение криминалистических средств и методов, изъятие, упаковку и сохранность изъятых следов преступления, сравнительных образцов и иных предметов, их доставку для проведения лабораторных исследований, а также за достоверность отражения сведений об осмотре места происшествия в протоколе.

По окончании осмотра места происшествия следователь собирает воедино все данные осмотра места происшествия, анализирует их и в соответствии с полученными результатами решает вопрос о дальнейшем направлении работы. Действуя быстро и оперативно, исходя из анализа обнаруженных следов преступления и других доказательств, имеющихся на момент осмотра, поступающей оперативной информации, следователь определяет обстоятельства, при которых было совершено преступление, решает вопрос о возбуждении уголовного дела. В зависимости от результатов осмотра места происшествия и оперативных данных принимает меры к установлению и задержанию лица, подозреваемого в совершении преступления.

Осмотр изъятых или истребованных предметов и документов, если впоследствии они могут быть признаны вещественными доказательствами по делу (ст. 81 УПК РФ).

При проверке сообщения (заявления) о преступлении следователем в соответствии с ч. 1 ст. 144 УПК РФ могут быть осмотрены все обнаруженные и изъятые при производстве осмотра места происшествия или истребованные предметы и документы.

Осмотр компьютерных устройств, электронных носителей информации, мобильных телефонных аппаратов и их содержимого, видеозаписей, документов и др. может являться составной частью осмотра места происшествия. Как самостоятельное же следственное действие он производится в тех случаях, когда в ходе осмотра места происшествия обнаруженные и изъятые предметы и документы, имеющие значение для дела, не были сразу осмотрены, или когда возникает необходимость в повторном их осмотре, требуется длительное время для более детального изучения, применение специальных знаний и технических средств.

В случае, когда хищение денежных средств осуществлялось путем неправомерного вмешательства в функционирование компьютерных устройств или информационно-телекоммуникационных сетей, обязательным условием при принятии решения о возбуждении уголовного дела является установление способа совершения данного преступления. Для чего необходимо располагать *заключением эксперта* (судебной компьютерной экспертизы)[11].

Выполнение поручений следователя. Следователь в ходе предварительной проверки вправе давать органу дознания обязательное для исполнения письменное поручение о проведении оперативно-

[11] Подробнее об этом см. в разделе «Назначение и производство судебных экспертиз».

розыскных мероприятий, о производстве отдельных следственных и иных процессуальных действий (п. 4 ч. 2 ст. 38, ч. 1 ст. 144 УПК РФ). Поручение адресуется начальнику органа дознания, который, в свою очередь, дает конкретное задание подчиненному сотруднику оперативного подразделения.

В поручении может быть указано о необходимости производства оперативно-розыскных мероприятий, направленных на:

получение разрешения суда и направление запроса об истребовании у оператора сотовой связи входящих и исходящих телефонных соединений абонентского номера, с которого звонили заявителю, с указанием места нахождения (адресов) базовых станций, а также получение информации на чье имя зарегистрирован указанный абонентский номер;

получение разрешения суда и направление запроса в кредитные организации для предоставления сведений: о номере счета, на который заявителем осуществлялся денежный перевод, лице, на чье имя (паспортные данные, адрес фактического проживания, контактные номера) зарегистрирован счет, о подключении услуги «Мобильный банк», с указанием номеров телефонов и периода действия; о подключении услуги «Сбербанк Онлайн» (или аналогичной услуги в других кредитных организациях), дате подключения и способе получения паролей; других подключенных услугах СМС-подтверждения операций, с указанием номеров телефонов и периода действия; о снятии денежных средств в кредитных организациях и банкоматах;

получение разрешения суда и направление запроса в кредитную организацию для предоставления сведений по банковской карте, на которую заявитель перевел денежные средства: о дате выпуска карты, когда и где она выпущена (номер и адрес дополнительного офиса) и получена, номер лицевого счета; имеются ли у лицевого счета другие карты, если имеются, то указать их номера, период действия; о держателе карты (паспортные данные, адрес фактического проживания, контактные номера); о подключении услуги «Мобильный банк» с указанием номеров телефонов и периода действия; о подключении услуги «Сбербанк Онлайн» (или аналогичной услуги в других кредитных организациях), дате подключения и способе получения паролей; других подключенных услугах СМС-подтверждения операций с указанием номеров телефонов и периода действия;

проверку абонентского номера телефона (банковской карты или счета) на совпадение по другим уголовным делам, преступления по которым совершены аналогичным способом и др.

Срок исполнения поручения в ходе предварительной проверки сообщения о преступлении не должен превышать 10 суток.

Поручение о производстве оперативно-розыскных мероприятий исполняется в порядке, предусмотренном Инструкцией о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд[12]. Результаты выполнения поручения о проведении оперативно-розыскных мероприятий могут быть доложены начальнику органа дознания рапортом, после чего приобщаются следователем к материалу проверки. Сообщение о выполнении поручения должно носить конкретный информативный характер.

Принятие решения по итогам предварительной проверки сообщения о преступлении. По результатам рассмотрения заявления (сообщения) о преступлении следователем может быть принято одно из следующих решений:

1) о возбуждении уголовного дела в порядке, установленном ст. 146 УПК РФ;

2) об отказе в возбуждении уголовного дела в порядке, предусмотренном ст. 148 УПК РФ;

3) о передаче заявления (сообщения) по подследственности в соответствии со ст. 145, 151 УПК РФ. В случае принятия данного решения следователь принимает меры по сохранению следов преступления.

Однако следует учитывать, что в соответствии с Приказом МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений» проверка по сообщениям о преступлениях, предусмотренных ст. 158, 159–159.3, 159.5, 159.6 УК РФ, совершенных с использованием платежных карт, средств мобильной связи, сети Интернет, проводится в порядке ст. 144 УПК РФ, а принятие решения о возбуждении уголовного дела по указанным фактам осуществляется в органе, в который поступило первоначальное сообщение о преступлении.

[12] 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 сент. 2013 г. «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд» // Российская газета. 2013. № 282.

III. ОСОБЕННОСТИ ПРОИЗВОДСТВА ОТДЕЛЬНЫХ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ ПО УГОЛОВНЫМ ДЕЛАМ О ХИЩЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ, СЕТИ ИНТЕРНЕТ И СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

При наличии повода и достаточных данных, указывающих на признаки преступления, следователь возбуждает уголовное дело, о чем выносится соответствующее постановление. О принятом решении следователь незамедлительно уведомляет заявителя, разъясняет ему право на обжалование данного решения и порядок обжалования.

Признание потерпевшим и допрос потерпевшего (ст. 42 УПК РФ, ст. 187–191 УПК РФ). После возбуждения уголовного дела следователь незамедлительно признает заявителя потерпевшим, допрашивает его в качестве потерпевшего об обстоятельствах совершенного преступления.

В ходе допроса потерпевшему разъясняется его право на предъявление гражданского иска, предусмотренное ст. 44 УПК РФ, и при поступлении от него заявления последний признается гражданским истцом.

Круг вопросов, которые подлежат выяснению у потерпевшего при его допросе, аналогичен тем, что выясняются при получении письменных объяснений от заявителя в ходе проверки сообщений о рассматриваемых преступлениях.

Допрос свидетелей (ст. 56 УПК РФ, ст. 187–191 УПК РФ).

В ходе предварительного расследования в качестве свидетелей по уголовным делам данной категории могут быть допрошены *лица, которые располагают сведениями о совершенном преступлении*, например, члены семьи, проживающие с потерпевшим.

Так, при личном контакте кого-либо из членов семьи потерпевшего с лицом, которому были переданы денежные средства, следователю в ходе допроса свидетеля необходимо подробно описать внешность данного лица и выяснить возможность его опознания. После чего, следует направить свидетеля на составление композиционного портрета, предъявление фотокартотеки лиц, ранее судимых и состоящих на учете в органах внутренних дел и разослать ориентировки в территориальные подразделения органов внутренних дел с приметами лица, которому потерпевшим были переданы денежные средства.

При установлении *лица, которому потерпевший передал денежные средства*, необходимо в ходе допроса выяснить его роль в совершенном преступлении, а также установить:

когда, где, кому, каким способом были переданы денежные средства, полученные от потерпевшего;

оставлялась ли часть денежных средств себе, если да, то где они или на что были потрачены;

каким способом осуществлялась связь с лицом, сообщившим ему, куда и как перевести полученные от потерпевшего денежные средства, в каких отношениях он состоит с этим лицом;

подробно описать особенности речи этого лица (темп речи, манера говорить, голос, речевые дефекты), выяснить данные о его личности;

абонентский номер подозреваемого лица, а также абонентские номера, на которые были переведены денежные средства потерпевшего;

иные сведения.

После получения ответа от оператора сотовой связи в качестве свидетеля может быть допрошено *лицо, на которое зарегистрирована SIM-карта, с использованием которой звонили потерпевшему*. В ходе допроса необходимо установить:

когда, где и при каких обстоятельствах данное лицо приобрело указанную SIM-карту;

пользовалось ли оно этой SIM-картой, передавалась ли она кому-либо, если да, то когда, где, при каких обстоятельствах, имеются ли установочные данные гражданина, которому была передана SIM-карта, если нет, то почему, где в настоящее время находится данная SIM-карта.

В случае если гражданин, на которого оформлена SIM-карта, говорит о том, что не оформлял ее, то необходимо произвести выемку у оператора сотовой связи договора об оказании услуг сотовой связи с использованием данной SIM-карты, а также иных документов, послуживших основаниям для его заключения, и назначить по ним почерковедческую судебную экспертизу.

Если SIM-карта с интересующим следствие абонентским номером зарегистрированы на вымышленных лиц, то к материалам уголовного дела должна быть приобщена соответствующая справка территориального подразделения Управления по вопросам миграции МВД России по субъекту РФ и протоколы допросов лиц, проживаю-

щих по указанному адресу, а также их соседей, подтверждающих факт, что лицо по данному адресу не проживает.

При установлении факта несоответствия персональных данных фактических пользователей сведениям, заявленным в договоре об оказании услуг связи, а также для предотвращения и пресечения преступлений с использованием сетей связи и средств связи, следователем, в целях прекращения оказания услуг такому абоненту, направляется в подразделение органов внутренних дел, осуществляющее оперативно-розыскную деятельность, соответствующее уведомление.

В соответствии с ч. 1 ст. 46 Федерального закона от 7 июля 2003 г. № 126-ФЗ (в ред. от 30 декабря 2021 г.) «О связи»[13] оператор связи обязан прекратить оказание услуг связи при поступлении запроса от органа, осуществляющего оперативно-розыскную деятельность в случае неподтверждения в течение пятнадцати суток соответствия персональных данных фактических пользователей сведениям, заявленным в абонентских договорах, а также в случае предотвращения и пресечения преступлений с использованием сетей связи и средств связи.

В качестве свидетелей могут быть допрошены *сотрудники банков (кредитных организаций)* у которых необходимо выяснить:

должность, функциональные обязанности;

условия обслуживания банковских счетов и предоставления определенных услуг;

виды выпускаемых банковских карт, механизм перевода денежных средств с банковской карты;

наличие договора с потерпевшим как держателем банковской карты;

тип программного обеспечения, предоставляемый держателю банковской карты для удаленного доступа и управления банковским счетом, порядок его установки и использования;

операции, которые возможно совершить с использованием данного программного обеспечения;

обращался ли потерпевший с заявлением о блокировке банковской карты;

проводилась ли банком (кредитной организацией) проверка правомерности перевода денежных средств с банковского счета потерпевшего, если проводилась, то каковы ее результаты;

[13] Собр. законодательства Рос. Федерации. 2003. № 28, ст. 2895 // СПС КонсультантПлюс.

иные обстоятельства, имеющие значение для расследования уголовного дела.

У сотрудников *банков (кредитных организаций)*, на банковские счета в которых были переведены похищенные денежные средства, следует выяснить:

какие документы, удостоверяющие личность, предъявило подозреваемое лицо;

когда и какие именно действия им были совершены;

находились ли с ним иные лица;

имеются ли в зале обслуживания камеры видеонаблюдения;

иные сведения.

В качестве свидетеля может быть допрошен *сотрудник организации, предоставляющей услуги оператора сотовой связи*, например, об особенностях оказания соответствующих услуг, в том числе, удаленного доступа к сети Интернет для использования программного обеспечения «Онлайн банк», «Мобильный банк».

Также, в качестве свидетелей могут быть допрошены:

родственники, знакомые потерпевшего, которые располагают какой-либо информацией, имеющей значение для расследования уголовного дела;

родственники, знакомые, соседи по месту жительства подозреваемого, обвиняемого об обстоятельствах, характеризующих его личность и образ жизни;

сотрудники оперативных подразделений органов, осуществляющих оперативно-розыскную деятельность, выявившие преступление и установившие личность подозреваемого по обстоятельствам, ставшим им известным относительно совершенного преступления;

иные лица, которые располагают какой-либо информацией, имеющей значение для расследования уголовного дела.

При необходимости для разъяснения данного им заключения может быть допрошен *эксперт* (ст. 205 УПК РФ).

Необходимая информация, имеющая доказательственное значение по уголовному делу, может быть получена путем направления ***запросов***[14] в соответствующие органы, организации и учреждения.

[14] См.: Практическое пособие следователя по расследованию уголовных дел о хищениях, совершенных дистанционным способом со сборником типовых запросов направляемых при расследовании уголовных дел указанной категории, подготовленное ГСУ ГУ МВД России по Кемеровской области // Материалы предоставлены Следственным департаментом МВД России.

Для установления анкетных данных владельца абонентского номера, который использовался при совершении преступления, следователем на основании ч. 4 ст. 21, подп. 3 и 6 ч. 2 ст. 38 УПК РФ, ч. 5 ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи» может быть направлен запрос соответствующему *оператору связи* о предоставлении необходимых сведений:

об абоненте, на которого зарегистрирован номер телефона, с указанием паспортных данных, даты активации SIM-карты и ее состоянии в текущий момент;

об абонентских номерах, действующих с использованием SIM-карт с ICC №_____, с указанием паспортных данных абонентов, на которых зарегистрированы абонентские номера;

о точке продажи SIM-карты с интересующим абонентским номером, с указанием адреса и контактных данных организации;

о месте хранения оригинала договора об оказании услуг связи, заключенного при регистрации интересующего абонентского номера, с указанием адреса и контактных данных.

В *кредитных организациях*, где открыты счета потерпевшего и счета, используемые подозреваемым лицом при совершении преступления, следователем с согласия руководителя следственного органа, в соответствии с ч. 4 ст. 21, подп. 3 и 6 ч. 2 ст. 38 УПК РФ, ч. 4 ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 (ред. от 30 декабря 2021 г.) «О банках и банковской деятельности» может быть получена информация:

о движении денежных средств по банковской карте/счету №_____, за период с _____ по _____;

о безналичных переводах по банковской карте №_____, с указанием времени совершения операции (МСК), информации о контрагентах (владельцах банковских карт отправителей/получателей денежных средств, абонентских номеров, при перечислении денежных средств в период с _____ по _____;

о подключении услуги удаленных каналов обслуживания «Мобильный банк» на банковскую карту №_____;

об IP-адресах с которых осуществлялся вход в ДБО «Название системы» банковской карты №_____ с _____ по _____;

о банковских картах, к которым подключена услуга «Мобильный банк» на абонентский номер 8_____ (данные владельца карты, движение денежных средств по счету, расширенный отчет о движении денежных средств, отчет о безналичных переводах, подключение

услуги «Мобильный банк», IP-адреса при использовании ДБО «Название системы»).

При совершении операций по банковской карте через устройство самообслуживания (банкомат), следователю в запросе в кредитную организацию следует указать на необходимость архивации видеозаписи с камер наблюдения, и ее предоставлении в следственный орган на электронном носителе.

В случае если полный номер банковской карты подозреваемого лица не известен, то в запросе необходимо указать все данные об интересующей следствие транзакции, например:

сведения о банковской карте, на счет которой __.__.20__ в __ ч. __ мин. (время московское) со счета абонентского номера (банковской карты) №_____ осуществлен перевод в сумме _____ рублей (номер транзакции ____, получатель денежных средств – 427684__0020)

расширенный отчет по счету указанной банковской карты, отчет о безналичных переводах, информацию об IP-адресах с которых осуществлялся вход в ДБО «Название системы».

В ходе предварительного следствия следователем с согласия руководителя следственного органа, в соответствии с ч. 4 ст. 21, подп. 3 и 6 ч. 2 ст. 38 УПК РФ, ст. 26 Федерального закона от 27 июня 2011 г. № 161-ФЗ (ред. от 2 июля 2021 г.) «О национальной платежной системе», ч. 4 ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 (ред. от 30 декабря 2021 г.) «О банках и банковской деятельности», может быть направлен запрос в *организацию, осуществлявшую перевод денежных средств,* о предоставлении имеющей значение для уголовного дела информации о пользователях, совершивших операции в системе «Наименование платежной системы» с использованием абонентских номеров № _____, № _____, а именно:

о данных пользователя, указанных при регистрации;

о поступлении денежных средств на счет и их движении на другие счета в период с _____ до _____, с указанием номера банковской карты/счета, с которой поступили денежные средства;

о данных об IP-адресах, использовавшихся при совершении транзакций.

Следователю в запросах необходимо обязательно разъяснять, что невыполнение его законных требований является административным правонарушением, ответственность за совершение которого предусмотрена статьей 17.7 КоАП РФ.

Одним из наиболее распространенных следственных действий на первоначальном этапе расследования является ***выемка*** (ст. 183 УПК РФ). При проведении данного следственного действия необходимо иметь в виду, что часть документов могла быть изъята в процессе проверки сообщения о преступлении или осмотра места происшествия. В ряде случаев необходимые сведения и информацию можно получить путем направления запросов в различные соответствующие органы, организации и учреждения.

Выемка производится на основании постановления следователя, а выемка в жилище; предметов и документов, содержащих государственную или иную охраняемую федеральным законом тайну; предметов и документов, содержащих информацию о вкладах и счетах граждан в банках и иных кредитных организациях; а также вещей, заложенных или сданных на хранение в ломбард – на основании судебного решения, принимаемого в порядке, установленном ст. 165 УПК РФ.

С целью установления способа хищения денежных средств с банковской карты (банковского счета), места нахождения подозреваемого лица в момент изъятия из законного владения собственника (иного владельца) денежных средств с банковской карты (банковского счета), следователю необходимо в соответствии со ст. 182, 183 и ч. 1 ст. 165 УПК РФ с согласия руководителя следственного органа возбудить перед судом ходатайство о производстве выемки информации о вкладах и счетах граждан в банках и иных кредитных организациях.

Анализ уголовных дел о преступлениях рассматриваемого вида, проведенный ГСУ ГУ МВД России по Саратовской области[15], показал, что следователи территориальных органов предварительного следствия при возбуждении перед судами ходатайства в выносимых постановлениях ограничиваются лишь получением информации о движении денежных средств по банковскому счету потерпевшего. Данная информация позволяет лишь подтвердить факт изъятия из законного владения потерпевшего денежных средств, но не установить способ их хищения и место нахождение подозреваемого лица в момент такого изъятия.

[15] Методические рекомендации «Тактика и методика раскрытия преступлений по фактам хищения денежных средств граждан с банковских счетов, совершенных в системе дистанционного банковского обслуживания, посредством использования всемирной сети Интернет, средств мобильной связи, IT-технологий», подготовлены ГСУ ГУ МВД России по Саратовской области // Материалы предоставлены Следственным департаментом МВД России.

По мнению авторов указанных методических рекомендаций с целью получения исчерпывающей информации в постановлениях о возбуждении перед судом ходатайства о производстве выемки информации о вкладах и счетах граждан в банках и иных кредитных организациях, необходимо конкретизировать запрашиваемую информацию: «Ходатайствовать перед судом о производстве выемки в ПАО «Банк» (получении) информации о движении денежных средств по банковской карте № _____ (банковскому счету № _____), открытой на имя (потерпевшего) Иванова Ивана Ивановича, __.__.19__ года рождения, а именно:

информации о дате открытия счета, месте открытия счета, дате, времени и месте подключения к банковской карте (счету) услуги «Мобильный банк», услуги «Онлайн банк», идентификационном номере пользователя и пароле, необходимых для входа в «Личный кабинет» заявителя;

посредством какой услуги («Мобильный банк», через «Личный кабинет», «Онлайн банк», pos-терминал, банкомат) в установленную в ходе следствия дату __.__.20__ денежные средства в сумме _____ рублей перечислены с банковской карты № _____ (банковского счета № _____) Иванова Ивана Ивановича, __.__.19__ года рождения (потерпевшего);

на какой номер счета (номер банковской карты) __.__.20__ были перечислены денежные средства в сумме _____ рублей, место открытия счета, кредитной организации, в которой открыт счет, на который перечислены денежные средства, фамилия, имя, отчество, дата рождения, паспортные данные лица, на который данный счет открыт;

информации о месте обналичивания (снятия) денежных средств, начиная с __ часов __ минут __.__.20__ (с указанием номера банкомата и места его расположения);

если перечисление денежных средств осуществлялось посредством услуги «Мобильный банк» с банковской карты № _____ (банковского счета №_____) Иванова Ивана Ивановича, __.__.19__ года рождения, то предоставить информацию: с какого абонентского номера телефона поступило СМС-сообщение с кодом-подтверждения (поручением/распоряжением на проведение операции по перечислению __.__.20__ денежных средств в сумме _____ рублей с банковского счета потерпевшего), точном времени (дата, час, минута) поступления в банк СМС-сообщения с кодом-подтверждения (поручением/распоряжением на проведение операции по

перечислению __.__.20__ денежных средств в сумме _____ рублей с банковского счета потерпевшего);

если перечисление денежных средств осуществлялось посредством услуги «Онлайн банк» (через «Личный кабинет» потерпевшего), то предоставить информацию: в какое точное время (дата, час, минута, секунда) и с какого IP-адреса __.__.20__ осуществлялся вход в «Личный кабинет» «Онлайн банка» в момент перечисления денежных средств в сумме _____ рублей;

если перечисление денежных средств осуществлялось посредством банкомата, то предоставить информацию: в какое точное время (дата, час, минута, секунда), с какого номера банкомата, места его расположения были перечислены денежные средства (аналогично в отношении pos-терминала).

После получения информации о том, что *перечисление денежных средств было осуществлено посредством услуги «Онлайн банк»,* с указанного банком IP-адреса в точно определенное время (поминутное, либо посекундное), следует установить компанию-провайдер, предоставившую IP-адрес в точное время.

Для этого следователю необходимо[16]:

направить в порядке, предусмотренном п. 4 ч. 2 ст. 38 УПК РФ, письменное поручение в оперативное подразделение территориального органа внутренних дел, с целью получения из соответствующего подразделения специальных технических мероприятий органов внутренних дел Российской Федерации информации о компаниях – провайдерах и MAC-адресе устройства, (логине, пароле, месте нахождения устройства), с которого был осуществлен доступ в сеть Интернет с указанного банком IP-адреса в точное время (дата, час, минута, секунда).

либо самостоятельно установить компанию-провайдер через справочные интернет-ресурсы (сервисы): *«reg.ru»*, «*whois-service.ru»*, *«2ip.ru»* (в случае необходимости открыть вкладку «IP-LOOKUP»), указать IP-адрес, содержащийся в ответе банка при предоставлении сведений о движении денежных средств по счетам, и нажать «Проверить». После чего справочным интернет-ресурсом будет выведена

[16] Методические рекомендации «Тактика и методика раскрытия преступлений по фактам хищения денежных средств граждан с банковских счетов, совершенных в системе дистанционного банковского обслуживания, посредством использования всемирной сети Интернет, средств мобильной связи, IT-технологий», подготовлены ГСУ ГУ МВД России по Саратовской области // Материалы предоставлены Следственным департаментом МВД России.

информация о компании – провайдере, использующей интересующие IP-адреса. Как правило, информация предоставляется на латинском алфавите в сочетании английских и русских слов, с указанием компании – провайдера, ее юридического и фактического адреса, контактных номерах телефонов (факс). Полученную посредством данных справочных интернет-ресурсов информацию можно перекопировать посредством производства скриншота[17], который приобщается следователем к материалам уголовного дела рапортом, доложенным руководителю следственного органа.

После установления компании-провайдера необходимо направить в порядке, предусмотренном ч. 4 ст. 21 УПК РФ, в данную организацию запрос (заверенный гербовой печатью, с обязательным указанием разумных сроков исполнения и разъяснением последствий, предусмотренных ст. 17.7 КоАП РФ) о предоставлении сведений о том, кому в точное время (дата, час, минута, секунда) был предоставлен IP-адрес, содержащийся в ответе банка, месте нахождения абонента, использующего данный IP-адрес, дате регистрации договора предоставления услуг связи в сети Интернет, с кем заключен договор (ФИО, дата рождения, место регистрации, паспортные данные), информации о логине, пароле, при помощи которых осуществляется доступ клиента в сеть Интернет, информации о MAC-адресе устройства[18], с которого осуществлялся выход в сеть Интернет в момент совершения преступления.

[17] Скриншот (англ. screenshot) – это снимок экрана (фотография) того, что видит человек на мониторе. Чтобы сделать скриншот, в момент открытия нужного «окна», необходимо нажать на кнопку клавиатуры «Print/Screen» или «PrtSc/SysRq», либо, если работаете на ноутбуке, сочетание клавиш: «Fn»- «PrtSc/SysRq». После этого необходимо открыть «Microsoft Office Word», либо программу «Pain», затем нажать сочетание клавиш «Ctrl»-«V» («горячая кнопка «Вставить»), скопированное фотографическое изображение будет вставлено в документ, после чего необходимо сохранить скриншот (команда «Сохранить», либо сочетание клавиш «Ctrl»-«S»).

[18] MAC-адрес (англ. Media Access Control — управление доступом к среде, также Hardware Address) – уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Интернет (Ethernet). При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес), прошитый в ней при изготовлении. Этот номер используется для идентификации при появлении в сети нового компьютера (или другого устройства, способного работать в сети). Его еще называют «Физический адрес». Именно поэтому определение MAC-адреса устройства для доказывания места совершения преступления (места нахождения преступника, похитившего денежные средства с банковского счета потерпевшего посредством услуги «Онлайн банка» путем выхода в сеть Интернет), имеет одно из приоритетных значений.

Поле получения из компании – провайдера сведений о месте (адресе) выхода во всемирную сеть Интернет, MAC-адресе устройства, необходимо провести обыск в указанном помещении, либо на основании судебного решения обыск в жилище, с целью обнаружения и изъятия орудий совершения преступления (системных блоков, компьютеров, ноутбуков, планшетов, wi-fi-роутеров, модемов, смартфонов, договоров об оказании услуг связи в сети Интернет).

В случае получения из банка информации о том, что *перечисление денежных средств потерпевшего с банковского счета (банковской карты) было осуществлено посредством услуги «Мобильный банк»*, необходимо принять меры к установлению лица, на которого зарегистрирован абонентский номер, с которого в банк поступило СМС-сообщение с кодом-подтверждения перечисления денежных средств с банковского счета потерпевшего.

Для этих целей следователю надлежит в порядке, предусмотренном ст. 186.1 УПК РФ, выйти в суд с ходатайством о получении информации о соединениях между абонентами и (или) абонентским устройствами с привязкой к приемопередающим базовым станциям[19].

При получении из банка информации *о движении денежных средств по банковскому счету (банковской карте) потерпевшего с указанием номера счета (банковской карты), на который были перечислены денежные средства потерпевшего*, места его открытия, места обналичивания (снятия) денежных средств следователю необходимо[20]:

принять меры к своевременному изъятию видеозаписей с камер наблюдения банкоматов (поскольку, как правило, они хранятся банком не более 60–90 суток);

с целью установления места нахождения лица, обналичившего (снявшего) похищенные у потерпевшего денежные средства, а также проверки его на причастность к совершению иных (аналогичных) преступлений, в соответствии со ст. 182, 183 и ч. 1 ст. 165 УПК РФ с согласия руководителя следственного органа возбудить перед судом

[19] Подробнее об этом см. в разделе «Получение информации о соединениях между абонентами и (или) абонентскими устройствами».

[20] Методические рекомендации «Тактика и методика раскрытия преступлений по фактам хищения денежных средств граждан с банковских счетов, совершенных в системе дистанционного банковского обслуживания, посредством использования всемирной сети Интернет, средств мобильной связи, IT-технологий», подготовлены ГСУ ГУ МВД России по Саратовской области // Материалы предоставлены Следственным департаментом МВД России.

ходатайство о производстве выемки информации о вкладах и счетах граждан в банках и иных кредитных организациях.

В постановлении следует указать: «Ходатайствовать перед судом о производстве выемки в ПАО «Наименование банка» (получении) информации о движении денежных средств по банковской карте № _____, открытой ПАО «Наименование банка», расположенном по адресу: _____ (с реквизитами получателя: _____), а именно:

о дате открытия счета (банковской карты), месте (отделении) открытия счета (банковской карты), фамилии, имени, отчестве лица, на которого счет (банковская карта) открыт, информацию о дате рождения, месте рождения, серии и номере паспорта гражданина Российской Федерации, месте регистрации;

о подключении к банковской карте № _____ услуги «Мобильный банк», к какому абонентскому номеру телефона данная услуга подключена, дата, время и место подключения;

о подключении к счету услуги «Онлайн банк», с каких IP-адресов с указанием точного времени (дата, час, минута, секунда) осуществлялся вход в личный кабинет клиента данного счета («Онлайн банка»), начиная с __ часов __ минут __ секунд __.__.20__ по настоящее время;

о последних десяти IP-адресах с обязательным указанием точного времени (дата, час, минута, секунда) входа в «Личный кабинет» услуги «Онлайн банк» банковской карты № _____;

о движении денежных средств по банковской карте № _____, начиная с __ часов __ минут __ секунд __.__.20__ по настоящее время, с указанием мест обналичивания (снятия со счета) денежных средств (номеров банкоматов и адресах их расположения); если с момента обналичивания (снятия со счета) денежных средств прошло менее 90 суток, предоставить видеозаписи с камер наблюдения банкоматов (мест обналичивания (снятия со счета) денежных средств;

о статусе банковского счета на настоящий момент (открыт, действует, либо закрыт; если закрыт – то указать дату и основания для закрытия счета).

При получении информации о том, что *похищенные денежные средства перечислены на абонентский номер*, который не выходил в эфир и зачастую является аккаунтом «виртуального кошелька» (виртуального счета) электронной платежной системы, позволяющей

производить платежи с использованием различных устройств и каналов связи, как стационарных, так и мобильных (Яндекс-деньги, QIWI-кошелек, «WebMoney» и т.п.), следователю необходимо в соответствии со ст. 182, 183 и ч. 1 ст. 165 УПК РФ с согласия руководителя следственного органа возбудить перед судом ходатайство о производстве выемки информации о вкладах и счетах граждан в банках и иных кредитных организациях, например, информации о движении денежных средств по виртуальному счету «8_____» (либо «+7_____») платежной системы «WebMoney», расположенной по адресу: 119049, Россия, г. Москва, ул. Коровий вал, д. 7, строение 1, секция 9, а именно[21]:

о дате создания аккаунта «+7_____» виртуального счета, с какого IP-адреса с указанием точного времени (дата, час, минута, секунда) был активирован (авторизован) данный счет, какие анкетные данные указаны при создании аккаунта виртуального счета: фамилия, имя, отчество, дата рождения, серия и номер паспорта, дата выдачи, орган, выдавший, гражданство, адрес регистрации, ИНН, СНИЛС, ИН ОМС, данные об адресе электронной почты (e-mail);

о движении денежных средств по виртуальному счету за периоды, например: с 00 часов 01 минуты 28.03.2020 до 23 часов 59 минут 30.03.2020, с 09 часов 01 минуты 06.05.2020 до 23 часов 59 минут 10.05.2020 (включительно);

об IP-адресе с которого осуществлялся последний вход в «Личный кабинет» виртуального счета «+7_____» с указанием точного времени (дата, час, минута, секунда);

о состоянии виртуального счета (на дату обращения с ходатайством в суд), его балансе.

Выемка также может быть произведена в целях изъятия электронных носителей информации, средств мобильной связи, иных предметов и документов, имеющих значение для уголовного дела, в случаях, когда точно известно, где и у кого они находятся.

При наличии достаточных данных полагать, что в каком-либо месте или у какого-либо лица могут находиться средства мобильной связи, компьютерные устройства, носители компьютерной информации, в том числе вредоносные компьютерные программы, устройства

[21] Методические рекомендации «Тактика и методика раскрытия преступлений по фактам хищения денежных средств граждан с банковских счетов, совершенных в системе дистанционного банковского обслуживания, посредством использования всемирной сети Интернет, средств мобильной связи, IT-технологий», подготовлены ГСУ ГУ МВД России по Саратовской области // Материалы предоставлены Следственным департаментом МВД России.

телекоммуникации и иное оборудование, явившиеся орудием или средством совершения преступления, а также иные предметы, документы и ценности, которые могут иметь значение для уголовного дела, то может быть произведен ***обыск*** (ст. 182 УПК РФ).

Обыск производится на основании постановления следователя, а обыск в жилище – на основании судебного решения, принимаемого в порядке, установленном ст. 165 УПК РФ.

Так, например, при получении из компании – провайдера сведений о месте (адресе) выхода в сеть Интернет, MAC-адресе устройства подозреваемого лица обыск в жилище может быть произведен на основании судебного решения следователем с участием специалиста в области компьютерных технологий с целью обнаружения и изъятия следующих предметов и документов:

компьютерной техники, электронных носителей информации (системных блоков персональных компьютеров, установленных в них накопителей на жестких магнитных дисках, иных электронных носителей информации, а также устройств телекоммуникации (wi-fi-роутера, модема), средств мобильной связи);

договора об оказании услуг связи в сети Интернет, документов, отражающих факты выдачи денежных средств, удостоверяющих личность, наличие соответствующего образования и уровень квалификации подозреваемого лица, а также дневников, записных книжек и черновых записей, содержащих информацию о его социальных связях и роде деятельности;

литературы, содержащей сведения, которые относятся к этапам подготовки, совершения и сокрытия хищений денежных средств с использованием банковских карт, сети Интернет и средств мобильной связи;

свободных образцов почерка и подписи, содержащихся в письмах, личных дневниках, записных книжках и т.д.;

фотографий, видеозаписей (особенно важно их изъятие при расследовании преступлений, совершенных в соучастии, например, организованными группами, в целях доказывания наличия устойчивых межличностных связей между участниками);

иных предметов и документов, имеющих доказательственное значение.

Изъятие электронных носителей информации производится в порядке, предусмотренном ст. 164 и 164.1 УПК РФ.

Все изъятые при производстве выемки и обыска объекты должны быть осмотрены, о чем составляется соответствующий протокол.

Согласно ч. 1 ст. 176 УПК РФ ***осмотр жилища, иного помещения, предметов и документов*** производится в целях обнаружения следов преступления, выяснения других обстоятельств, имеющих значение для уголовного дела. Порядок производства осмотра определен в ст. 177 УПК РФ.

В ходе предварительного следствия по уголовному делу следователем может быть произведен *осмотр ранее изъятых мобильных средств связи, как потерпевшего, так и подозреваемого*. К такому осмотру целесообразно привлекать специалиста в области компьютерных технологий и при необходимости использовать технические средства («UFED», «XRY», «Мобильный криминалист» и др.).

Осмотр *мобильных средств связи* может быть произведен с целью отыскания и закрепления следующей информации:

IMEI телефонного аппарата;

наличия SIM-карт с абонентскими номерами;

информации, содержащейся в журнале вызовов мобильного устройства, в банке СМС-сообщений, в записной книжке (или «контактах») внутренней памяти мобильного устройства или SIM-карты;

в виде сохраненных текстов переписки между соответствующими абонентскими устройствами по средством СМС-сообщений или других мессенджеров, например «WhatsApp», «Viber»;

об истории посещения интернет-сайтов;

о поиске через установленный на устройстве браузер в интернете сведений, имеющих отношение к исследуемому событию;

об использовании соответствующих интернет-сервисов, позволяющих осуществлять виртуальный оборот денежных средств (различные электронные кошельки);

о регистрации в качестве пользователя в социальной сети, на личной странице которого могут содержаться данные, представляющие интерес для расследования (социальные сети «Вконтакте», «Одноклассники» и пр.);

в виде сохраненных логинов и паролей (например, некоторые установленные на мобильное средство связи утилиты (программы) позволяют сохранять информацию о логинах и паролях всех, когда-либо посещенных сайтов);

о типе программного обеспечения мобильного устройства, наличия в нем собственной антивирусной программы и ее активности.

В рамках осмотра необходимо детально исследовать соответствующие разделы приложения «Мобильный банк» («История платежей», «Последние операции» и пр.), в которых зафиксировано движение денежных средств по счету (банковской карте), сделать снимки экрана мобильного устройства, запечатлевающие данную информацию с помощью самого устройства (если позволяет его аппаратно-программное обеспечение), либо сфотографировать экран любым устройством, позволяющим получить фотографическое изображение. Обнаружению и закреплению (фотографированию) также подлежит информация, находящаяся в памяти мобильного устройства, отражающая переписку с подозреваемым лицом, с помощью СМС-сообщений, переписки в Viber, WatsApp и пр., сохраненные страницы в мобильном браузере из социальных сетей, электронных торговых площадок (и их мобильных приложений) и пр.

Информация, полученная в ходе осмотра мобильного устройства, подлежит занесению в протокол, а фотоматериалы необходимо приобщить фототаблицей.

Одним из наиболее спорных вопросов, связанных с осмотром содержимого мобильного устройства, изъятого у подозреваемого, является вопрос о наличии оснований для проведения такого следственного действия без получения судебного решения.

Так, Тверским областным судом в порядке, предусмотренном ст. 125 УПК РФ, была рассмотрена апелляционная жалоба заявителя на постановление Пролетарского районного суда г. Твери от 13 мая 2016 г., которым жалоба на действия следователя, связанные с незаконным поручением руководителю отдела криминалистики <наименование, адрес> осмотра сотовых телефонов, изъятых в ходе обыска в жилище, оставлена без удовлетворения.

В апелляционной жалобе заявитель в обосновании своей позиции указал, что при отказе в удовлетворении жалобы суд не учел положения ст. 23 Конституции РФ, определяющей право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а также требования ст. 13 и п. 3 ст. 38 УПК РФ. Считает, что вывод суда о признании законным ограничения прав собственников телефонов на тайну переписки без судебного решения не основан на законе, поскольку осмотр телефона включает в себя осмотр телефонного аппарата, но не его содержимого, в том числе телефонных соединений, контактов, СМС-сообщений, переписки в социальных сетях, на

осмотр которых следователем без судебного решения было дано поручение эксперту произвести осмотр.

Рассмотрев жалобу, суд апелляционной инстанции пришел к следующему.

Суд первой инстанции, принимая решение об отказе в удовлетворении жалобы заявителя, правильно пришел к выводу об отсутствии оснований для признания незаконными и необоснованными действий следователя СУ <наименование, адрес>, связанные с поручением руководителю отдела криминалистики <наименование, адрес> осмотра сотовых телефонов, изъятых в ходе обыска в жилище.

Как следует из представленных материалов ДД.ММ.ГГГГ следователем СУ <наименование, адрес>, в присутствии двух понятых, в рамках возбужденного ДД.ММ.ГГГГ уголовного дела, был произведен обыск в квартире ФИО в целях отыскания и изъятия предметов, документов, ценностей, изъятых из гражданского оборота, имеющих значение к расследуемому уголовному делу.

В ходе обыска в жилище были изъяты предметы, имеющие значение для уголовного дела, в том числе, мобильные телефоны которые были направлены в отдел криминалистики <наименование, адрес> для проведения осмотра с применением специальной техники. Постановлением Пролетарского районного суда г. Твери от 2 апреля 2016 г. производство обыска в указанной квартире было признано законным.

При таких обстоятельствах у суда не было оснований полагать, что действиями следователя при производстве обыска и последующей процессуальной реализации его результатов были допущены нарушения уголовно-процессуального закона, способные причинить ущерб конституционным правам и свободам заявителя либо затруднить доступ к правосудию.

Доводы заявителя о том, что его права на тайну телефонных переговоров, переписку, закрепленные ст. 23 Конституции РФ, были нарушены в ходе проведения осмотра изъятых в ходе обыска принадлежавших ему телефонов с применением специальной техники, по мнению суда апелляционной инстанции не обоснованы и не подлежат удовлетворению, поскольку действия следователя по собиранию доказательств были выполнены в полном соответствии с требованиями уголовно-процессуального закона. Ссылка заявителя на ст. 186.1 УПК РФ, в которой закреплен порядок получение информации о соединениях между абонентами и (или) абонентскими устройствами,

является ошибочной, поскольку для осуществления обжалуемых заявителем действий следователя судебного решения, не требуется[22].

Следует отметить, что вопросы, касающиеся производства осмотра изъятых абонентских устройств без получения судебного решения, рассматривались и Конституционным судом Российской Федерации.

Так, в Определении от 25 января 2018 г. № 189-О Конституционный Суд Российской Федерации отметил, что *проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств, изъятых при производстве следственных действий в установленном законом порядке, не предполагает вынесения об этом специального судебного решения*. Лица же, полагающие, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения способны причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, могут оспорить данные процессуальные решения и следственные действия в суд в порядке, предусмотренном ст. 125 УПК РФ[23].

Таким образом, основным критерием оценки законности действий следователя, осмотревшего мобильное устройство и получившего доступ к содержащейся в нем информации, является его правомерное изъятие с соблюдением требований действующего законодательства.

При хищениях денежных средств, совершенных при помощи вредоносного программного обеспечения (ВПО), потерпевшими от такого рода преступлений становятся владельцы мобильных устройств на базе платформы Android. Вирус позволяет удаленно управлять отправкой СМС-сообщений с телефона и перехватывать ответные сообщения, не уведомляя владельца телефона. Пропажа денежных средств обнаруживается потерпевшим при проверке баланса карты или проведении операций по обналичиванию. По этой причине

[22] Апелляционное постановление Тверского областного суда № 22-1501/16 22К-1501/2016 от 29 июня 2016 г. по делу № 22К-1501/2016 // https://sudact.ru/regular/doc/Cg2haahb1SHr/ (дата обращения: 14.02.2021).

[23] Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав ст. 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации: Определение Конституционного Суда РФ от 25 янв. 2018 г. № 189-О // СПС КонсультантПлюс.

осмотр самого телефона на предмет сохраненных сообщений не дает результата.

Признаками противоправного деяния при наличии в мобильном устройстве ВПО будут служить СМС-сообщения, направляемые на сервисные номера банка с абонентского номера потерпевшего, которые будут видны только при получении детализации соединений его абонентского номера.

В соответствии с ч. 5 ст. 186.1 УПК РФ представленные документы операторов сотовой связи, содержащие информацию о соединениях между абонентами и (или) абонентскими устройствами, осматриваются следователем с участием специалиста (при необходимости), о чем составляет протокол, в котором должна быть указана та часть информации, которая, по мнению следователя, имеет отношение к уголовному делу (дата, время, продолжительность соединений между абонентами и (или) абонентскими устройствами, номера абонентов и другие данные).

Так, например, следователю в ходе *осмотра информации о соединениях между абонентами и (или) абонентскими устройствами* подозреваемого лица необходимо обращать внимание на совершение последним звонков в банковские учреждения, операторам сотовых компаний, на иные стационарные телефоны, где производится аудиозапись телефонных переговоров. При выявлении таких звонков и наличии соответствующей аудиозаписи, следователем должна быть произведена ее выемка. В последующем, в целях идентификации (отождествления) голоса звонившего с голосом подозреваемого (обвиняемого) может быть назначена фоноскопическая судебная экспертиза.

Объектом осмотра также могут являться *результаты оперативно-розыскной деятельности*, в том числе, например, аудиозапись телефонных переговоров лиц, подозреваемых в совершении преступления. Аудиозапись переговоров осматривается с тем, чтобы обеспечить достоверность записанной информации. В протоколе осмотра фиксируются содержание записи, время звучания. Если значение для дела имеет не вся фонограмма, а лишь ее часть, в протоколе отражается содержание только этой части и фиксируются фразы, которыми начинается и заканчивается фонограмма.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ).

В соответствии с ч. 1 ст. 186.1 УПК РФ получение следователем информации о соединениях между абонентами и (или) абонентскими

устройствами допускается на основании судебного решения при наличии достаточных данных полагать, что такая информация имеет значение для уголовного дела.

Следует отметить, что при расследовании преступлений, совершенных с использованием средств мобильной связи, получение следователем такой информации должно проводиться по каждому уголовному делу.

Процессуальный порядок получения информации о соединениях между абонентами и (или) абонентскими устройствами закреплен в ст. 186.1 УПК РФ.

Кроме того, правовыми основами получения информации о соединениях между абонентами и (или) абонентскими устройствами являются ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ (в ред. от 30 декабря 2021 г.) «О связи»[24] и постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 (ред. от 17 апреля 2021 г.) «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность»[25]. Правила хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи, утверждены постановлением Правительства РФ от 12 апреля 2018 г. № 445 (ред. от 28 мая 2019 г.)[26].

Согласно п. 24.1 ст. 5 УПК РФ, под получением информации о соединениях между абонентами и (или) абонентскими устройствами понимается получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих базовых станций.

К другим данным, позволяющим идентифицировать абонентов, могут относиться, в частности, сведения о IMEI-коде абонентского

[24] Собр. законодательства Рос. Федерации. 2003. № 28, ст. 2895 // СПС КонсультантПлюс.

[25] Собр. законодательства Рос. Федерации. 2005. № 36, ст. 3704 // СПС КонсультантПлюс.

[26] Собрание законодательства РФ. 2018. № 17. Ст. 2489.

устройства или о местоположении телефонного аппарата относительно базовой станции[27].

Стоит обратить внимание на тот факт, что, в отличие от ст. 186 УПК РФ, для получения согласия суда на получение информации о соединениях между абонентами и (или) абонентским устройствами не требуется квалификация деяния как преступления средней тяжести, тяжкого, особо тяжкого (ст. 15 УК РФ).

В соответствии с ч. 1 ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ (в ред. от 30 декабря 2021 г.) «О связи» операторы связи обязаны хранить на территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий;

2) 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.

Для получения информации о соединениях между абонентами и (или) абонентскими устройствами следователь в соответствии со ст. 186.1 и ч. 1 ст. 165 УПК РФ с согласия руководителя следственного органа возбуждает перед судом ходатайство о производстве указанного следственного действия, в котором указываются:

1) уголовное дело, при производстве которого необходимо выполнить данное следственное действие;

2) основания, по которым производится данное следственное действие;

3) период, за который необходимо получить соответствующую информацию, и (или) срок производства данного следственного действия;

4) наименование организации, от которой необходимо получить указанную информацию.

[27] См.: О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (ст. 165 УПК РФ): Постановление Пленума Верховного Суда РФ от 1 июня 2017 г. № 19, п. 11 // Бюллетень Верховного Суда Рос. Федерации. № 7. 2017.

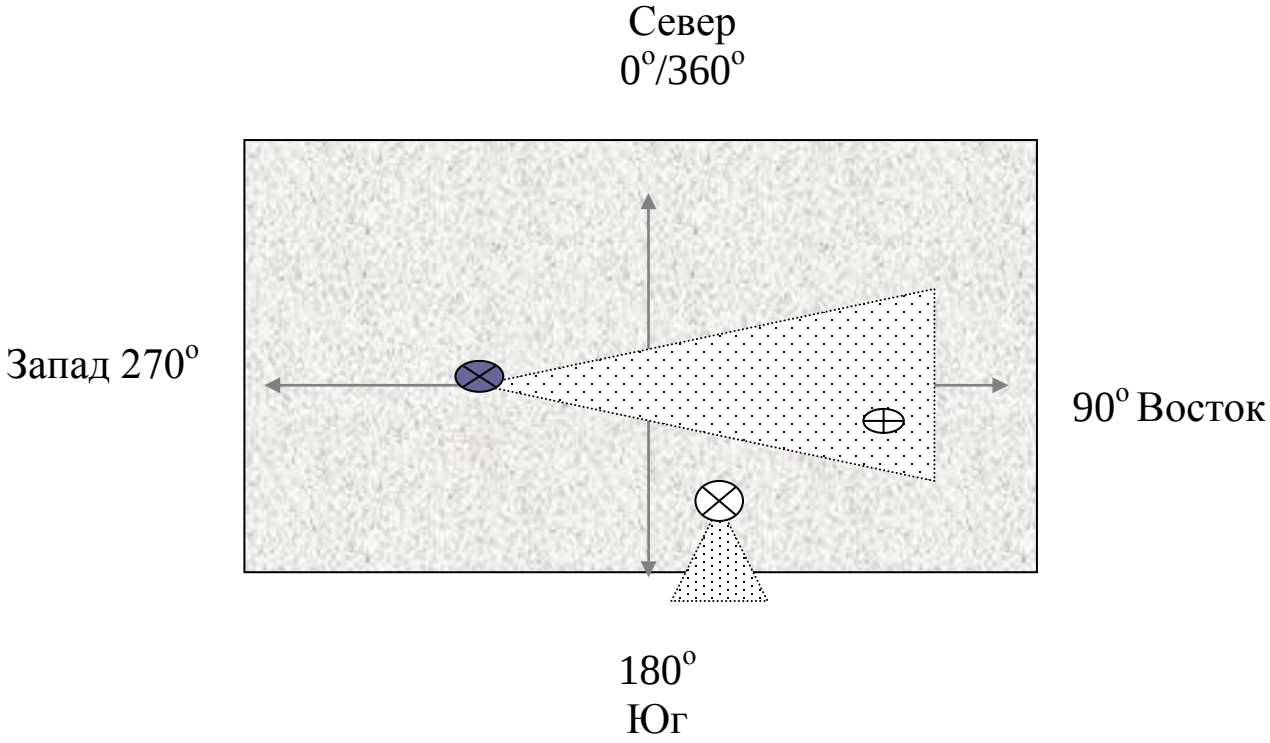
Анализ уголовных дел о преступлениях рассматриваемого вида, проведенный ГСУ ГУ МВД России по Саратовской области[28], показал, что следователи органов внутренних дел при возбуждении перед судами ходатайства в выносимых постановлениях затребуют не исчерпывающий перечень информации, позволяющий впоследствии установить местонахождение подозреваемого лица по месту «выхода в эфир» абонентского устройства (сотового телефона с установленным абонентским номером, либо по установленному IMEI-номеру телефона (абонентского устройства)).

Следует согласиться с мнением авторов указанных методических рекомендаций, что для установления места нахождения подозреваемого лица не достаточно получить информацию о номере и месте расположения приемопередающей базовой станции. Зачастую, наблюдаются случаи, что при «выходе в эфир» абонентского устройства (телефона), с которого лицо совершает преступные действия, услуги связи оказываются через базовую станцию, расположенную на большем удалении при наличии иных близлежащих приемопередающих базовых станций. Это объясняется следующими факторами. Емкость каждой приемопередающей базовой станции определятся двумя факторами:

азимут (в градусах) – угол разворота станции относительно сторон света (Север, Юг, Запад, Восток; при этом показатели Севера – 0^{o}, либо $360^{o,}$ Запад – 90^{o}, Юг – 180^{o}, Запад – 270^{o}; иные показатели градусов устанавливаются, исходя из данной градации);

ширина направленности диаграммы антенны (измеряются в Мегагерцах).

[28] Методические рекомендации «Тактика и методика раскрытия преступлений по фактам хищения денежных средств граждан с банковских счетов, совершенных в системе дистанционного банковского обслуживания, посредством использования всемирной сети Интернет, средств мобильной связи, IT-технологий», подготовлены ГСУ ГУ МВД России по Саратовской области // Материалы предоставлены Следственным департаментом МВД России.



Условные обозначения:

– базовая станция № 1 с азимутом А: 90°, расположенная на большем удалении;

– базовая станция № 2 с азимутом А: 180°, расположенная в наименьшем удалении от места происшествия (близлежащая);

– место происшествия.

Кроме того, по мнению авторов, существенным показателем является показатель, имеющий обозначение «LAC» (англ. – location aria cod) – зона с неповторяющимися частотами, на которых излучает приемопередающая базовая станция. При установлении данного показателя, можно объяснить, почему, если место происшествия находится в зоне действия двух приемопередающих базовых станций, покрывающих (охватывающих) одновременно место происшествия, в качестве доказательств берется показания лишь одной (почему не зафиксирован факт выхода в эфир телефона с другой базовой станции, покрывающей место происшествия).

Таким образом, в постановлениях о возбуждении перед судом ходатайства, в порядке, предусмотренном ст. 186.1 УПК РФ, о получении информации о соединениях между абонентами и (или) або-

нентскими устройствами с привязкой к приемопередающим базовым станциям, следователю необходимо конкретизировать запрашиваемую информацию: «Ходатайствовать перед судом о получении информации о соединениях между абонентами и (или) абонентскими устройствами с привязкой к приемопередающим базовым станциям, а именно:

детализации телефонных переговоров с привязкой к приемопередающим базовым станциям абонентского номера (например) «+79111111111» за период с __ часов __ минут до __ часов __ минут __.__.2020 с обязательным указанием номеров приемопередающих базовых станций (CID), местах их расположения (адрес), информации о зоне с неповторяющимися частотами, на которых излучает каждая базовая станция (LAC), азимутах и ширине направленности диаграммы антенны каждой базовой станции;

получении информации в компании сотовой связи ПАО «Наименование организации», с целью установления данных владельца абонентского номера «+79111111111» (по состоянию на __.__.2020), даты заключения с ним договора об оказании услуг, imsi-номере[29] (номерах) данной SIM-карты с абонентским номером «+79111111111», IMEI-номере (номерах) телефона, выходящему в эфир с абонентского номера «+79111111111» с момента начала оказания услуг связи по настоящий момент, а также по состоянию на __.__.2020, обращался ли с __.__.2020 данный владелец с заявлением об изменении абонентского номера телефона (если да, то предоставить информацию о новом абонентском номере телефона, imsi-номере SIM-карты с новым абонентским номером телефона)».

При принятии судом решения о получении информации о соединениях между абонентами и (или) абонентскими устройствами его копия направляется следователем в соответствующую осуществляющую услуги связи организацию, руководитель которой обязан предоставить указанную информацию, зафиксированную на любом материальном носителе информации.

Постановление суда о разрешении получения информации о соединениях между абонентами и (или) абонентскими устройствами

[29] imsi-номер – это индивидуальный номер SIM-карты абонентского номера телефона, в случае утери SIM-карты, при обращении клиента в компанию сотовой связи с заявлением о восстановлении номера телефона, ему выдается новая SIM-карта с иным imsi-номером, но тем же абонентским номером телефона. Установление данного imsi-номера позволяет опровергнуть позицию стороны защиты об утере SIM-карты с абонентским номером (на день совершения преступления) и использовании ее не подзащитным, а иным лицом.

направляется следователем в соответствующую организацию, осуществляющую услуги связи, с надлежащим образом оформленным запросом (заверенным гербовой печатью) в порядке, предусмотренном ч. 4 ст. 21 УПК РФ. В запросе необходимо обязательно указать разумные сроки исполнения постановления суда[30], а также разъяснить, что невыполнение законных требований следователя является административным правонарушением, ответственность за которое предусмотрена ст. 17.7 КоАП РФ.

Информация о соединениях между абонентами и (или) абонентскими устройствами предоставляется операторами связи в опечатанном виде с сопроводительным письмом, в котором указываются период, за который она предоставлена, и номера абонентов и (или) абонентских устройств.

Получив указанную информацию, следователь должен изучить абонентские номера телефонов, продолжительность переговоров с этих телефонов и другую информацию, которая позволит идентифицировать соответствующего абонента, причастного к совершению преступления. Например, при выявлении звонков подозреваемого лица в банковские учреждения, операторам сотовых компаний, на стационарные телефоны должна быть произведена выемка аудиозаписей таких телефонных разговоров. В целях идентификации (отождествления) голоса звонившего с голосом подозреваемого (обвиняемого) может быть назначена фоноскопическая судебная экспертиза.

Следует отметить, что при наличии сведений о номере приемопередающей базовой станции и информации о зоне с неповторяющимися частотами, на которых излучает базовая станция, место расположения приемопередающей базовой станции возможно установить самостоятельно посредством интернет-ресурса на сайте «Xinit.ru».

Для этого на сайте «Xinit.ru» необходимо открыть «вкладку»: «Местоположение базовых станций», затем заполнить «поля»: MCC – необходимо указать код России – 250; MNC – код оператора сотовой связи (выбрать вкладку с наименованием операторов сотовой связи, при этом у следующих операторов сотовой связи следующие обозначения: «ВымпелКоммуникации (Билайн)» – 99, МТС – 01, ПАО «Ме-

[30] Так, например, в практическом пособии следователя по расследованию уголовных дел о хищениях, совершенных дистанционным способом со сборником типовых запросов направляемых при расследовании уголовных дел указанной категории, подготовленным ГСУ ГУ МВД России по Кемеровской области, говорится об исполнении такого запроса в течение 10 суток с момента его получения // Материалы предоставлены Следственным департаментом МВД России.

гаФон» – 02, «TELE-2» – 20, «Ростелеком» – 39; LAC – известные параметры; CID – ID (идентификационный номер) базовой станции[31].

Необходимо отметить, что в соответствии с ч. 4 ст. 44 Федерального закона от 7 июля 2003 г. № 126-ФЗ (в ред. от 9 марта 2021 г.) «О связи», абонент имеет право сохранить абонентский номер в пределах территории, определенной Правительством Российской Федерации, при условии расторжения действующего договора об оказании услуг связи, погашения задолженности по оплате услуг связи и заключения нового договора об оказании услуг связи с другим оператором связи. При этом операторы связи должны предоставлять информацию о перенесенных абонентских номерах оператору базы данных перенесенных абонентских номеров, которым, в соответствии с распоряжением Правительства РФ от 9 октября 2013 г. № 1832-р «Об операторе базы данных перенесенных абонентских номеров»[32], является федеральное государственное унитарное предприятие «Центральный научно-исследовательский институт связи».

Контроль и запись переговоров (ст. 186 УПК РФ).

Согласно ч. 1 ст. 186 УПК РФ при наличии достаточных оснований полагать, что телефонные и иные переговоры подозреваемого, обвиняемого и других лиц могут содержать сведения, имеющие значение для уголовного дела, их контроль и запись допускаются при производстве по уголовным делам о преступлениях средней тяжести, тяжких и особо тяжких преступлениях на основании судебного решения, принимаемого в порядке, установленном ст. 165 УПК РФ.

При расследовании уголовных дел рассматриваемой категории по преступлениям средней тяжести, тяжким и особо тяжким, возникает необходимость в проверке лица, на чье имя зарегистрирован абонентский номер телефона, с которого осуществлялся звонок потерпевшему, на причастность к совершению преступления, а также установления иных лиц, причастных к совершению указанного преступления.

В связи с этим следователю необходимо в порядке, предусмотренном ст. 186 УПК РФ выйти в суд с ходатайством о контроле и записи телефонных и иных переговоров абонентского номера, с кото-

[31] Методические рекомендации «Тактика и методика раскрытия преступлений по фактам хищения денежных средств граждан с банковских счетов, совершенных в системе дистанционного банковского обслуживания, посредством использования всемирной сети Интернет, средств мобильной связи, IT-технологий», подготовлены ГСУ ГУ МВД России по Саратовской области // Материалы предоставлены Следственным департаментом МВД России.

[32] Собр. законодательства Рос. Федерации. 2013. № 42, ст. 5402 // СПС КонсультантПлюс.

рого осуществлялся звонок на номер телефона потерпевшего, и совершались преступные действия.

Согласно ч. 3 ст. 186 УПК РФ в ходатайстве следователя о производстве контроля и записи телефонных и иных переговоров должно быть указано:

1) уголовное дело, при производстве которого необходимо применение данной меры;

2) основания, по которым производится данное следственное действие;

3) фамилия, имя и отчество лица, чьи телефонные и иные переговоры подлежат контролю и записи;

4) срок осуществления контроля и записи;

5) наименование органа, которому поручается техническое осуществление контроля и записи.

Постановление о производстве контроля и записи телефонных и иных переговоров направляется следователем для исполнения в соответствующий орган.

При этом производство контроля и записи телефонных и иных переговоров может быть установлено на срок до 6 месяцев. Оно прекращается по постановлению следователя, если необходимость в данной мере отпадает, но не позднее окончания предварительного следствия по данному уголовному делу.

Допрос подозреваемого (обвиняемого). При допросе *подозреваемого по факту хищения, совершенного посредством телефонного звонка*, следует выяснять:

факт и обстоятельства (место, время, способы и средства) совершения хищения;

механизм подготовки к совершению преступления;

количество и данные лиц, участвовавших в совершении преступления, наличие предварительного сговора между ними, роль каждого из них и длительность совместных действий;

принципы выбора потерпевшего;

используемый порядок и способ получения денежных средств от потерпевшего;

какими абонентскими номерами пользуется, какие абонентские номера использовал при совершении преступления;

способы сокрытия преступления (уничтожение телефонных аппаратов, SIM-карт, оформление счетов, телефонных номеров на подставных лиц, по подложным документам);

каким образом распоряжался похищенными денежными средствами;

отношение к последствиям преступления;

уровень образования, наличие профессиональных навыков и иные характеризующие его личность данные;

иные обстоятельства, имеющие значение для расследования уголовного дела.

В ходе допроса *подозреваемого по факту хищения, совершенного с использованием информационно-телекоммуникационной сети Интернет (вредоносного программного обеспечения),* помимо вышеуказанного, необходимо выяснить:

насколько подозреваемый хорошо владеет компьютерной техникой и программным обеспечением;

какая компьютерная техника имеется по месту его проживания и работы, кто имеет к ней доступ, ее технические характеристики;

каким образом настроен удаленный доступ к сети для выхода в сеть Интернет (кто и когда производил настройку);

как часто осуществляет выход в сеть Интернет, наиболее часто посещаемые ресурсы;

каким интернет-браузером пользуется при осуществлении выхода в сеть Интернет, каковы его настройки;

установлены ли на компьютере антивирусные или защитные программы, если да, выяснить их наименование;

имеются ли у подозреваемого электронная почта, сайты, домашние страницы, каковы их реквизиты;

каким образом взломана информационная защита компьютера потерпевшего: подбор или хищение ключей и паролей, отключение средств защиты, использование несовершенства защиты;

иные обстоятельства, имеющие значение для расследования уголовного дела.

В соответствии с ч. 1–6 ст. 115 УПК РФ следователем с согласия руководителя следственного органа на основании судебного решения может быть применена ***иная мера процессуального принуждения – наложение ареста на имущество***.

Согласно ч. 3 ст. 115 УПК РФ арест может быть наложен на имущество, находящееся у других лиц, не являющихся подозреваемыми, обвиняемыми или лицами, несущими по закону материальную ответственность за их действия, если есть достаточные основания по-

лагать, что оно получено в результате преступных действий подозреваемого, обвиняемого.

При наложении ареста на принадлежащие подозреваемому, обвиняемому денежные средства и иные ценности, находящиеся на счете, во вкладе или на хранении в банках и иных кредитных организациях, операции по данному счету прекращаются полностью или частично в пределах денежных средств и иных ценностей, на которые наложен арест. Руководители банков и иных кредитных организаций обязаны предоставить информацию об этих денежных средствах и иных ценностях по запросу суда, а также следователя на основании судебного решения (ч. 7 ст. 115 УПК РФ).

При наложении ареста на денежные средства, находящиеся на счете, во вкладе или на хранении в кредитных организациях следует учитывать положения ст. 26, 27 Федерального закона от 2 декабря 1990 г. № 395-1 (ред. от 30 декабря 2021 г.) «О банках и банковской деятельности».

При наличии достаточных данных арест может налагаться на денежные средства иных юридических лиц (индивидуальных предпринимателей), на счета которых необоснованно поступили похищенные денежные средства (например, в целях обналичивания). В данном случае возникает проблема установления, какая часть денежных средств, находящаяся на счетах организации является похищенной. В этих целях необходимо получить сведения о движении денежных средств по счетам такого юридического лица, исследовать платежные документы о поступлении средств на расчетный счет, особое внимание обратив на основание платежа, наименование плательщика, дату перечисления суммы платежа.

IV. НАЗНАЧЕНИЕ И ПРОИЗВОДСТВО СУДЕБНЫХ ЭКСПЕРТИЗ

По уголовным делам о преступлениях рассматриваемой категории может быть назначена *судебная компьютерная экспертиза*[33] (ст. 195 УПК РФ).

Основанием для назначения данной экспертизы является необходимость исследования:

информации, имеющейся в компьютере;

данных о действиях пользователя и возможности совершения определенных действий с помощью компьютера;

свойств программ и программных продуктов;

фактических обстоятельств совершения преступления с использованием компьютера.

Объектами судебной компьютерной экспертизы помимо персонального компьютера (ноутбука, планшетного компьютера) могут выступать мобильный телефон (смартфон), накопители информации (флеш-карты, жесткие диски, CD и DVD диски и пр.), а также хранящаяся в компьютере информация, например, о действиях пользователя, связанных с процессом обработки файлов, передачи данных и т.п., отдельные технические средства и устройства компьютера, системы обработки информации в целом.

При назначении экспертизы для правильной постановки вопросов необходимо предварительно обсудить с экспертом перечень вопросов, подлежащих разрешению, а также достаточность представляемых на исследование материалов.

На разрешение эксперта могут быть поставлены следующие основные вопросы:

1. Имеется ли на накопителе на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, информация о том, что пользователь осуществлял работу

[33] Приказ МВД России от 29 июня 2005 г. № 511: ред. от 27 июня 2019 г. «Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (вместе с «Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», «Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации») // Бюллетень нормативных актов федеральных органов исполнительной власти. 2005. № 35.

на персональном компьютере в определенный период времени (указывается дата и время)?

2. Если да, то когда (указать временные отметки) и с какими программами и файлами, периферийным оборудованием работал пользователь в указанный период времени?

3. Возможно ли осуществление доступа к сети Интернет с использованием представленного на исследование компьютерного средства? Если да, то каким образом осуществлялся доступ?

4. Имеются ли сведения о работе пользователей представленного компьютерного средства в сети Интернет? Каково содержание установок удаленного доступа и протоколов соединений?

5. Имеется ли на накопителе на жестком магнитном диске системного блока персонального компьютера (в памяти мобильного телефона), представленного на исследование, информация об осуществлении сеансов доступа к сети Интернет за период с … по …, в том числе с использованием учетных данных …? Если да, то, какие учетные данные использовались для выхода в сеть Интернет? В каких файлах содержатся сведения об использовавшихся логинах и паролях?

6. Какие программы установлены в автоматическую загрузку в оперативной системе на предоставленном на исследование носителе информации?

7. Имеется ли на представленных на исследование объектах программное обеспечение, способное осуществлять без ведома пользователя уничтожение, блокирование, модификацию, копирование компьютерной информации либо нейтрализацию средств защиты компьютерной информации, следы исполнения которого содержатся на этих объектах? Если такое программное обеспечение имеется, то какими функциональными возможностями оно обладает, когда и каким образом оно появилось на объекте, каковы следы его использования?

8. Имеется ли на представленных на исследование объектах программное обеспечение, используемое для удаленного управления устройством (например, компьютером), а также следы доступа, либо попыток осуществления доступа к устройству (например, к компьютеру) с помощью данного программного обеспечения? Когда и каким образом оно появилось на объекте, каковы следы его исполнения?

9. Имеется ли на накопителе на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, программное обеспечение, позволяющее пользоваться

услугами электронной почты? Если да, то, какое программное обеспечение (название, версии)?

10. Имеются ли на накопителе на жестком магнитном диске системного блока персонального компьютера, представленного на исследование, файлы, содержащие электронные почтовые сообщения? Каков адрес электронного почтового ящика, на который получены входящие сообщения?

11. Имеются ли на представленном на исследование носителе информации сведения о человеке с ФИО (доступ к социальным сетям, переписка, паспортные данные и т.д.)? Если да, то каковы атрибуты соответствующих файлов их содержащих?

12. Имеются ли в дампе оперативной памяти сведения о запущенных процессах, сетевых соединениях? Если да, то какие?

13. Имеются ли в дампе сетевого трафика сетевые соединения от/к следующим IP-адресам (перечисление IP-адресов)?

14. Какие MAC-адреса имеет сетевое оборудование представленных на экспертизу объектов?

При назначении компьютерной экспертизы средств мобильной связи (мобильного телефона, смартфона, планшетного компьютера, оборудованного слотом для использования SIM-карты (модуль идентификации абонента)) перед экспертом могут быть поставлены вопросы, позволяющие:

установить номер IMEI (международный идентификатор мобильного оборудования, состоящий из 15 цифр) телефона (смартфона, планшетного компьютера) в привязке к SIM-карте, установленной в данном устройстве (при регистрации устройства в сотовой сети происходит привязка информации оператора связи, содержащейся на SIM-карте к IMEI устройства, позволяющий идентифицировать владельца SIM-карты (абонента), по номеру IMEI устройства, и наоборот, информация привязки «SIM-карта-IMEI» позволяет установить все IMEI номера устройств, работавших в паре с данной SIM);

определить и скопировать всю содержащуюся в памяти устройства информацию (номера из абонентской книжки, СМС-сообщения, последние набранные номера, входящие вызовы, фото, видео файлы и пр.);

определить и скопировать информацию из чатов (переписка с помощью мгновенных сообщений (WhatsApp, Viber) как текстовых,

так и пересылаемых фото и видео файлов), по содержанию которых можно установить обстоятельства совершения преступления[34].

При назначении судебной компьютерной экспертизы по конкретному уголовному делу могут быть сформулированы и другие вопросы, способствующие установлению фактов и обстоятельств, имеющих доказательственное значение.

Обналичивание (снятие со счета) похищенных у потерпевшего денежных средств может быть совершено с использованием банкоматов, расположенных в торговом или ином помещении, где ведется видеонаблюдение. В целях идентификации (отождествления) личности по признакам внешности назначается *портретная судебная экспертиза*. Объектами данной экспертизы являются фотографические снимки и кадры видеозаписи.

При назначении портретной судебной экспертизы на разрешение эксперта могут быть поставлены следующие вопросы:

1. Пригодны ли для сравнительного идентификационного исследования представленные фотографические снимки (кадры видеозаписи)?

2. Одно или разные лица изображены на видеозаписи и фотографическом снимке?

3. Изображено ли на представленном фотографическом снимке (кадре видеозаписи) конкретное лицо?

В некоторых случаях может возникнуть необходимость в получении экспериментальных образцов (фотоснимков). Для этого производится фотографирование отождествляемого лица, по возможности в ракурсе (позе, с мимикой), схожем с тем, который отражен на исследуемом фотографическом снимке (кадре видеозаписи).

В случае постановки перед экспертом вопросов, связанных с установлением конкретного лица, в постановлении о назначении экспертизы следует, исходя из ситуации, указать известные следователю сведения о: лице, изображенном на фотоснимке, кадре видеозаписи (пол, возраст, национальность и т.п.); сходстве внешних его черт с родственниками; наличии у него близнеца; об изменении признаков внешности лица, возникших в результате травм или болезни либо пластических операций, и т.д.; времени и месте изготовления иссле-

[34] См.: Методические рекомендации «Особенности расследования дознавателями преступлений по фактам совершения мошеннических действий с использованием мобильных средств связи, путем перевода денежных средств со счетов банковских карт потерпевших на счета третьих лиц», подготовленные авторским коллективом НИЦ № 5 ФГКУ «ВНИИ МВД России». 2017.

дуемого фотоснимка; условиях его хранения, обстоятельствах появления в уголовном деле и т.п.[35]

При выявлении (например, в ходе проведенного осмотра информации о соединениях между абонентами и (или) абонентскими устройствами) звонков подозреваемого лица в банковские учреждения, операторам сотовых компаний, на стационарные телефоны должна быть произведена выемка аудиозаписей таких телефонных разговоров. В целях идентификации (отождествления) голоса звонившего с голосом подозреваемого (обвиняемого) назначается *фоноскопическая судебная экспертиза*.

Объектами данной экспертизы являются аналоговые (на магнитной ленте, кассете, микрокассете, видеокассете) и цифровые носители (на магнитном или электронном носителе), содержащие фонограммы устной речи, устройства для передачи и записи звука, которые должны быть надлежащим образом (исключающим их размагничивание в процессе транспортировки) упакованы и опечатаны.

В постановлении о назначении фоноскопической судебной экспертизы в обязательном порядке должны быть воспроизведены из материалов уголовного дела и описаны технические средства и условия проведения звукозаписи; четко указаны границы и местонахождение на представляемом носителе каждой подлежащей исследованию фонограммы (с указанием начальных 2–3 слов текста и конечных 2–3 слов текста, времени звучания).

Для решения вопроса об идентификации лица по голосу и речи в распоряжение эксперта предоставляются сравнительные его образцы голоса и речи.

Свободными образцами речи (которые по времени и характеру не связаны с назначением и производством данной экспертизы) являются, например, фонограммы личного характера и т.д.

В качестве условно свободных образцов голоса и речи могут быть представлены фонограммы допросов, очных ставок и иных следственных действий, в ходе которых применяется звукозапись (в порядке, установленном ст. 189 УПК РФ).

Основные требования, предъявляемые к представляемым в качестве сравнительных образцов фонограммам:

несомненность их происхождения от конкретного лица;

[35] См.: Муженская Н.Е. Экспертиза в российском законодательстве. Руководство-справочник для следователя, дознавателя, судьи. М.: Проспект, 2014. С. 180–181.

хорошее качество и представительность (как по объему (продолжительностью не менее 10–15 минут), так и по характеру речевого материала).

При назначении фоноскопической судебной экспертизы на разрешение эксперта могут быть поставлены следующие вопросы:

1. Пригодны ли для идентификации говорящих по голосу и речи записи (указывается местонахождение подлежащей исследованию фонограммы на представляемом носителе, описывается тип носителя записи)?

2. Имеются ли на фонограмме (указывается местонахождение подлежащей исследованию фонограммы на представляемом носителе) голос и речь лица (указываются фамилия и инициалы), чьи образцы представлены на диске (описывается тип носителя записи)? Если имеются, то какие реплики, слова или фразы им произнесены?

3. Каково дословное содержание разговора, записанного на фонограмме (указывается тип носителя звукозаписи и описывается местонахождение фонограммы; указываются словесные границы фонограммы)?

4. Имеются ли на фонограмме признаки монтажа или иных изменений (например, выборочной фиксации, наложение на записи), привнесенных в процессе или после производства звукозаписи?

В процессе производства предварительного следствия могут быть назначены и иные виды экспертиз, например, судебная почерковедческая экспертиза, судебная дактилоскопическая экспертиза.

V. ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ, СЕТИ ИНТЕРНЕТ И СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

Предупреждение преступлений следователями органов внутренних дел осуществляется в рамках расследования уголовных дел в соответствии с УПК РФ и Инструкцией о деятельности органов внутренних дел по предупреждению преступлений, утвержденной приказом МВД России от 17 января 2006 г. № 19 (ред. от 28 декабря 2021 г.) «О деятельности органов внутренних дел по предупреждению преступлений»[36].

В ч. 2 ст. 73 УПК РФ говорится, что обстоятельства, способствовавшие совершению преступления, подлежат выявлению. При производстве по уголовному делу выявление таких обстоятельств позволяет следователю правильно определить меры по их устранению и предупредить совершение новых преступлений.

В соответствии с ч. 2 ст. 158 УПК РФ следователь (руководитель следственного органа), установив в ходе досудебного производства по уголовному делу обстоятельства, способствовавшие совершению преступления, вносит в соответствующую организацию или соответствующему должностному лицу представление о принятии мер по устранению указанных обстоятельств или других нарушений закона.

На основании подп. 18.1 Инструкции о деятельности органов внутренних дел по предупреждению преступлений сотрудники следственных подразделений обязаны при расследовании уголовных дел выявить причины и условия, способствовавшие совершению преступления.

Так как в последнее время преступления, совершаемые с использованием банковских карт, сети Интернет и средств мобильной связи, получают все большее распространение, то их предупреждение является одним из приоритетных направлений деятельности органов предварительного следствия.

Анализ следственной практики позволяет выделить ряд причин и условий, способствующих совершению данных преступлений.

Так, имеются существенные проблемы и упущения в системе безопасности, обеспечиваемой со стороны *банковских (кредитных) организаций*:

[36] СПС КонсультантПлюс.

недостаточная профилактическая работа с клиентами, например, неразъяснение при получении, замене банковских карт, обращении по вопросам оплаты кредитов и покупок через интернет-приложения, мер предосторожности и порядка действий, в случае поступления информации сомнительного характера;

слабая информационная осведомленность клиентов об особенностях дистанционного банковского обслуживания, услугах, предоставляемых банком с использованием сотовой связи, обстоятельствах при которых банковский счет может быть заблокирован;

неориентированность сотрудников банковских (кредитных) организаций на предупреждение возможных мошеннических действий в отношении граждан пожилого возраста, находящихся без сопровождения (либо с малознакомыми), имеющих намерение снять со счета крупную сумму денежных средств, либо самостоятельно осуществляющих операции на терминалах самообслуживания, размещенных в офисах банка, с получением возможных инструкций от неизвестных лиц посредством сотовой связи;

отсутствие системной работы по удостоверению сотрудниками банков законности и добровольности подачи заявок на оформление кредитных договоров и перевода денежных средств на счета третьих лиц дистанционным способом без личного посещения банка, путем телефонного звонка лицу, подающему заявку с проверкой его личности, паспортных данных, кодовых слов и других необходимых сведений.

Совершению рассматриваемых преступлений также способствуют нарушения требований ст. 44 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи», допускаемые *операторами сотовой связи и уполномоченными ими лицами*.

В частности, нарушения могут касаться:

порядка реализации сим-карт оператора сотовой связи;

порядка подключения и обслуживания абонентов, не подтвердивших свою личность документально (без заключения договора), лиц с вымышленными анкетными и паспортными данными, включая иностранных граждан, которые на территорию Российской Федерации не въезжали;

своевременного приостановления оператором сотовой связи оказания услуг по предоставлению обслуживания абонентского номера.

В связи с этим следователем в адрес оператора сотовой связи должно быть направлено представление, в котором бы предлагалось:

рассмотреть данное представление и довести до сведения руководителей и сотрудников выявленные в ходе предварительного следствия нарушения;

организовать проведение служебной проверки по указанным в представлении фактам нарушений Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»;

рассмотреть вопрос о возможности дальнейшего сотрудничества с лицом, уполномоченным оператором связи, с учетом допущенных нарушений федерального законодательства;

организовать силами оператора сотовой связи проведение мероприятий, направленных на устранение имеющихся недостатков, связанных с ненадлежащей реализацией сим-карт, порядка подключения и обслуживания абонентов, не подтвердивших свою личность документально;

выработать и использовать в деятельности оператора сотовой связи комплекс дополнительных мер, направленных на недопущение выявленных нарушений и обеспечение исполнения лицами, действующими от имени оператора сотовой связи, требований федерального законодательства в части надлежащего порядка регистрации лиц, которым предоставляются абонентские номера и услуга по их обслуживанию (удостоверение личности, заключение индивидуального договора, проверка достоверности предоставленных сведений);

рассмотреть возможность организации необходимого контроля и информирования соответствующего территориального органа внутренних дел сотрудниками службы безопасности оператора сотовой связи в случае установления неоднократной немотивированной смены лицом абонентских номеров в короткий промежуток времени, в целях предупреждения совершения им преступлений.

Одним из важных вопросов противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, является соблюдение требований, предусмотренных п. 2 ч. 1 ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи». Данная норма обязывает операторов сотовой связи хранить на территории Российской Федерации 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.

Не предоставление указанных сведений, либо их предоставление несвоевременно, является основанием для внесения следователем соответствующего представления в адрес оператора сотовой связи.

Совершение рассматриваемых преступлений может быть связано с использованием IP-телефонии, доменных имен, серверного оборудования и иных ресурсов сети Интернет. Организации-провайдеры, осуществляющие услуги предоставления доступа к сети Интернет на территории Российской Федерации, в целях экономии адресного сетевого пространства, в значительной мере используют технологию NAT[37], которая заключается в объединении большого количества пользователей под одним IP-адресом. При исполнении запросов правоохранительных органов Российской Федерации[38] данными провайдерами не предоставляются сведения о конкретных пользователях, ссылаясь на отсутствие технической возможности, что противоречит ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи».

Таким образом, в работе рассмотрены основные вопросы, возникающие при возбуждении и расследовании уголовных дел о хищениях, совершенных с использованием банковских карт, сети Интернет и средств мобильной связи.

[37] NetworkAddressTranslation – преобразование сетевых адресов.

[38] Взаимодействие с операторами сотовой связи, интернет-провайдерами и администрациями социальных сетей в настоящее время осуществляется путем направления соответствующих запросов в БСТМ МВД России. Запросы в организации интернет-провайдеров, не относящихся к сотовым операторам, направляются самостоятельно.

СПИСОК ИСПОЛЬЗОВАННЫХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ И ЛИТЕРАТУРНЫХ ИСТОЧНИКОВ

1. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ : ред. от 30 декабря 2021 г. // Собрание законодательства Российской Федерации. 2001. № 52 (ч. I). Ст. 4921. – Текст : электронный.

2. О банках и банковской деятельности : Федеральный закон от 2 декабря 1990 г. № 395-1 : ред. от 30 декабря 2021 г. // Собрание законодательства Российской Федерации. 1996. № 6. Ст. 492. – Текст : электронный.

3. О национальной платежной системе : Федеральный закон от 27 июня 2011 г. № 161-ФЗ : ред. от 2 июля 2021 г. // Собрание законодательства Российской Федерации. 2011. № 27. Ст. 3872. – Текст : электронный.

4. Об оперативно-розыскной деятельности : Федеральный закон от 12 августа 1995 г. № 144-ФЗ : ред. от 30 декабря 2021 г. // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349. – Текст : электронный.

5. О связи : Федеральный закон от 7 июля 2003 г. № 126-ФЗ : ред. от 30 декабря 2021 г. // Собрание законодательства Российской Федерации. 2003. № 28. Ст. 2895. – Текст : электронный.

6. Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность : постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 : ред. от 25 сентября 2018 г. // Собрание законодательства Российской Федерации. 2005. № 36. Ст. 3704. – Текст : электронный.

7. Об утверждении Правил хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи : постановление Правительства Российской Федерации от 12 апреля 2018 г. № 445 : ред. от 28 мая 2019 г. // Собрание за-

конодательства Российской Федерации. 2018. № 17. Ст. 2489. – Текст : электронный.

8. Об операторе базы данных перенесенных абонентских номеров : распоряжение Правительства Российской Федерации от 9 октября 2013 г. № 1832-р // Собрание законодательства Российской Федерации.2013. № 42. Ст. 5402. – Текст : электронный.

9. Об утверждении Инструкции по организации информационного обеспечения сотрудничества по линии Интерпола : приказ МВД РФ № 786, Минюста РФ № 310, ФСБ РФ № 470, ФСО РФ № 454, ФСКН РФ № 333, ФТС РФ № 971 от 6 октября 2006 г. (ред. от 22 сентября 2009 г.) // Бюллетень нормативных актов федеральных органов исполнительной власти. № 47. 20.11.2006. – Текст : электронный.

10. Вопросы организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации» (вместе с «Инструкцией по организации производства судебных экспертиз в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации», «Перечнем родов (видов) судебных экспертиз, производимых в экспертно-криминалистических подразделениях органов внутренних дел Российской Федерации») : приказ МВД России от 29 июня 2005 г. № 511 : ред. от 27 июня 2019 г. // Бюллетень нормативных актов федеральных органов исполнительной власти. № 35. 2005. – Текст : электронный.

11. О деятельности органов внутренних дел по предупреждению преступлений» (вместе с «Инструкцией о деятельности органов внутренних дел по предупреждению преступлений») : приказ МВД России от 17 января 2006 г. № 19 : ред. от 28 декабря 2021 г. // СПС КонсультантПлюс. – Текст : электронный.

Акты судебных органов

12. Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-процессуального кодекса Российской Федерации : определение Конституционного Су-

да Российской Федерации от 25 января 2018 г. № 189-О // СПС КонсультантПлюс. – Текст : электронный.

13. О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ) : постановление Пленума Верховного Суда Российской Федерации от 1 июня 2017 г. № 19 // Бюллетень Верховного Суда Российской Федерации. № 7. 2017. – Текст : электронный.

14. Апелляционное постановление Тверского областного суда № 22-1501/16 22К-1501/2016 от 29.06.2016 по делу № 22К-1501/2016 URL : https://sudact.ru/regular/doc/Cg2haahb1SHr/ (дата обращения : 14.02.2021). – Текст : электронный.

Юридическая литература

15. Тактика и методика раскрытия преступлений по фактам хищения денежных средств граждан с банковских счетов, совершенных в системе дистанционного банковского обслуживания, посредством использования всемирной сети Интернет, средств мобильной связи, IT-технологий : методические рекомендации, подготовлены ГСУ ГУ МВД России по Саратовской области // Материалы предоставлены Следственным департаментом МВД России. – Текст : непосредственный.

16. Особенности расследования дознавателями преступлений по фактам совершения мошеннических действий с использованием мобильных средств связи, путем перевода денежных средств со счетов банковских карт потерпевших на счета третьих лиц : методические рекомендации, подготовленные авторским коллективом НИЦ № 5 ФГКУ «ВНИИ МВД России», 2017. – Текст : непосредственный.

17. Муженская, Н. Е. Экспертиза в российском законодательстве : руководство-справочник для следователя, дознавателя, судьи / Н. Е. Муженская. – Москва : Проспект, 2014. – 744 с. – Текст : непосредственный.

18. Практическое пособие следователя по расследованию уголовных дел о хищениях, совершенных дистанционным способом со сборником типовых запросов направляемых при расследовании уго-

ловных дел указанной категории, подготовленным ГСУ ГУ МВД России по Кемеровской области // Материалы предоставлены Следственным департаментом МВД России. – Текст : непосредственный.

19. Состояние преступности в России за январь – декабрь 2020 года. ФКУ «ГИАЦ МВД России». Москва : 66 с. – Текст : непосредственный

20. Состояние преступности в России за январь – декабрь 2021 года. ФКУ «ГИАЦ МВД России». Москва : 66 с. – Текст : непосредственный

ОГЛАВЛЕНИЕ

План-график ВНИИ МВД России, 2022, поз. 14

Рязанцев Василий Анатольевич

ВОЗБУЖДЕНИЕ И РАССЛЕДОВАНИЕ УГОЛОВНЫХ ДЕЛ О ХИЩЕНИЯХ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ БАНКОВСКИХ КАРТ, СЕТИ ИНТЕРНЕТ И СРЕДСТВ МОБИЛЬНОЙ СВЯЗИ

Практическое пособие

Редактор *И. П. Кульпа*
Компьютерная верстка *С. В. Первовой*

Подписано в печать 26.10.2022 Тираж 150 экз.
Формат 60Х84 1/16 Печ. л. 4,25 Уч.-изд. л. 3,5 Заказ № 36

Издатель: ФГКУ «ВНИИ МВД России»
121069, Москва, ул. Поварская, д. 25, стр. 1

Группа ОП РИО ФГКУ «ВНИИ МВД России»