МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ДЕПАРТАМЕНТ
ГОСУДАРСТВЕННОЙ СЛУЖБЫ И КАДРОВ

Н.А. Жукова, Ю.А. Ковтун,
И.А. Жуков, А.В. Лагуточкин

РАССЛЕДОВАНИЕ И РАСКРЫТИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ ПОСРЕДСТВОМ SMS-СООБЩЕНИЙ

Методические рекомендации

Москва
2014

Жукова Н.А. Расследование и раскрытие преступлений, совершенных посредством sms-сообщений: методические рекомендации / Н.А. Жукова, Ю.А. Ковтун, И.А. Жуков, А.В. Лагуточкин. – М.: ДГСК МВД России, 2014. – 48 с.

Рецензенты: **Матвеева Н.В.,** кандидат юридических наук, доцент: **Шихов П.И.,** кандидат юридических наук, Заслуженный юрист Российской Федерации (Санкт-Петербургский университет МВД России);
Алябьев А.А. (УМВД России по г. Белгороду).

В методических рекомендациях освещены вопросы, касающиеся организации работы следователя, дознавателя, сотрудника уголовного розыска при расследовании и раскрытии мошенничеств с использованием sms-сообщений.

Пособие предназначено для курсантов, слушателей и преподавателей образовательных организаций МВД России.

ОГЛАВЛЕНИЕ

Введение……....

Раздел 1. Некоторые особенности раскрытия преступлений, совершенных посредством sms-сообщений……...

Раздел 2. Расследование преступлений, совершенных посредством sms-сообщений……..

Заключение…….

Список литературы……

ВВЕДЕНИЕ

Интенсивное развитие телекоммуникаций и компьютерных технологий является главной чертой нашего времени. Возникшие в 80-х гг. прошлого века беспроводные (мобильные) системы связи, благодаря своим функциональным возможностям, приобрели огромную популярность и распространились по всему земному шару. Однако системы сотовой связи стали привлекательны не только для обычных пользователей, но и для преступных элементов различного рода. Появился новый вид криминальной деятельности, выражающийся в незаконном использовании сетей мобильной связи в целях завладения имуществом абонентов (физических лиц), а также конфиденциальной информацией, циркулирующей в этих системах, и негативном воздействии на их элементы.

Несанкционированный доступ к системам связи стал одной из главных угроз операторам мобильных телекоммуникаций и их абонентам, причиняющий колоссальный материальный ущерб.

Особую опасность среди видов преступлений в сфере телекоммуникационных технологий представляют мошенничества, в том числе с использованием услуг операторов сотовой связи – sms-сообщений. Этим видом деятельности, как правило, занимаются организованные преступные группы, оснащенные техническими средствами, отвечающими последним достижениям научного прогресса.

По данным аналитиков, доходы от указанной преступной деятельности оцениваются наравне с наркоторговлей. В нашей стране отдельной статистики по преступлениям на сетях мобильной связи нет.

Высокая латентность, отсутствие выработанной единой судебной и следственной практики, а также несовершенство российского законодательства в области телекоммуникационных технологий обусловливают существенные трудности в деятельности правоохранительных органов по раскрытию и расследованию фактов мошенничеств, совершаемых с использованием sms-сообщений. Кроме того, учитывая, что указанный аспект деятельности право-

охранительных органов практически не изучен, а также в целях повышения эффективности работы правоохранительных органов по борьбе с данным видом преступлений, требуется формирование, разработка и развитие научного знания, предлагающего действенные рекомендации для выявления, раскрытия и расследований обозначенных преступлений.

Методические рекомендации могут быть использованы при изучении дисциплин «Уголовный процесс», «Криминалистика», «Оперативно-разыскная деятельность».

Раздел 1. Некоторые особенности раскрытия преступлений, совершенных посредством sms-сообщений

Раскрытие преступлений – это деятельность оперативных подразделений ОВД и предварительного следствия по обнаружению признаков преступлений, установлению лиц, их совершивших, и принятию к ним мер, предусмотренных законом. Таким образом, процесс по раскрытию преступлений состоит из трёх основных элементов: выявление и закрепление информации о событии преступления; установление лиц, его совершивших; обеспечение процесса доказывания.

Установление виновных лиц – наиболее сложный элемент в раскрытии преступлений, особенно тех, которые предварительно планируются и совершаются в условиях неочевидности. Большая часть регистрируемых преступлений компетенции уголовного розыска являются неочевидными, т.е. такими, по которым лица, их совершившие, неизвестны.

Обеспечение процесса доказывания как элемент деятельности по раскрытию преступлений предполагает осуществление оперативно-разыскных мероприятий, направленных на обнаружение доказательственной информации, которую крайне затруднительно либо невозможно получить процессуальным путем.

Правовой основой деятельности по раскрытию преступлений служит блок законодательных и ведомственных нормативных актов, определяющих задачи и компетенцию аппаратов уголовного розыска. В своей деятельности сотрудники уголовного розыска обязаны в первую очередь руководствоваться Конституцией Российской Федерации, основами уголовного судопроизводства, Законом РФ «О полиции», Федеральным законом «Об оперативно-розыскной деятельности». Последний Закон определяет основания и условия проведения оперативно-разыскных мероприятий, направленных на раскрытие преступлений.

Характеристика преступлений, совершенных посредством sms-сообщений. Одним из основных видов преступлений, совершенных посредством sms-сообщений, является мошенничество, которое стремительно набирает силу и превращается в настоящую эпидемию. Оградить от мошенников в первую очередь может лишь внимательность и здравомыслие самих граждан. Жертвами мошенников становятся все без исключения – это и бизнесмены, и чиновники, и звезды шоу-бизнеса, и обычные граждане.

Мошенничество является одной из форм хищения, поэтому ему присущи все признаки данного понятия: а) незаконность действий виновного; б) безвозмездность изъятия чужого имущества; в) изъятие имущества и (или) обращение чужого имущества в пользу виновного или других лиц; г) наличие корыстной цели; д) наличие причиненного собственнику или иному владельцу ущерба.

Современное мошенничество, совершаемое посредством sms-сообщений, в целом может быть охарактеризовано следующими признаками:

- преобладание в его структуре преступных действий против личной собственности граждан;

- большое разнообразие способов совершения преступления (обмана) и их чрезвычайная изменчивость, связанная с преобразованиями в социальной и экономической сферах жизни общества;

- неизменный рост материального ущерба от преступной деятельности мошенников за счет все более активного посягательства на ценности граждан;

- высокий уровень групповых мошеннических посягательств (до 90%), высокий уровень организованности;

- межрегиональный и международный характер действий мошенников, раздел сфер преступного влияния, постепенное преобразование мошеннических групп в структурные звенья организованных преступных сообществ;

- отличный по социально-демографическим, уголовно-правовым, нравственно-психологическим характеристикам от среднестатистического корыстного

преступника портрет мошенника, усиление «интеллектуализации» данной криминальной среды за счет привлечения новых участников;

- виктимное, порой неправомерное, поведение значительной части потерпевших;

- высокая латентность данного вида преступления.

Анализ характера действий мошенников позволяет говорить о наличии типичных для большинства мошеннических операций этапах совершения преступления, включающих:

- подготовку к проведению мошеннической операции, в том числе разработку схемы операции, осуществление необходимых организационных и технических мероприятий;

- непосредственное осуществление обманных действий;

- присвоение похищенного имущества;

- уклонение от ответственности.

Мошенничество совершается всегда открыто для потерпевшего, но связано с введением его в заблуждение относительно тех или иных фактических обстоятельств. При этом обман обнаруживается, как правило, не сразу, а через определенный период времени, позволяющий не только полностью завладеть денежными средствами, но и быть недоступными для обнаружения.

Рассмотрение способов и приемов обмана в сфере сотовой связи имеет определенное практическое значение. Например, изучение приемов обмана дает возможность создать более полное представление о личности мошенника, его интеллектуальных качествах, что важно для прогнозирования возможной линии поведения преступника на различных стадиях совершения преступления и предварительного следствия. Кроме того, нужно принять во внимание, что обман может осуществляться не только путем передачи информации, полностью не соответствующей действительности. Ложь может быть «разбавлена» элементами правды (например, когда мошенник действительно имеет возможность оказать услугу, о которой его просит потерпевший). В таких случаях ана-

лиз ситуации преступления окажет помощь в правильной оценке действий виновного.

По данным пресс-службы Управления «К» МВД России существует несколько видов телефонного мошенничества.

Случай с родственником. Мошенник представляется родственником или знакомым и взволнованным голосом сообщает, что задержан сотрудниками полиции за совершение того или иного преступления (совершил ДТП, хранение оружия или наркотиков, нанесение тяжких телесных повреждений). Далее в разговор вступает якобы сотрудник полиции. Он уверенным тоном сообщает, что уже не раз помогал людям таким образом. Но если раньше деньги привозили непосредственно ему, то сейчас так делать нельзя, так как он боится потерять погоны. Деньги необходимо привезти в определенное место или передать какому-либо человеку. Цена решения вопроса составляет сумму от одной до тридцати тысяч долларов США.

При совершении мошенничества данным способом звонящий абонент может находиться как в исправительном учреждении, так и на свободе, но при этом всегда имеет одного или нескольких сообщников. Основной фигурант, если он на свободе, обычно находится в съемной квартире и, используя мобильный телефон, осуществляет перебор номеров по возрастанию либо убыванию последней цифры. И если раньше звонки осуществлялись на мобильные телефоны с прямым абонентским номером, то в настоящее время это и прямые, и федеральные, и городские номера. Если абонент согласился привезти деньги, то ему называют адрес, куда он должен приехать. По приезду на данный адрес ему сообщают еще один адрес, но при этом он уже попадает под наблюдение сообщников преступника. Люди, осуществляющие наблюдение, осведомлены о методах наблюдения и контрнаблюдения, имеют хороший опыт управления автотранспортом. После того как гражданин оставляет деньги в указанном месте или кому-то их передает, ему сообщают, где он может увидеть своего родственника или знакомого.

Розыгрыш призов. На мобильный телефон абонента звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем (телефон, ноутбук, автомобиль) в лотерее, организованной радиостанцией и оператором мобильной связи. Чтобы получить приз, необходимо в течение минуты дозвониться на радиостанцию.

Перезвонившему абоненту отвечает сотрудник «призового отдела» и подробно объясняет условия игры: просит представиться и назвать год рождения; грамотно убеждает в честности акции (никаких взносов, переигровок и т.д.); спрашивает, может ли абонент активировать на свой номер карты экспресс-оплаты на сумму 300 долларов; объясняет, что в течение часа необходимо подготовить карты экспресс-оплаты любого номинала на указанную сумму и еще раз перезвонить для регистрации и присвоения персонального номера победителя, сообщает номер; поясняет порядок последующих действий для получения приза: с 10.00 до 20.00 такого-то числа абоненту необходимо с паспортом, мобильным телефоном и присвоенным персональным номером прибыть по указанному адресу для оформления радостного события.

Если по каким-то причинам абонент не сможет в течение часа найти экспресс-карты на 300 $, то все равно должен позвонить для согласования дальнейших действий. Затем мошенник объясняет порядок активации карт: стереть защитный слой; позвонить в призовой отдел; при переключении на оператора - сообщить свои коды. Оператор их активирует на номер абонента, а призовой отдел контролирует правильность его действий, после чего присваивает ему персональный номер «победителя», с которым гражданин должен ехать за призом. Предложение самостоятельно активировать карты на свой номер и приехать с доказательными документами из сотовой компании не принимается, таковы правила рекламной акции.

СМС-просьба. Абонент получает на мобильный телефон сообщение «У меня проблемы, позвони по такому-то номеру, если номер недоступен, положи на него определенную сумму и перезвони».

Платный код. Поступает звонок якобы от сотрудника службы технической поддержки оператора мобильной связи с предложением подключить новую эксклюзивную услугу или для перерегистрации во избежание отключения связи из-за технического сбоя, или для улучшения качества связи. Для этого абоненту предлагается набрать под диктовку код, который является комбинацией для осуществления мобильного перевода денежных средств со счета абонента на счет злоумышленников.

Штрафные санкции оператора. Злоумышленник представляется сотрудником службы технической поддержки оператора мобильной связи и сообщает, что абонент сменил тарифный план, не оповестив оператора (также могут быть варианты: не внес своевременную оплату, воспользовался услугами роуминга без предупреждения) и, соответственно, ему необходимо оплатить штраф в определенном размере, купив карты экспресс-оплаты и сообщив их коды.

Ошибочный перевод средств. Абоненту поступает sms-сообщение о поступлении средств на его счет, переведенных с помощью услуги «Мобильный перевод». Сразу после этого поступает звонок и мужчина или женщина сообщает, что ошибочно перевел деньги на его счет и просит вернуть их обратно тем же «Мобильным переводом».

Предложение получить доступ к sms-переписке и звонкам абонента. Зная склонность некоторых граждан «пошпионить» за близкими и знакомыми, злоумышленники придумали очередной способ мошенничества в Интернете. Пользователю предлагается изучить содержание sms-сообщений и список входящих и исходящих звонков интересующего абонента. Для этого необходимо отправить сообщение стоимостью от 10 до 30 руб. на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента. После того, как пользователь отправляет sms, с его счета списывается сумма гораздо большая той, что была указана мошенниками - до 500 руб., а интересующая информация так и не поступает. Поскольку большинство пострадавших не обращается в полицию в связи с незначительностью ущерба, мошенники остаются безнаказанными и продолжают обманывать граждан.

Мошенничество с использованием коротких номеров. В настоящее время широкое распространение на всей территории России получили мошеннические действия, связанные с использованием сервисов так называемых коротких номеров. Данный вид противоправных деяний стремительно развивается, приобретает все новые формы и, как показывает практика, наносит материальный ущерб доверчивым гражданам. Существует несколько способов совершения этого преступления.

Распространение вредоносных программ. Через сеть Интернет распространяются различные вредоносные программы, блокирующие операционную систему ПК, с предложением ее разблокирования посредством отправки sms-сообщений на «короткий» номер. Как правило, стоимость sms-сообщений злоумышленниками не указывается, либо указывается заведомо заниженная в разы стоимость. В ряде случаев на информационном табло (баннере), появляющемся после блокировки, имеется ссылка с указанием реальной стоимости sms-сообщения (как правило, колеблется от 300 до 600 рублей за разблокирование одного компьютера). После отправки sms-сообщений возможны два варианта развития событий: действительно будет выслан код, с помощью которого работа ПК возобновится, либо, несмотря на списание со счета некоторой суммы спасительный код так и останется неизвестным. В настоящее время достигнута договоренность с операторами мобильной связи о внедрении сервисов по информированию абонентов о принадлежности короткого номера и реальной стоимости sms-сообщения на данный номер; компания «МТС» уже предоставляет данную услугу.

Предложение псевдоуслуг и псевдопрограмм. На различных сайтах предлагаются несуществующие услуги и программное обеспечение, обладающее совершенно невероятными свойствами (перехватчики sms-сообщений интересующего вас абонента; мобильные сканеры, якобы «раздевающие» человека, на которого направлена камера мобильного телефона, программы, позволяющие читать, что пишут о тебе пользователи различных социальных сетей, и другие подобные услуги и ПО). Также на различных интернет-ресурсах гражданам

предлагается пройти всевозможные тесты, порой совершенно анекдотичные (например, онлайн-тест на беременность), предсказать будущее.

Оплата этих псевдоуслуг также осуществляется посредством sms-сообщений. Вместо ожидаемых услуг граждане получают игровые приложения. Несмотря на пристальное внимание правоохранительных органов, сотовых операторов, агрегаторов коротких номеров, данный вид правонарушений остается весьма и весьма распространенным.

В описанных выше условиях тактика деятельности оперативных аппаратов в значительной степени зависит от исходной информации, которая является основанием для принятия оперативно-разыскных мер по раскрытию преступления, а также от вида противоправного деяния. В данном разделе рассмотрим отдельные особенности тактики раскрытия рассматриваемых преступлений в связи с ее закрытым регламентированием ведомственными актами.

Исходя из полученной информации, процесс раскрытия sms-мошенничества складывается из следующих этапов:

– реагирование на заявления и сообщения о совершении sms-мошенничества в соответствии с законом и подзаконными нормативными актами (включая проверку, проведение первоначальных оперативно-разыскных мероприятий и неотложных следственных действий);

– проведение общих оперативно-разыскных действий, выдвижение оперативно-разыскных версий и планирование мероприятий по их проверке (если работа по горячим следам не привела к задержанию мошенников);

– поиск, систематизация и использование фактических данных в отношении обоснованно подозреваемых в совершении преступления.

Организация и тактика раскрытия мошенничества зависят от складывающейся на момент поступления заявления ситуации. Здесь возможны две типичные ситуации:

1. В ОВД заявление (сообщение) о совершенном мошенническом действии неизвестными лицами поступило сразу же (через некоторое время) после совершения преступления.

2. В ОВД поступило заявление (сообщение) о лицах, совершающих мошеннические действия посредством sms-сообщений.

Мероприятия, проводимые в первой ситуации, имеют целью, во-первых, преследование и задержание преступника по «горячим следам», а во-вторых, получение информации, необходимой для проведения последующих поисковых либо проверочных действий, а в случае задержания - проведения всех следующих процессуальных действий, необходимых в целях решения стоящих правоохранительных задач.

В рамках реагирования на заявление (сообщение) об sms-мошенничестве проводятся следующие мероприятия:

– опрос потерпевшего;

– опрос лиц, которые могут дать информацию, представляющую интерес для раскрытия и расследования;

– ориентирование о преступлении других органов внутренних дел и общественность;

– осуществление мероприятий, связанных с установлением лица, совершившего данное деяние (изъятие распечатки телефонных номеров переговоров, установление IMEI сотового телефона)[1]. IMEI устанавливается на телефоны во время изготовления на заводе. Он служит для идентификации устройства в сети и хранится в прошивке аппарата. Как правило, IMEI указывается в четырёх местах: на самом аппарате (в большинстве случаев вызывается набором *#06#), под аккумуляторной батареей, на упаковке и в гарантийном талоне. Он играет роль серийного номера аппарата и передаётся в эфир при авторизации в сети;

– задержание и отработка на причастность к совершенному преступлению установленного лица;

– изъятие технических средств для последующего изучения находящейся там информации, в целях доказывания.

---

[1] IMEI - International Mobile Equipment Identity (русск. Международный идентификатор мобильного оборудования) - число (обычно 15-разрядное в десятичном представлении), уникальное для каждого использующего его аппарата. Применяется в сотовых телефонах GSM, WCDMA и IDEN сетей, а также в некоторых спутниковых телефонах.

В процессе опроса потерпевших устанавливаются подробные обстоятельства совершения преступления:

1. Во сколько поступил звонок потерпевшему?

2. Если на сотовый телефон или стационарный телефон с автоматическим определением номера, с какого номера телефона звонили ему?

3. Кем представился преступник, о чем говорил, что предлагал сделать?

4. Какую сумму денежных средств и за какие услуги преступник просил передать ему?

5. Какой способ передачи денежных средств:

а) если блиц-переводом - на чье имя (Ф.И.О.), его адрес?

б) если с нарочным - во сколько подъехали за деньгами, на каком транспортном средстве, описание транспортного средства, запомнили ли государственный номер автомашины, подробное описание человека, который пришел за деньгами, может ли его опознать и составить фоторобот, где осуществлялась передача денег?

в) если положить на счет определенного номера сотового телефона – какой номер сотового телефона?

6. Звонил ли потерпевший повторно преступнику, если да, то о чем говорил с ним, предлагал ли преступник передать ему еще денежные средства, если да, то за какие услуги, сделал ли это потерпевший, если нет, то почему?

При опросе следует уделять внимание получению сведений о деталях общения преступника и потерпевшего, которые могут способствовать установлению мошенников (упоминавшиеся преступниками адреса, организации, номера телефонов и др.).

В зависимости от способа передачи денежных средств последовательность действий оперативного работника можно представить в следующем направлении:

а) если деньги направлены блиц-переводом, необходимо:

– истребовать в ОМВД по месту жительства гражданина, получившего деньги, следующие документы: копию формы 1 для получения паспорта гражданина, получившего деньги, сведения о его судимости, характеристику, копии документов о совершенном потерпевшим блиц-переводе;

– направить шифротелеграмму в ОВД по месту жительства гражданина, получившего деньги, с просьбой опросить его по факту получения денег: по чьей просьбе он получал денежные средства, как познакомился с данным гражданином, как ему объяснили просьбу получения денежного перевода, знал ли он о том, что деньги получены преступным путем, после получения денег кому и каким способом он их передал или переслал;

б) если деньги переданы с нарочным необходимо:

– составить субъективный портрет, направив потерпевшего (совместно) к экспертам для составления фотокомпозиционного портрета преступника, для использования и приобщения к материалам проверки;

– принять меры к розыску автомашины, на которой приезжали за деньгами, а также личности гражданина, который забирал деньги (при этом использовать также содержимое цифровых записей с камер наружного наблюдения юридических лиц);

в) если деньги положили на счет определенного номера сотового телефона, необходимо:

- направить запрос в сотовую компанию с целью установления личности владельца номера sim-карты;

- внести в базу данных информацию о номере sim-карты, на которую положили деньги, установив, что телефон использовался при совершении преступления.

Важным является получение распечатки телефонных номеров переговоров с установлением IMEI сотового телефона или IP-адресов[1] компьютерных и

[1] IP-адрес (ай-пи адрес, сокращение от англ. Internet Protocol Address) - сетевой адрес узла в компьютерной сети, построенной по протоколу IP.

иных устройств связи, которыми пользовались мошенники. При связи через сеть Интернет требуется глобальная уникальность адреса, в случае работы в локальной сети требуется уникальность адреса в пределах сети.

На первоначальном этапе раскрытия важным является временной фактор, ускоряющий процесс обнаружения подозреваемых, поэтому практики чаще прибегают к правовым возможностям самого потерпевшего, который обращается к оператору сотовой связи для установления абонентов, с которыми осуществлялся процесс связи посредством требования детализаций.

Кроме детализации сотрудникам оперативных подразделений необходимо получить от оператора сотовой связи короткий телефонный номер и префикс (в виде цифр или букв, подлежащих размещению в sms-сообщениях), используемый мошенниками. Необходимо иметь в виду, что на одном и том же номере может располагаться множество самых различных продавцов с различными сервисами, а идентификация конкретного продавца производится по префиксу.

После установления необходимых идентификационных номеров технических средств, используемых преступниками, необходимо принять меры к установлению личности владельца номера sim-карты (короткого номера) посредством дачи запросов в организации обслуживания (сотовые или иные операторы, провайдеры). После получения ответа из сотовой компании возникает необходимость в опросе гражданина, на которого зарегистрирована sim-карта (короткий номер), с использованием которой звонили потерпевшему, с обязательным получением информации по следующим вопросам:

– когда, где и при каких обстоятельствах приобрел sim-карту (регистрация короткого номера), используемую преступником?

– где в настоящее время находится данная sim-карта?

– если передал какому-либо лицу когда, где, при каких обстоятельствах, имеются ли установочные данные гражданина, которому была передана sim-карта (кто использует короткий номер), если нет, то почему?

Достаточно важным в определении методики и тактики раскрытия рассматриваемых преступлений остается информация о механизме финансового потока получаемых денежных средств. Так, как известно, крупные операторы сетей (МТС, «Билайн», «Мегафон» и т.п.) с контент-провайдерами никак не связаны, для этого есть особый эшелон агрегаторы. Именно агрегатор резервирует у десятков крупных и мелких сотовых операторов номера (не только в России - на всем постсоветском пространстве), на которые и «садится» потом мошенник с выданным ему префиксом по условленному тарифу. Агрегатор отслеживает потоки sms-сообщений, сортирует их по префиксам и биллингует, то есть начисляет вознаграждение инициаторам трафика тем самым контент-провайдерам.

Агрегаторы, кстати, управляют большими денежными потоками и напрямую с мошенником тоже не связаны. Для этого у них есть партнеры помладше. Они так и называются партнерские программы, или партнерки. Деньги, списанные с баланса телефона за отправку короткого сообщения на платный номер, распределяются в следующих пропорциях: крупные операторы берут себе 30-50%, агрегаторы 7-10%, партнерки чуть больше, остальное идет в карман непосредственному продавцу, подвигнувшему абонента «тряхнуть кошельком». Цепочка выстроена совершенно законно в самой пирамиде «мобильной ответственности» мошеннический компонент не заложен.

Процессуальная задача в данном «караване» отсылок и распределения денежных средств потерпевшего это фиксация посредством: экспертиз, изъятия документов, допроса свидетелей и других процессуальных следственных действий. Все это образует очень сложный механизм доказывания и требует определенной процессуальной специализации лиц, осуществляющих подобные расследования.

Правоохранительные органы не вправе осуществлять выемку в учреждениях связи, получение информации о соединениях между абонентами и (или) абонентскими устройствами без судебного решения.

Конечно, проблемы с установлением идентификационного информационного следа преступников с технической точки зрения весьма сложный процесс, и эта затруднительность вызвана рядом субъективных и объективных факторов. В системе МВД требуются высококвалифицированные кадры, обладающие знаниями в системе информационных технологий. Это направление весьма востребовано большинством современных предприятий и организаций не только на территории России, но и иностранных государств. В то же время, необходимо понимать, что услуги специалистов информационных технологий в современных условиях довольно востребованы, и будет сложно привлечь таких специалистов к решению стоящих правоохранительных задач в условиях жесткой конкуренции спроса профессии. К объективным факторам необходимо отнести уровень оснащенности специальной техникой, который остается на довольно низком уровне.

В тех случаях, когда с момента совершения преступления прошло значительное время, приходится действовать в более сложных ситуациях: усложняется процесс выявления свидетелей, в ряде случаев исключается возможность эффективного исследования вещественных доказательств. Кроме того, в подобных ситуациях проводится проверка причастности к преступлению лиц, которые задержаны за подобное мошенничество в период после совершения раскрываемого преступления. Это происходит во всех случаях, когда первоначальные оперативно-разыскные мероприятия и следственные действия не позволили раскрыть преступление по «горячим следам».

Чаще всего в целях раскрытия данных мошеннических действий проводятся следующие сыскные действия:

– ориентирование конфидентов;

– ориентирование других органов внутренних дел;

– изучение материалов в отношении лиц, могущих совершить подобное мошенничество;

– личный сыск, в том числе в телекоммуникационных сетях;

– изучение прекращенных и приостановленных уголовных дел, а также материалов об отказе в возбуждении уголовного дела по данной категории преступлений;

– изучение сведений о раннее совершенных аналогичных преступлениях, имеющихся в информационных системах МВД, УМВД;

– опросы лиц, доставляемых в органы внутренних дел.

Результаты работы по раскрытию sms-мошенничества зависят от эффективности и своевременности проведения первоначальных поисковых мероприятий. Содержание и направленность первоначальных проверочных действий в каждом конкретном случае может быть различной и зависит от конкретных фактов, изложенных в заявлении или полученной оперативной информации. Основными задачами проводимой проверки являются:

– установление факта и всех обстоятельств совершения преступления (способа совершения обмана, использованных при этом приемов и средств, способов получения и присвоения похищенного);

– получение исходных данных о личности мошенников (в том числе сотрудников потерпевшей стороны, способствовавших достижению мошенниками преступного результата);

– принятие мер к обнаружению и задержанию преступников, в том числе по «горячим следам», если их личности известны или установлены в ходе проверки;

– сбор и фиксация следов и вещественных доказательств;

– установление размеров причиненного ущерба, а при подтверждении первичной информации о совершении мошенничества.

В случаях невозможности установить и задержать мобильных мошенников, кроме уже отработанных на практике оперативно-разыскных мероприятий, следует прибегать к уже зарекомендовавшим себя действиям.

Известно, что sms-мошенниками являются молодые люди, которых можно назвать не просто активными пользователями современных информационных технологий, но скорее всего специалистами в тех или иных направлениях.

Однако им свойственно социальное бахвальство не только в своем кругу, но и в условиях общения в глобальной и иных сетях, в том числе и со случайными пользователями.

Таким образом, в основе поисковой работы становится обязательным проведение разведывательного поиска информации и опросов лиц в представленных сетевых ресурсах.

Однако опрос с точки зрения теории оперативно-разыскной деятельности представляет собой оперативно-разыскное мероприятие, заключающееся в сборе (добывании) информации в процессе непосредственного общения оперативника или по его поручению другого лица с человеком, который осведомлен или может быть осведомлен о лицах, фактах и обстоятельствах, имеющих значение для решения задач ОРД[1]. Но в сфере проблематики нашего пособия следует расширить понятие данного ОРМ, так как тактика его проведения может осуществляться посредством новых информационных технологий и ресурсов:

- Skype (Скайп) – это бесплатное (частное, патентованное) программное обеспечение с закрытым кодом, обеспечивающее шифровальную голосовую связь и создание визуального контакта (видеонаблюдения между пользователями) через Интернет между компьютерами, а также платные услуги для звонков на мобильные и стационарные телефоны. Разработчик Skype Limited(eBay);

- ICQ – (I seek you – Я ищу тебя) централизованная служба мгновенного обмена сообщениями сети Интернет, в настоящее время принадлежащая инвестиционному фонду Mail.ru Group (Россия);

- социальные сети – интерактивный многопользовательский веб-сайт, контент которого наполняется самими участниками сети. Эта автоматизированная социальная среда позволяет общаться группе пользователей, объединенной общими интересами. Крупнейшие сети: Facebook, MySpace (США), Bebo (Великоборитания), Вконтакте, Одноклассники (Российская Федерация) и ряд других европейских сетей.

---

[1] Оперативно-розыскная деятельность: учебник / под ред. К.К. Горяинова, В.С. Овчинского, А.Ю. Шумилова. – М.: Инфра-М, 2008.

- электронная почта (Mail) – технология и предоставляемые ею услуги по пересылке и получению электронных сообщений (называемые «письма» или «электронные письма») по распределенной (в том числе глобальной) компьютерной сети. Для этого необходимо завести свой бесплатный электронный почтовый ящик, зарегистрировавшись на одном из интернет порталов (Mail.ru, Google.ru, Yandex.ru и др.).

Кроме опроса как оперативно-разыскного мероприятия необходимо применять и иные ОРМ с использованием информационных технологий, такие как: наблюдение, проверочная закупка (услуг), оперативный эксперимент (создание искусственно контролируемых условий), снятие информации с технических каналов связи и т.д.

Что касается реагирования оперативных подразделений на поступившие заявления (сообщения) в ОВД о лицах, совершающих мошеннические действия посредством SMS-сообщений, то в данном случае оперативные органы осуществляют проверку с последующей разработкой и реализацией оперативных материалов.

Рассмотрение вопросов документирования, особенности работы с конфидентами, методики и тактики отдельных оперативно-разыскных мероприятий преимущественно регламентируются ведомственными нормативными актами.

В заключение необходимо отметить, что:

– существует объективная необходимость создания единого нормативного акта, регулирующего правоотношения использования средств сотовой связи с внесением изменений в законодательство;

– прозрачность услуг и доступность к информационному ресурсу должны быть обязательными элементами договора с абонентами о предоставлении услуг сотовой связи, а также в договоре необходимо предусмотреть возможность получения согласия (отказа) абонента на мобильную рассылку рекламы и других оповещений;

– мероприятия, проводимые в целях раскрытия преступлений по «горячим следам», имеют целью, во-первых, преследование и задержание преступни-

ка, а во-вторых, получение информации, необходимой для проведения последующих поисковых либо проверочных действий, а в случае задержания – проведения всех следующих процессуальных действий, необходимых в целях решения стоящих правоохранительных задач.

Вопросы для самоконтроля

1. Назовите виды телефонного мошенничества.
2. Какие мероприятия проводятся при поступлении заявления (сообщения) об sms-мошенничестве?
3. Какие обстоятельства устанавливаются в процессе проведения опроса потерпевших?
4. Какие сыскные действия проводятся в целях раскрытия sms-мошенничеств?

Раздел 2. Расследование преступлений, совершенных посредством sms-сообщений

Предварительное расследование – одна из стадий уголовного процесса, самая большая по срокам и количеству составляемых документов часть уголовно-процессуальной деятельности. Именно на этой стадии до суда решаются задачи, которые определяются задачами всего уголовного судопроизводства и вытекают из них. Предварительное расследование направлено на быстрое и полное раскрытие преступлений, обнаружение и изобличение лиц, их совершивших, своевременное привлечение виновных к законной ответственности. Вместе с

тем в ходе расследования выявляются и исследуются все обстоятельства, оправдывающие или смягчающие ответственность обвиняемого.

Предварительное расследование осуществляется путем производства процессуальных действий и принятия процессуальных решений. Оно включает в себя:

- производство следственных действий;

- применение мер процессуального принуждения;

- привлечение лица в качестве обвиняемого;

- допуск к участию в деле защитника, законного представителя, гражданского истца и других субъектов уголовного процесса;

- ознакомление участников с материалами законченного производства при окончании предварительного следствия и т.д.

Н.А. Архипова в ходе исследования следственной практики выявила негативные факторы, влияющие на раскрытие и расследование преступлений данного вида. К таким факторам относятся: бесконтактная передача потерпевшими денежных средств злоумышленникам, несвоевременность обращения граждан в органы внутренних дел о совершенном преступлении, быстрая смена мошенниками абонентских номеров при сокрытии следов преступления, минимальные знания сотрудников органов внутренних дел о механизме образования виртуальных следов при использовании средств мобильной связи, ненадлежащая правовая регламентация взаимодействия между оперативными, следственными подразделениями и операторами связи при раскрытии и расследовании телефонного мошенничества[1].

Особенности производства отдельных следственных действий при расследовании преступлений в сфере мобильных телекоммуникаций рассматривались Г.В. Семеновым, который считает, что информационное содержание мобильного телефона «может быть осмотрено и изъято в порядке обыска и выемки».

---

[1] Архипова Н.А. Организационно-тактические аспекты расследования телефонного мошенничества // Мир юридической науки. 2011. № 5. С. 69.

Для того чтобы установить, в рамках какого следственного действия следует проводить осмотр и изъятие компьютерной информации из мобильного телефона, необходимо определиться с правовым режимом доступа к такой информации.

С учетом нормативного регламентирования доступности представляется возможным выделить четыре вида информации: общедоступная информация; информация, доступ к которой не может быть ограничен; информация, не подлежащая распространению; информация с ограниченным доступом. Для обозначения информации, доступ к которой ограничивается, законодатель использует термин «тайна». Следует установить, имеются ли в мобильном телефоне сведения, отнесенные к различным видам тайны (личная, семейная тайна, коммерческая, служебная, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и т.д.).

Собственники мобильных телефонов используют в них sim-карты для пользования услугами операторов сотовой связи по осуществлению телефонных переговоров, обмена текстовыми сообщениями, изображениями и др. В.Н. Кукарцев и С.Ю. Ударцев, отмечают, что «тайна телефонных переговоров не связана с происхождением и принадлежностью сотового телефона конкретному лицу. В данном случае речь может идти лишь об абонентском номере конкретного потерпевшего...»[1] А.В. Шебалиным было уточнено, что «телефонная трубка в этом случае является предметом обезличенным, т.е. сеть оператора связи производит «узнавание» абонента именно по персональной идентификационной карте, а не по телефонной трубке. Соединения, произведенные абонентом, фиксируются и тарифицируются по sim-карте, независимо от того, в каком телефоне она функционирует»[2].

---

[1] Кукарцев В.К., Ударцев С.Ю. К вопросу о получении детализации телефонных переговоров при раскрытии хищений средств сотовой связи // Актуальные вопросы теории и практики оперативно-розыскной деятельности: материалы международной науч.-практ. конф. (17-18 апреля 2008 г.). – Волгоград, 2008. С. 41-45.

[2] Шебалин А.В. Правовая регламентация получения сведений о соединениях абонентов как важное условие успешного расследования хищений средств сотовой связи // Вестник БЮИ МВД России. 2009. № 2 (17). С. 73-77.

Технические возможности средств мобильной связи таковы, что сохраняют информацию о последних входящих и исходящих вызовах, времени начала и продолжительности соединения пользователя мобильного телефона с номером конкретного абонента, принятые и набранные вызовы. В Определении Конституционного Суда от 2 октября 2003 г. № 345-0 указано, что данные о входящих и исходящих сигналах соединения телефонных аппаратов составляют тайну телефонных переговоров. Анализируя текст данного нормативного документа, мы приходим к выводу, что Конституционный уд, определяя содержание тайны телефонных переговоров, имел в виду сведения, хранящиеся в базах данных оператора сотовой связи. В связи с этим сведения о последних соединениях абонента, имеющиеся в мобильном телефоне, тайной телефонных переговоров не охватываются.

Пользователи мобильных телефонов для удобства использования обычно вводят в память телефонные номера с соответствующими именами, фамилиями и домашними адресами родственников, друзей, коллег, знакомых; сохраняют sms-, ems-, mms-сообщения, осуществляют запись аудио-, фото- и видеоинформации, вносят в органайзер список запланированных встреч с партнерами, значимые события, а также устанавливают технические данные, участвующие в процессе идентификации телефона в сети мобильной связи.

А.М. Ишин и А.Н. Григорьев отмечают, что на сегодняшний день правоприменитель не располагает перечнем персональных данных, поэтому отсутствует реальная возможность обеспечения правовой защиты таких сведений, так как при наличии данного пробела в законодательстве можно говорить о необходимости защиты всего объема сведений, которые охватывают понятие частной жизни лица[1].

Статья 53 ФЗ «О связи» от 7 июля 2003 г. № 126-ФЗ определяет перечень персональных данных об абонентах, входящих в созданную операторами связи базу данных, и закрепляет правовой режим защиты данных сведений. Собст-

[1] Ишин А.М., Григорьев А.Н. Информация и расследование преступлений (технические меры обеспечения информационной защищенности деятельности по расследованию преступлений: научно-практическое пособие / под ред. В.М. Мешкова. – Калининград, 2002. С. 30.

венник мобильного телефона самостоятельно определяет необходимость защиты своей персональной информации в мобильном телефоне. Он может воспользоваться услугами операторов связи по установлению паролей и кодов блокировки sim-карты, что ограничит доступ к определенной информации в мобильном телефоне.

Интересы расследования преступлений обязывают следственные органы знакомиться с содержащейся в средствах мобильной связи персональной информацией. Осмотр и изъятие данной информации из мобильного телефона осуществляется в рамках предварительного расследования. Согласно ст. 161 УПК РФ, следователем или дознавателем, в ходе расследования преступлений, принимаются меры для неразглашения данных предварительного следствия, что является необходимым условием обеспечения законных прав и интересов владельцев мобильных телефонов как обладателей персональных данных, необходимых для расследования уголовного дела.

Таким образом, осмотр информационного содержимого мобильного телефона и изъятие компьютерной информации из него могут быть произведены в ходе следственного действия осмотра предметов и документов.

Общий порядок проведения осмотра предметов и документов подробно раскрыт в криминалистической литературе, поэтому рассмотрим только тактические особенности осмотра средств мобильной связи.

Осмотру подлежат имеющие значение для расследования уголовного дела мобильные телефоны, изъятые в процессуальном порядке путем осмотра места происшествия, обыска или выемки. В соответствии с п. 3 ст. 177 УПК РФ, следователь вправе проводить осмотр предметов и документов не только на месте производства данных следственных действий, но и по месту следствия, если для осмотра потребуется продолжительное время или осмотр на месте затруднен по иным причинам.

Для надлежащего проведения осмотра средств мобильной связи следователю необходимо решить задачи по обеспечению целостности обнаруженной компьютерной информации и по устранению сомнений относительно неизмен-

ности информационного содержимого мобильного телефона. Во время проведения следственного действия даже незначительное изменение компьютерной информации в мобильном телефоне недопустимо.

В ходе проведения осмотра средств мобильной связи следователь и специалист могут использовать как традиционные технико-криминалистические средства обнаружения, предварительного исследования, изъятия и фиксации следов, так и специальную технику, специальное программное обеспечение для доступа, считывания и хранения компьютерной информации.

При планировании следственного действия, в целях сохранения компьютерной информации, следователь должен учитывать, что в момент осмотра может произойти отключение мобильного телефона из-за быстрой разрядки аккумуляторной батареи. В связи с этим следует проверить состояние зарядки мобильного телефона или позаботиться о наличии зарядного устройства, чтобы обеспечить работу мобильного телефона от электросети.

Кроме того, осмотр мобильного телефона вблизи предметов, обладающих сильным электромагнитным излучением, может привести к уничтожению компьютерной информацию. Таким образом, готовясь к следственному осмотру, следователю следует провести мероприятия по обеспечению работы мобильного телефона.

После окончания выполнения комплекса подготовительных действий начинается непосредственное проведение осмотра мобильного телефона, которое осуществляется в два этапа:

1. Внешний осмотр мобильного телефона.

2. Осмотр и изъятие информационного содержания телефона.

Осмотр средства мобильной связи начинается с изучения упаковки. Упаковывают мобильный телефон обычно в коробку (бумажную, пластмассовую, металлическую), в бумажный конверт, в целлофановый пакет и др. В протоколе осмотра указываются материал, из которого изготовлена упаковка, форма, размеры, цвет, наличие надписей, их содержание и расположение, способ нанесения, целостностность, способ опечатывания упаковки.

При внешнем осмотре обращается внимание на общие и индивидуальные признаки мобильного телефона. При описании общих признаков мобильного телефона в протоколе фиксируются: модель, серийный номер, материал, из которого телефон изготовлен, цвет, размер, антенна, конструктивные особенности, характеристика клавиатуры, дисплея с описанием изображения (цветного или черно-белого) на нем, если телефон находится в активном режиме.

При описании индивидуальных признаков в протоколе осмотра должны быть отражены состояние корпуса мобильного телефона, отдельных клавишей, дисплея: потертости, царапины, трещины, отколы. Необходимо обратить внимание на IMEI-номер, указанный на ярлыке, который располагается на корпусе мобильного телефона под аккумуляторной батареей. В случае, если на корпусе телефона имеются наклейки, рисунки, украшения, то отмечается их расположение, содержание, цвет, форма и т.п. Обязательно в протоколе отражаются неисправности каких-либо деталей мобильного телефона, что также фиксируется в протоколе осмотра с указанием соответствующих действий следователя, специалиста и других лиц, участвующих в следственном действии.

Второй этап осмотра состоит в изучении информационного содержания мобильного телефона. Вся компьютерная информация в мобильном телефоне хранится в файлах и представлена в виде текстовой, числовой, графической информации, фотоизображений, видеоклипов и т.д.

При включении мобильного телефона может понадобиться PIN-код, который необходим для доступа к данным, которые имеются в sim-карте. Мобильный телефон может работать, если в него вставить другую sim-карту без PIN-кода. Однако замена sim-карты приведет к уничтожению части компьютерной информации в мобильном телефоне, что является недопустимым действием. Сведения о PIN-коде и PUK-коде содержатся в базе данных компании оператора мобильной связи. Указанные коды блокировки можно получить путем направления запроса оператору связи на соответствующий номер sim-карты.

К разновидностям блокировок мобильных терминалов относятся блокировки региона, блокировки пользования ресурсами сети, блокировки конкретно-

го оператора. В частности, отдельными паролями могут защищаться: услуга запрета вызовов (всех исходящих, междугородних, входящих вызовов и т.д.), клавиатура или отдельные клавиши, голосовая почта и т.д. Следует отметить, что если коды блокировки телефона и sim-карты постоянно активированы, то остальные коды блокировки устанавливаются самим пользователем, в связи с чем вводятся достаточно редко[1].

Если следователю еще до проведения осмотра стало известно, что в мобильном телефоне имеются коды блокировок, то для проведения следственного действия можно пригласить владельца мобильного телефона, которому будет предложено самостоятельно разблокировать свой телефон или заранее уточнить данные коды у владельца мобильного телефона, получив согласие на разблокирование телефона без его участия.

В случае если владелец мобильного телефона отказывается предоставлять информацию о паролях мобильного телефона, а следователю или специалисту в ходе проведения следственного действия установить их не удалось, то осмотр мобильного телефона и sim-карты будет только внешним. Такой осмотр необходим для идентификации мобильного телефона и SIM-карты и направления их на судебную компьютерно-техническую экспертизу.

Исследование информационного содержания мобильного телефона осуществляется следователем или специалистом с помощью русифицированного меню пользователя. Осматривая информацию в мобильном телефоне, следователь или специалист должен пояснять понятым и участвующим лицам каждое свое нажатие на клавиатуру мобильного телефона. Следователю не обязательно полностью отражать в протоколе всю установленную в мобильном телефоне информацию, так как для ее прочтения и фиксации может понадобиться продолжительное время. В то же время интересующая следствие информация записывается подробно, с обязательным указанием последовательности всех действий, произведенных с мобильным телефоном.

---

[1] Абдурагимова Т.И. Основы судебной компьютерно-технической экспертизы. – М., 2004. С. 72.

Первоочередным действием следователя является установление идентификационного номера мобильного телефона, что осуществляется путем нажатия на клавиатуре мобильного телефона комбинации цифр: *#06#. На дисплее можно будет увидеть номер, состоящий из 15 цифр.

Другая техническая информация, участвующая в процессе идентификации телефона в сети мобильной связи (переадресация вызова, запреты на входящие номера, заставки и мелодии на определенные вызовы, возможность подключения телефона к персональному компьютеру для выхода в полноценный Интернет и просмотра своей электронной почты и т.д.), исследуется с участием специалиста. При этом обязательно принимаются меры для непосредственного ознакомления с данной информацией всех участников следственного действия.

Значительную часть данных в мобильном телефоне занимает раздел «Телефонная записная книга», в котором содержатся внесенные пользователем телефонные номера и краткие сведения об их владельцах. Осмотр данной информации позволит установить круг общения пользователя мобильного телефона, его интересы, место работы.

В разделе «Контакты» мобильного телефона отображаются принятые, непринятые, исходящие телефонные номера. Изучение данного раздела дает общее представление о количестве, повторяемости последних местных или междугородних звонков. При описании в протоколе осмотра исходящих и входящих телефонных номеров следует обращать внимание на дату, время начала и продолжительность соединения пользователя мобильного телефона с номером конкретного абонента.

Раздел «Сообщения» содержит сведения о входящих, исходящих sms, mms, ems, голосовых сообщениях и отчет о доставке таких сообщений. Принятые и отправленные сообщения могут содержать текст, иллюстрации, фотографии, звукозаписи. В протоколе следственного действия отображаются сведения об sms-, ems-, mms-сообщениях и их дословное содержание. Сведения об sms-, ems-, mms-сообщениях включают номер, на который они отправлены и с которого они получены, дата и время отправления и получения сообщения.

После осмотра компьютерной информации, содержащейся в средстве мобильной связи, надо установить, какие сведения имеют отношение к расследуемому событию, чтобы использовать их в качестве доказательств по уголовному делу. Данные, содержащиеся на техническом носителе, могут быть использованы в качестве доказательств, если их программными средствами можно преобразовать в форму, пригодную для обычного восприятия и хранения.

Таким образом, при обнаружении в мобильном телефоне интересующей следствие информации необходимо перенести ее на бумажный носитель и оформить как приложение к протоколу следственного действия. В протоколе указывается, какие файлы были распечатаны, на скольких листах, индивидуальные технические характеристики устройств, используемые для распечатки компьютерной информации. В ходе осмотра понятые и все участвующие лица должны видеть, что компьютерная информация на дисплее осматриваемого мобильного телефона и на бумажном носители соответствуют друг другу.

Если мобильный телефон представлен на осмотр с sim-картой, зарядным устройством, коробкой, документами по эксплуатации, то после описания телефона производится осмотр данных предметов. При внешнем осмотре sim-карты отмечается ее номер, цвет, размер, логотип, особые приметы, а затем устанавливается абонентский номер и осматривается сохраненная на ней компьютерная информация. В случае отсутствия сигнала мобильной связи в месте проведения следственного действия, доступ к информации в sim-карте будет невозможен.

По окончании следственного действия необходимо произвести корректное выключение мобильного телефона, о чем обязательно нужно сделать отметку в протоколе. Объекты осмотра заново упаковываются и опечатываются следователем с целью исключить возможность доступа и уничтожения доказательственной компьютерной информации посторонними лицами; при этом первоначальная упаковка сохраняется. Следователем наносится пояснительная записка на упаковку, которая затем опечатывается бумажной биркой с оттиском печати

следственного подразделения. На упаковке ставят свои подписи все участники осмотра и следователь.

По результатам осмотра на основании постановления следователя мобильный телефон приобщается к материалам уголовного дела как вещественное доказательство. После этого следователь должен либо передать мобильный телефон на хранение собственнику под расписку, либо принять меры к сохранности вещественного доказательства.

Для того чтобы виртуальная следовая картина в мобильном телефоне не подверглась изменениям при хранении или транспортировке, следователю необходимо учитывать следующие рекомендации:

1. Упакованный мобильный телефон следует хранить в опечатанном виде.

2. Необходимо обеспечить хранение мобильного телефона в условиях, рекомендуемых изготовителем, указанных в руководстве по эксплуатации. Мобильным телефонам противопоказаны высокие и низкие температуры, механические воздействия, влажность, воздействия электрических и магнитных полей.

3. При хранении мобильного телефона необходимо избегать воздействия на него вибрации, нахождения вблизи с химически активными веществами, а также оградить его от воздействия электронных приборов.

4. Для транспортировки мобильный телефон следует помещать в металлическую коробку, чтобы предохранить компьютерную информацию от воздействия электромагнитного поля.

При расследовании рассматриваемой категории преступлений выемка является одним из наиболее востребованных следственных действий, направленных на установление обстоятельств, входящих в предмет доказывания.

Технические особенности телекоммуникационных сервисов систем мобильной связи обуславливают ряд специфических тактических рекомендаций частного характера при проведении выемки при расследовании рассматриваемой категории преступлений, а именно:

1. Проведение выемки указанных сообщений, адресованных абоненту, у оператора мобильной связи мало эффективно, так как в базе данных у операто-

ра будут храниться только не дошедшие до абонента сообщения. Соответственно возрастает эффективность обыска мобильного телефона (sim-карты), в связи с тем, что сообщения могут быть сохранены лицом, отправляющим/получающим сообщение.

2. Если указанные сообщения посылаются на электронную почту, то эффективность выемки возрастает, так как отправление будет содержаться не только в компьютере лица, получившего сообщение, но и на сервере провайдера или бесплатном почтовом Интернет-сервере, получающем данное сообщение. Подобный вывод можно сделать и для сообщений голосовой почты, так как они хранятся системой оператора мобильной связи до тех пор, пока пользователь не удалит их.

3. Большое ориентирующие значение для успешного проведения обыска и выемки будут иметь данные относительно активации абонентом тех или иных телекоммуникационных сервисов. Данная задача может быть решена в порядке оперативно-разыскных мероприятий, либо путем направления официального запроса следователя оператору мобильной связи.

4. При принятии решения о наложении ареста на сообщения телекоммуникационных сервисов оператора мобильной связи и их выемку в постановлении должны быть указаны основания производства этого процессуального действия; сведения об абонентском номере и лице, за которым он закреплен, обеспечивающие идентификацию интересующего следствие абонента; дата ареста; порядок информирования следователя о поступающих сообщениях. В зависимости от следственной ситуации в постановлении может быть указано на необходимость блокировать некоторые команды управления телекоммуникационным сервисом (переадресация, удаление) и обеспечить хранение телекоммуникационных сообщений в режиме конфиденциальности и целостности. Постановление направляется соответствующему оператору мобильной связи, а также организациям, предоставляющим услуги доступа в информационные сети, через которые доставляются сообщения на абонентскую подвижную станцию.

5. Специфика объектов выемки и обыска делает необходимым обеспечить участие в обыске специалиста, главным образом, инженера по средствам связи или сетевому обслуживанию.

6. Существенной особенностью обыска мобильного телефона является то, что следователь, как правило, не всегда может оценить на месте значение обнаруживаемой информации, так как, во-первых, он сталкивается с большим объемом персональных данных и технических настроек, и, во-вторых, она представлена в специальном виде, для восприятия которого необходимы определенные специальные познания, а иногда специальные аппаратные и программные средства, в том числе и способствующие доступу к искомой информации.

Следователь и дознаватель при расследовании уголовных дел указанной категории обязан провести следующие мероприятия:

1. Вносить в базу данных ПТК «Марафон» дополнительную информацию о возбужденном уголовном деле, установить связь номера sim-карты преступника с возбужденным уголовным делом.

2. Если ПТК «Марафон» выдаст информацию о том, что данный телефон использовался при совершении иных преступлений, для решения вопроса о соединении уголовных дел в одно производство докладывает об этом начальнику подразделения следствия (дознания) рапортом, в котором излагает данную информацию, а именно: при совершении каких еще преступлений использовался указанный телефон, номера уголовных дел, возбужденных по данным преступлениям.

3. Незамедлительно после возбуждения и принятия к производству уголовного дела по факсу направляет докладную записку, в которой отражает следующую информацию: фабула преступления, дата возбуждения уголовного дела, его номер, ст. УК РФ, номер sim-карты преступника, при наличии - IMEI и базовую станцию в момент звонка потерпевшему. Докладную записку с листком подтверждения, выданным факсимильным аппаратом, приобщить к материалам уголовного дела.

4. Если звонок совершен на стационарный телефон:

- получает в суде разрешение на получение в телефонной компании, обслуживающей данный абонентский номер, детализации звонков телефона потерпевшего в день совершения преступления;

- после чего направляет запрос в телефонную компанию с просьбой предоставить детализацию звонков на телефон потерпевшего в день совершения преступления;

- по получении ответа приобщает его к материалам проверки.

5. Получает в суде разрешение на получение в сотовой компании информации с детализацией звонков преступника, с привязкой к базовым станциям, IMEI сотового телефона преступника, после чего направляет соответствующий запрос в сотовую компанию, в котором просит предоставить детализацию звонков номера sim-карты, с использованием которой звонили потерпевшему, с привязкой к базовым станциям, IMEI сотового телефона, с которого звонили с использованием данной sim-карты.

6. Признаёт потерпевшим и допрашивает его по следующим вопросам:

- во сколько поступил звонок потерпевшему;

- если на сотовый телефон или стационарный телефон с автоматическим определением номера, с какого номера телефона звонили ему;

- кем представился преступник, о чем говорил, что предлагал сделать;

- какую сумму денежных средств и за какие услуги преступник просил передать ему;

- способ передачи денежных средств;

- звонил ли потерпевший повторно преступнику, если да, то о чем говорил с ним, предлагал ли преступник передать ему еще денежные средства, если да, то за какие услуги, сделал ли это потерпевший, если нет то почему;

7. Просит потерпевшего описать голос преступника (хриплый, высокий или низкий, молодой или старый и т.д.), какая манера строить фразы, имеет ли речь преступника или его голос какие-то особенности (например, шепелявит, проглатывает окончание фразы, говорит скороговоркой и т.д.). Спрашивает, сможет ли потерпевший опознать голос преступника.

8. Если деньги направлены блиц-переводом:

- направляет запрос в банк, указав определенные реквизиты с просьбой предоставить следующую информацию: о денежных переводах, полученных за последние 12 месяцев фигурантом по уголовному делу, с просьбой указать дату получения, название и адреса филиала, где они были получены, полученной суммы, установочных данных отправителя (Ф.И.О.) и его домашнего адреса;

- направляет отдельное поручение в ОВД по месту жительства получателя денег с целью истребования копии формы 1 на получение паспорта получателя денег, сведений о судимости; характеристики; с просьбой допросить данного гражданина по факту получения денег: по чьей просьбе он получал денежные средства, как познакомился с данным гражданином, как ему объяснили просьбу получения денежного перевода, знал ли он о том, что деньги получены преступным путем, после получения денег кому и каким способом он их передал или переслал.

9. Производит выемку документов о совершенном блиц-переводе.

10. По получении ответа из компании сотовой связи:

- вносит в базу данных ПТК «Марафон» дополнительную информацию о IMEI сотового телефона, используемого преступником;

- если ПТК «Марафон» выдаст информацию о том, что данный телефон использовался при совершении иных преступлений, для решения вопроса о соединении уголовных дел в одно производство докладывает об этом начальнику подразделения следствия (дознания) рапортом, в котором излагает данную информацию, а именно: при совершении каких еще преступлений использовался указанный телефон, номера уголовных дел, возбужденных по данным преступлениям.

11. Допрашивает гражданина, на которого зарегистрирована sim-карта, с использованием которой звонили потерпевшему:

- когда, где и при каких обстоятельствах приобрел sim-карту, используемую преступником;
- где в настоящее время находится данная sim-карта;

- если передал какому-либо лицу - когда, где, при каких обстоятельствах, имеются ли установочные данные гражданина, которому была передана SIM-карта, если нет, то почему.

12. В случае если гражданин, на которого оформлена sim-карта, говорит о том, что не оформлял данную sim-карту, производит выемку в сотовой компании пакета документов, послуживших основаниям для заключения договора о предоставлении услуг сотовой связи с использованием данной sim-карты. Направляет в подразделение уголовного розыска отдельное поручение, в котором просит провести оперативно-розыскные мероприятия, направленные на установление личности преступника. Если к основному уголовному делу присоединены два и более уголовных дел, возбужденных по аналогичным преступлениям, совершенным с применением сотового телефона с одной sim-картой либо с применением одного сотового телефона (совпадает IMEI сотового телефона):

- получает в суде разрешение на прослушивание телефонных переговоров преступника;
- направляет в подразделение уголовного розыска отдельное поручение, в котором просит провести оперативно-разыскные мероприятия с использованием возможностей ПСТМ (провести прослушивание телефонных переговоров);
- за 10 дней до истечения сроков расследования инициирует проведение совместного заслушивания по уголовному делу, в ходе которого рассматриваются результаты проведенных оперативно-разыскных мероприятий, полноту проведенного расследования. Решает вопрос о дальнейшем прослушивании телефона преступника.

Подводя итог данному вопросу, следует сделать вывод о том, что на стадии предварительного расследования уголовных дел о мошенничествах, совершаемых с использованием sms-сообщений, следователь, дознаватель сталкивается с рядом факторов и проблем при осуществлении дальнейшего производства по делу. Как видно из вышеперечисленных проблем, процессуальное зако-

нодательство в той или иной мере не до конца регламентирует проведение необходимых следственных или экспертных мероприятий.

Вопросы для самоконтроля

1. Какие этапы включает в себя предварительное расследование?
2. Каким образом производится следственный осмотр мобильного телефона?
3. Назовите особенности проведения обыска и выемки при расследовании преступлений, совершенных посредством sms-сообщений.

ЗАКЛЮЧЕНИЕ

Практика показывает, что целенаправленная работа, основанная на знании современных способов мошенничества и методики их раскрытия, взаимодействие с другими службами органов внутренних дел, и, в первую очередь, с аппаратами БЭП, приносит положительные результаты в выявлении и изобличении мошеннических групп.

Создание и использование базы данных АИПС «Досье-мошенник» всеми заинтересованными службами, повышение квалификации сотрудников по выявлению и раскрытию sms-мошенничеств как средства повышения эффективности борьбы с этим видом преступлений, в условиях роста количества регистрируемых фактов, с одной стороны, и ограниченности кадровых и материально-технических ресурсов с другой, и некоторые иные актуальные вопросы борьбы с мошенничеством должны стать предметом рассмотрения на уровне руководителей МВД, УВД субъектов Российской Федерации.

Вопросы борьбы с sms-мошенничеством уже переросли рамки любой отдельно взятой службы, они являются общей проблемой для всей системы органов внутренних дел и требуют своего адекватного организационного оформления.

В системе МВД требуются высококвалифицированные кадры, обладающие знаниями в системе информационных технологий. Это направление весьма востребовано большинством современных предприятий, организаций не только на территории России, но и иностранных государств. Однако необходимо понимать, что услуги специалистов по информационным технологиям в современных условиях довольно востребованы, и руководителям МВД будет сложно привлечь их к решению задач, стоящих перед правоохранительными органами. К объективным факторам, затрудняющим борьбу с данным видом преступлений, необходимо отнести и слабый уровень оснащенности специальной техникой подразделений, занимающихся раскрытием и расследованием sms-мошенничеств.

СПИСОК ЛИТЕРАТУРЫ

1. Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 года) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ) // Текст опубликован в новой редакции в издании: Собрание законодательства Российской Федерации. 2009. № 4. Ст. 445.

2. Европейская конвенция по предупреждению пыток и бесчеловечного и унижающего достоинство обращения или наказания от 28.10.1987 г. // Собрание законодательства РФ. 1998. № 36. Ст. 4465.

3. Международный пакт о гражданских и политических правах от 19.12.1966 г. // Ведомости Верховного Совета СССР. 1976. № 17 (1831). Ст. 291.

4. Конвенция о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (Минск, 22 января 1993 г.) // Вестник Высшего Арбитражного Суда Российской Федерации. 1994. № 2. С. 101.

5. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Первоначальный текст документа опубликован в издании : Собрание законодательства РФ. 2001. № 52.

6. О прокуратуре Российской Федерации: Федеральный закон от 17.01.1992 № 2202-1 (в ред. от 3.12.2012) // Первоначальный текст документа опубликован в издании : Собрание законодательства РФ. 1995. № 47. Ст. 4472.

7. О полиции : Федеральный закон от 07.02.2011 № 3-ФЗ (в ред. от 06.12.2011) // Первоначальный текст документа опубликован в издании : Собрание законодательства РФ. 2011. № 7. Ст. 900.

8. О содержании под стражей подозреваемых и обвиняемых в совершении преступлений: Федеральный закон от 15.07.1995 № 103-ФЗ (в ред. от 03.12.2011) // Первоначальный текст документа опубликован в издании : Собрание законодательства РФ. 1995. № 29. Ст. 2759.

9. О государственной судебно-экспертной деятельности в Российской Федерации : Федеральный закон от 31.05.2001 № 73-ФЗ (в ред. от 06.12.2011) // Первоначальный текст документа опубликован в издании : Собрание законодательства РФ. 2001. № 32. Ст. 2291.

10. О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства : Федеральный закон от 20.08.2004 № 119-ФЗ (в ред. от 30.11.2011) // Первоначальный текст документа опубликован в издании : Собрание законодательства РФ. 2004. № 34. Ст. 3534.

11. Вопросы организации деятельности подразделений дознания (организации дознания) территориальных органов Министерства внутренних дел Российской Федерации : Приказ МВД РФ от 21 ноября 2012 № 1051.

12. О деятельности органов внутренних дел по предупреждению преступлений : Приказ МВД России от 17.01.2006 № 19 (в ред. от 30.12.2011).

13. О мерах по совершенствованию деятельности органов внутренних дел по производству предварительного расследования в форме дознания : Приказ МВД РФ от 21.11.2012 № 1051.

14. О едином учете преступлений : Приказ Генпрокуратуры России, МВД России, МЧС России, Минюст России, ФСБ России, Минэкономразвития России, ФСКН России от 29.12.2005 № 39/1070/1021/253/780/353/399.

15. Об утверждении Инструкции о порядке представления результатов оперативно-разыскной деятельности дознавателю, органу дознания, следователю, прокурору или в суд : Приказ МВД России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, МО России от 17.04.2007 № 368/185/164/481/32/184/97/147.

16. Об утверждении Инструкции по статистической отчетности о следственной работе и дознании : Приказ Генпрокуратуры России, МВД России, Минюст России, ФСБ России, ФТС России, ФСКН России от 31.05.2006 № 27/395/208/229/502/189.

17. Об утверждении Положения об организации взаимодействия подразделений органов внутренних дел Российской Федерации при раскрытии и расследовании преступлений : Приказ МВД РФ от 26.03.2008 № 280 дсп.

18. Об организации планирования в системе органов внутренних дел РФ : Приказ МВД России от 18 октября 2005 № 840 (в ред. от 18.02.2009).

19. Об организации прокурорского надзора за процессуальной деятельностью органов дознания : Приказ Генерального прокурора РФ от 05.09.2007 № 137 (в ред. от 28.12.2008).

20. Об организации прокурорского надзора за исполнением законов при приеме, регистрации и разрешении сообщений о преступлениях в органах дознания и предварительного следствия : Приказ Генерального прокурора РФ от 05.09.2011 № 277.

21. Абдурагимова Т.И. Основы судебной компьютерно-технической экспертизы. – М., 2004.

22. Архипова Н.А. «Организационно-тактические аспекты расследования телефонного мошенничества» // Мир юридической науки. 2011. № 5. С. 69.

23. Большой юридический словарь / под ред. А.Я. Сухарева, В.Е. Крутских. – М.: НОРМА-М, 2002.

24. Васильев А.А., Дудник А.Г. Аспекты формирования криминалистической характеристики преступлений, совершаемых с использованием ЭВМ и радиоэлектронных устройств // Следователь. 2004. № 2. С. 34-38.

25. Вехов В.Б. Аспекты расследования преступлений в сфере электросвязи // Труды Тамбовского филиала юридического института МВД России за первое полугодие 2001. Вып. 4. – Тамбов: Тамбов. Филиал ЮИ МВД России, 2001.

26. Волынский В.В. Судебный контроль, прокурорский надзор и ведомственный процессуальный контроль на стадии возбуждения уголовного дела: назначение и соотношение // Российский следователь. 2011. № 9; СПС «КонсультантПлюс». 2013.

27. Гаврилов М., Иванов А. Следственный осмотр при расследовании преступлений в сфере компьютерной информации // Законность. 2001. № 9.

28. Гирько С.И. Суждения об уголовно-процессуальной деятельности милиции в режиме нового УПК России // Новый уголовно-процессуальный за-

кон: теория и практика применения: материалы межведомственного «круглого стола». – М., 2003.

29. Ефимичев С.П. Правовые и организационные вопросы окончания предварительного расследования с обвинительным заключением: учебное пособие. – Волгоград, 1977.

30. Ефимичев С.П., Ефимичев П.С. Функции в уголовном судопроизводстве: понятие, сущность, значение // Журнал российского права. 2005. № 7. С. 62-63.

31. Завидов Б.Д. Правовой анализ отдельных действий, наносящих потерпевшим ущерб в сфере высоких технологий (фрикерство, хакерство и радиопиратство) // Корпоративный менеджмент. 2001. № 2.

32. Завидов Б.В. Комментарий отдельных положений и новаций УПК РФ (главы 30-32, статьи 215-226 УПК РФ // СПС «КонсультантПлюс». 2013.

33. Ишин А.М., Григорьев А.Н. Информация и расследование преступлений (технические меры обеспечения информационной защищенности деятельности по расследованию преступлений: научно-практическое пособие / под ред. В.М. Мешкова. – Калининград, 2002.

34. Колоколов Н.А. Судебный контроль в стадии предварительного расследования: учебное пособие. – М.: ЮНИТИ-ДАНА, Закон и право, 2004.

35. Крылов В.В. Информационные компьютерные преступления. – М.: ИНФРА-М-НОРМА, 1997.

36. Кукарцев В.К., Ударцев С.Ю. К вопросу о получении детализации телефонных переговоров при раскрытии хищений средств сотовой связи // Актуальные вопросы теории и практики оперативно-розыскной деятельности: материалы международной науч.-практ. конф. (17-18 апреля 2008 г.). – Волгоград, 2008. С. 41-45.

37. Лагуточкин А.В., Алябьев А.А. Проблемы осуществления оперативно-разыскных мероприятий в информационном пространстве сети Интернет // Проблемы правоохранительной деятельности. – Белгород, 2013.

38. Оперативно-розыскная деятельность: учебник / под ред. К.К. Горяинова, В.С. Овчинского, А.Ю. Шумилова. – М.: ИНФРА-М, 2008.

39. Указ Президента РФ от 25.01.2011 № 88 «О назначении на должность и освобождении от должности сотрудников органов внутренних дел Российской Федерации».

40. Семенов Г.В. Расследование преступлений в сфере мобильных телекоммуникаций: дис. ... канд. юрид. наук. – М., 2003.

41. Семенцов В.А. Судебный контроль при производстве следственных действий // Российский судья. 2005. № 12. С. 26.

42. Строгович М.С. Курс советского уголовного процесса. Т. 1. – М.: Наука, 1956.

43. Уголовный процесс: учебник для вузов / под ред. Б.Б. Булатова, А.М. Баранова. – М.: Высшее образование, 2008. С.169.

44. Уланов В.В. Содержание процессуальных функций следователя // Российский следователь. 2008. № 17. С.18.

45. Черепанова Л.В. О проблемах ведомственного контроля при производстве дознания // Вестник Барнаульского юридического института МВД России. 2009. № 2. С. 70.

46. Шебалин А.В. Правовая регламентация получения сведений о соединениях абонентов как важное условие успешного расследования хищений средств сотовой связи // Вестник БЮИ МВД России. 2009. № 2 (17). С. 73-77.

47. Эркенов М.Б. Процессуальный статус дознавателя: автореф. дис. … канд. юрид. наук. – Н. Новгород, 2007.

48. Ярковой В.А. Пределы судебного контроля в досудебном производстве // Уголовный процесс. 2005. № 8. С. 21.

кандидат юридических наук, доцент
Наталья Алексеевна Жукова;
кандидат юридических наук
Юрий Анатольевич Ковтун;
кандидат юридических наук
Андрей Владимирович Лагуточкин
(Белгородский юридический институт МВД России)

Игорь Алексеевич Жуков
(Управление МВД России по Белгородской области)

РАССЛЕДОВАНИЕ И РАСКРЫТИЕ ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ ПОСРЕДСТВОМ SMS-СООБЩЕНИЙ

Методические рекомендации

Оригинал-макет
Белгородского юридического института МВД России

Подписано в печать 10.10.2014
Формат 60 х 90 $^{1}/_{16}$ Бумага офсетная
Печ. л. – 3,0 Тираж 1406 экз. Заказ №

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК