доказательств, подтверждающих вину подозреваемого. В этой ситуации следователь проводит следующие следственные действия: осмотр места происшествия (в данном случае следует учитывать возможность совершения преступления в информационно-телекоммуникационных сетях, с вытекающими отсюда последствиями); допрос свидетелей, допрос подозреваемого, предъявление для опознания, если это необходимо), обыск по месту жительства подозреваемого и в иных местах, имеющих отношение к публичному призыву к осуществлению террористической деятельности или публичного оправдания терроризма, назначение экспертиз, таких как компьютерно-техническая и др.

При второй следственной ситуации необходимо проведение таких же следственных действий, однако нацеленных на обнаружение следов, изобличающих подозреваемого в осуществлении публичных призывов к осуществлению террористической деятельности или публичного оправдания терроризма.

В третьей ситуации программа действий следователя сводится к взаимодействию с сотрудниками оперативных подразделений по обнаружению преступников. В ходе оперативно-розыскной деятельности по поиску лица необходимо активизировать оперативные работы в: этнически криминальных группах, центрах обучения молодежи исламу, сети Интернет; направить запросы в Интерпол о лицах, въехавших на территорию Российской Федерации, возможно, причастных к террористическому движению; получить информацию из консульских учреждений.

[1] Ожегов С.И. Толковый словарь русского языка. URL: http://www.ozhegov.org.

[2] Тяжкова И.М. Экстремистские преступления как посягательства на внутреннюю безопасность государства // Вестник Московского университета. Сер. 11. Право. 2012. № 4. С. 86.

Дерюгин Р.А.

Уральский юридический институт
МВД России (г. Екатеринбург)

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ СВЕДЕНИЙ, ПОЛУЧЕННЫХ ОТ ОПЕРАТОРА СОТОВОЙ СВЯЗИ, ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Рынок предоставления услуг связи в России стал развиваться с конца 1990-х гг., а пользователями сотовых средств связи стали не только законопослушные граждане, но и представители преступного мира. Так, еще в 2006 г. В.А. Козинкин писал: «Средства сотовой связи становятся все более доступными, а их технические возможности постоянно возрастают. Во многом благодаря указанным качествам средства мобильной связи сейчас – самый распространенный инструмент дистанционного человеческого общения, используемый и преступными формированиями при подготовке и совершении преступлений, а также для сокрытия следов противоправной деятельности и противодействия расследованию»[1].

По данным за 2016 г. количество абонентов (активных SIM-карт) в России увеличилось до 249 млн., что на 6,4 млн. больше чем в 2015 г. Согласно статистике МВД России, каждое третье преступление прямо или косвенно связано с мобильными телефонами.[2] Как показывает практика, средства связи задействуются преступниками при подготовке и совершении заказных убийств, террористических актов, похищения людей, вымогательств, взяточничества, преступлений, связанных с незаконным оборотом наркотических средств, мошенничеств, хищений и других общественно опасных деяний. Представляется актуальным изучение информационных свойств средств сотовой связи, а также процесса накопления и формирования сведений об обстоятельствах ее использования конкретным абонентом в качестве источника получения ориентирующей, а соот-

ветственно, криминалистически значимой информации.

Техническая необходимость регистрации и сохранения сведений об абонентах и (или) абонентских устройствах обусловлена особенностью организации работы оператора связи. При этом фиксируется не только факт соединений абонентских устройств, но их вид (входящий/исходящий вызовы, SMS, MMS – сообщения или использование сети Интернет). Также, сохраняются идентификационные данные абонента (сведения SIM-карты, IMEI-код оборудования и др.) и информация о базовых приемопередающих станциях, в зоне действия которых зафиксировано мобильное устройство. Таким образом, архивы оператора связи не только содержат данные о коммуникации и абоненте, но и сохраняют сведения о местоположении и возможных перемещениях абонентов и их устройств, что, несомненно, представляет особый интерес для правоохранительных органов и является важным критерием получения доказательственной информации по уголовному делу.

Использование функциональных возможностей сотовых сетей в преступных целях является стремительно распространяющимся явлением, которое требует пристального внимания и активных, кардинальных мер со стороны правоохранительных органов и государства. Современный преступник активно пользуется новейшими устройствами связи, позволяющими координировать деятельность посредством осуществления исходящих/входящих звонков, передачи SMS, MMS – сообщений, а также возможностей сети Интернет и специальных приложений. К последним следует отнести различные приложения – мессенджеры, которые достаточно популярны среди всех пользователей мобильных телефонов (Viber, Skipe, Whatsapp, Telegramm и др.). Общение посредством таких приложений позволяет находить контакты по всему миру, при этом вести беседу, используя псевдоним, что, как правило, гарантирует анонимность лица. Вышесказанное обуславливает необходимость контроля средств сотовой связи, а также расширения технических возможностей правоохранительных органов по получению информации об абонентах или абонентских устройствах.

На данный момент эффективным процессуальным средством получения сведений об абонентах, их соединениях и устройствах является следственное действие, предусмотренное ст. 186.1 УПК РФ.

С его помощью от оператора сотовой связи можно получить следующую информацию:

– фамилия, имя, отчество или псевдоним абонента-гражданина;

– наименование (фирменное наименование) абонента – юридического лица;

– фамилия, имя, отчество руководителя и работников этого юридического лица; адрес абонента или адрес установки оконечного оборудования; абонентские номера;

– сведения баз данных систем расчета за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонента;

– другие данные, идентифицирующие абонента или его техническое устройство связи.[3]

К примеру, актуально получение таких сведений при совершении заведомо ложного сообщения об акте терроризма, так как данные преступления чаще всего не обходятся без использования средств сотовой связи. Преступник осуществляет звонок с мобильного телефона, сообщает информацию о готовящемся взрыве, поджоге или иных действиях, создающих угрозу безопасности общества, а в базе оператора сотовой связи остаются не только сведения об используемом устройстве (код IMEI и данные SIM-карты), но и биллинговые значения, которые позволяют определить его местонахождение. Отметим, что результатом вышеуказанного следственного действия являются только данные о фактах соединений между абонентскими устройствами, сведения об абонентах, данные о местонахождениях устройств в момент вызова, но не содержание звонков и SMS-сообщений.

Как показывает практика, представители преступного мира ведут пропа-

ганду своей деятельности в социальных сетях, на форумах, а также осуществляют переписку посредством наиболее популярных мобильных приложений. Разработчиками таких приложений являются иностранные компании, а соответственно, все данные находятся на сервере за границей, что значительно затрудняет их получение. К тому же все пользователи перед установкой приложения подписывают условия конфиденциальности, в соответствии с которыми разработчик обязуется не разглашать сведения, касающиеся тайны связи. Этот фактор также значительно ограничивает возможности правоохранителей. Следует констатировать: проблема получения интересующей следствие информации об абонентах, их устройствах или других данных, идентифицирующих пользователей сотовых телефонов при использовании ими мобильных приложений (мессенджеров), остается нерешенной, так как при помощи рассматриваемого следственного действия это невозможно.

Таким образом, в целях повышения эффективности работы следственных органов, а также предотвращения совершения преступлений, необходимо унифицировать правоприменительную практику и разработать рекомендации по производству следственных действий и оперативно-розыскных мероприятий, направленных на получение информации о соединениях между абонентами или абонентскими устройствами, а также данных, содержащихся в мобильных приложениях.

[1] Козинкин В.А. Сведения о детализации телефонных соединений абонента сотовой связи как источник криминалистически значимой информации // Следователь. 2006. № 4. С. 33.

[2] Предупреждение совершения преступлений, связанных с хищением мобильных телефонов. URL: https://31.mvd.ru/press/ (дата обращения: 20.01.2017).

[3] О связи : Федеральный закон от 07.07.2003 № 126-ФЗ. URL: http:// www.consultant.ru (дата обращения: 20.01.2017).

Молоков В.В.,

кандидат технических наук, доцент
Сибирский юридический институт
МВД России (г. Красноярск)

Технические аспекты противодействия преступлениям, совершаемым с использованием сети Интернет

Безграничные возможности интернет-коммуникаций, глобализация открытых компьютерных систем и сетей, автоматизация многих сфер человеческой деятельности, безналичная система финансовых операций, виртуализация личностных отношений и многие другие факторы несознательно культивируют негативные сферы использования сети Интернет в противоправной деятельности. К ним относятся бесконтактный сбыт наркотиков, мошенничество, преступления в системах дистанционного банковского обслуживания, «чисто» компьютерные преступления и другие некомпьютерные, подготавливаемые и осуществляемые за счет использования интернет-коммуникаций.

Характерными особенностями преступлений, совершаемых посредством сети Интернет, являются их анонимность, территориальная неопределенность и латентность. В зависимости от вида преступления потерпевшая сторона может присутствовать, например, в случае мошенничества или кражи денег со счетов владельцев, может и напрямую отсутствовать – как при организации незаконного оборота наркотиков или управлении организованной группой преступного сообщества с использованием средств интернет-технологий.

Для обеспечения противодействия преступлениям, совершаемым посредством сети Интернет, необходимо объединение усилий как правоохранительных органов, так и потенциальных жертв.