УДК 343.132

Хагуров Амир Аскербиевич,
магистр,
ФГБОУ ВО «Кубанский государственный университет»,
г. Краснодар

ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Аннотация: *Статья посвящена анализу тактического и процессуального значения информации о соединениях между абонентами и абонентскими устройствами в уголовном судопроизводстве. В статье рассматривается роль этой информации при проведении различных следственных действий: осмотра места происшествия, допроса, очной ставки, обыска и выемки. Автор подчеркивает двойственную функцию иных следственных действий по отношению к получению информации о соединениях: подготовительную и проверочно-аналитическую. Особое внимание уделяется тактическим приемам использования детализации звонков в конфликтных и бесконфликтных следственных ситуациях, а также процессуальному закреплению полученных электронных данных.*

Ключевые слова: *расследование преступлений, абонентские устройства, информация о соединениях, следственные действия, тактика допроса, осмотр места происшествия, детализация звонков.*

ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Abstract: *The article is devoted to the analysis of the tactical and procedural significance of information about connections between subscribers and subscriber devices in criminal proceedings. The article examines the role of this information in conducting various investigative actions: examination of the scene of the crime, interrogation, confrontation, search, and seizure. The author emphasizes the dual function of other investigative actions in relation to obtaining information about connections: preparatory and verification-analytical. Special attention is paid to the tactical methods of using call details in conflict and non-conflict investigative situations, as well as to the procedural consolidation of the obtained electronic data.*

Keywords: *crime investigation, subscriber devices, connection information, investigative actions, interrogation tactics, crime scene examination, call details.*

Стремительная цифровизация общественных отношений и повсеместное распространение средств подвижной радиотелефонной связи качественно изменили как сам криминальный ландшафт, так и арсенал познавательных средств, доступных субъекту расследования. Абонентское устройство сегодня выступает одновременно в трех ипостасях: как предмет преступного посягательства, как орудие или средство совершения преступления и как уникальный носитель криминалистически значимой информации, фиксирующий поведенческую и пространственно-временную активность пользователя. Применительно к доказыванию по уголовным делам сведения, аккумулируемые в базах данных операторов связи, приобретают значение фактора, во многом определяющего направление расследования,

выбор тактических приемов и последовательность отдельных следственных действий.

Следственное действие, предусмотренное статьей 186.1 УПК РФ, обоснованно рассматривается в специальной литературе как основной процессуальный инструмент получения и систематизации сведений, хранящихся в информационных системах операторов сотовой связи [1, с. 66]. В то же время аналогичная по содержанию информация хотя и в меньшем объеме, в иной форме фиксации и с иной доказательственной нагрузкой может быть получена в ходе целого ряда других следственных действий. Такие действия выполняют по отношению к получению информации о соединениях двоякую функцию: либо подготовительную, предоставляя следователю сведения, необходимые для принятия решения о направлении ходатайства в суд (например, установление абонентского номера в ходе допроса потерпевшего), либо проверочно-аналитическую, позволяющую интерпретировать и верифицировать уже полученные от оператора связи данные. Полагаем, что именно во взаимосвязи этих следственных действий формируется доказательная база, способная преодолеть противодействие расследованию со стороны заинтересованных лиц.

Осмотр места происшествия традиционно относится к первоначальным неотложным следственным действиям и направлен на обнаружение, фиксацию и изъятие материальных следов, имеющих значение для уголовного дела. Применительно к получению информации о соединениях между абонентами особую значимость приобретают те результаты осмотра, которые позволяют выявить материальные носители телекоммуникационных контактов: сотовые телефоны, их составные части, SIM-карты, упаковочные материалы, накопители информации. Эмпирические данные свидетельствуют о том, что более половины опрошенных следователей (57 %) указали на получение в ходе осмотра места происшествия предмета, содержащего сведения о телекоммуникационных контактах [2].

Для обнаружения подобных объектов на месте происшествия необходимо обязательно привлечь специалиста, обладающего навыками работы с поисковым оборудованием. В лесопарковой зоне или на территории, поросшей кустарником, если установлен факт потери преступником сотового телефона или умышленного выбрасывания SIM-карты, рациональным представляется использование металлоискателя, что должно быть отражено в протоколе. При обнаружении абонентского устройства в протоколе подробно описываются его местонахождение, внешние признаки, функциональное состояние, а также фиксируются возможные сопутствующие следы — папиллярные узоры, биологические вещества, механические повреждения. Авторская позиция сводится к необходимости разделения внешнего (биологико-трасологического) и информационного аспектов осмотра: сначала устройство нужно изучить внешне, после чего его можно упаковать и отправить на дактилоскопическую, биологическую или иную судебно-медицинскую экспертизу, и только потом приступать к исследованию его информационной среды.

Особого тактического внимания заслуживает ситуация одновременного изъятия нескольких абонентских устройств во включенном состоянии. В таких условиях категорически не рекомендуется сразу выключать устройства, извлекать аккумуляторы и SIM-карты, поскольку для последующего включения может потребоваться ввод кодов блокировки, PIN-кодов и других защитных данных, которые следствию неизвестны. Конструктивный осмотр в данном случае целесообразно проводить только после тщательного изучения информационной среды устройства. Это тактическое правило обусловлено спецификой современных средств мобильной связи, оснащенных многоуровневой системой защиты.

По обоснованному мнению, изложенному в кандидатской диссертации В. Ф. Васюкова, осмотр мобильного телефона можно разделить на три этапа: внешний осмотр с фиксацией общих признаков (тип, состояние, видимые

повреждения); осмотр конструкции (задняя крышка, аккумуляторный отсек, флеш-накопитель, SIM-карта); осмотр информационной среды с фиксацией данных, хранящихся в памяти устройства и на съемных носителях. В протоколе должны быть указаны как идентификационные характеристики устройства (IMEI, ICCID SIM-карты, марка, модель), так и все манипуляции с устройством с указанием названий открываемых файлов и каталогов.

Применительно к фиксации именно тех сведений, которые отражают абонентские соединения, осмотр начинается с описания процедуры разблокировки устройства, далее с помощью сервисной комбинации *#06# запрашивается IMEI, после чего исследуются разделы «вызовы», «сообщения», «контакты», галерея, мессенджеры и другие приложения. При описании соединений из раздела «вызовы» следует фиксировать их тип (входящий, исходящий, пропущенный), время, продолжительность, абонентский номер контрагента. При большом объеме информационной среды допустимо использование видеозаписи с комментариями следователя о совершаемых манипуляциях.

Между тем процессуальная форма фиксации результатов применения подобных комплексов остается дискуссионной. Если получение информации о соединениях регулируется статьей 186.1 УПК РФ, то извлечение содержательной информации (фотоматериалов, видеозаписей, переписки в мессенджерах и социальных сетях) с помощью специализированных комплексов прямого процессуального закрепления не получило. Е. В. Бурцева и И. А. Рогова отмечают, что соответствующая криминалистическая техника применяется при осмотре предмета, в ходе оперативно-розыскных мероприятий или при проведении компьютерно-технической экспертизы [3, с. 54–56]. Разделяя позицию ряда исследователей, мы полагаем наиболее обоснованным процессуальное закрепление полученной таким образом информации в рамках проведения компьютерно-технической (компьютерно-информационной) экспертизы, поскольку именно эта форма обеспечивает

методическую корректность извлечения данных, документирование всех действий специалиста и возможность судебного контроля за их обоснованностью.

Информация о соединениях между абонентами и (или) абонентскими устройствами приобретает значительный тактический потенциал при проведении допроса — наиболее распространенного следственного действия, выполняющего функцию получения новых сведений и проверки уже имеющихся доказательств [4, с. 67–68]. Эмпирические данные показывают, что результаты следственного действия, предусмотренного статьей 186.1 УПК РФ, используются при допросе обвиняемого (подозреваемого) в 90 % случаев, потерпевшего (свидетеля) в 80 % случаев.

Тактика допроса с учетом информации о соединениях абонентов существенно различается в зависимости от характера складывающейся следственной ситуации бесконфликтной или конфликтной. В бесконфликтной ситуации основной задачей следователя является установление психологического контакта с допрашиваемым лицом, поддержание благоприятной обстановки для свободного изложения сведений и тактически грамотное представление сведений, полученных от оператора связи, в качестве подтверждающей или уточняющей информации о показаниях допрашиваемого. Исходя из предмета допроса, следователю необходимо продумать последовательность вопросов, касающихся наличия у допрашиваемого мобильного телефона, совершенных звонков и местонахождения в момент конкретных переговоров.

Особое тактическое значение приобретает использование детализации соединений при допросе потерпевшего, который на первоначальном этапе расследования дает неточные или недостоверные показания из-за шокового состояния, болевого синдрома или невозможности восстановить хронологию событий. Предъявление детализации, отражающей последние соединения и предположительное местонахождение абонента, позволяет восстановить

цепочку событий и существенно повысить полноту и достоверность показаний. В подобной ситуации используется такой тактический прием, как задействование ассоциативных связей в сочетании с наглядностью.

По мнению автора, тактические приемы допроса с использованием детализации соединений целесообразно классифицировать по способу предъявления информации:

1. приемы постепенного предъявления (поэтапное представление данных детализации в логической последовательности с одновременной фиксацией реакции допрашиваемого);

2. приемы внезапного предъявления (демонстрация ключевого фрагмента детализации после получения от допрашиваемого ложных показаний об отсутствии контактов с тем или иным лицом);

3. приемы косвенного использования (постановка контрольных вопросов, ответ на которые заведомо проверяется с помощью имеющейся детализации). Такая классификация позволяет более системно подходить к подготовке к допросу и выбору конкретной тактической комбинации.

В случаях, когда детализация позволяет установить лиц, использовавших похищенное устройство, при допросе таких лиц следует выяснить: способ приобретения телефона; обстоятельства передачи и личность передавшего; осведомленность о происхождении устройства; реквизиты документов, сопровождавших операцию (товарный чек, договор купли-продажи, гарантийный талон). При этом из тактических соображений вызов на допрос лица, использующего в данный момент похищенный телефон, рекомендуется осуществлять без указания причины вызова в противном случае высока вероятность утраты доказательства.

Существенное тактическое значение информация о соединениях между абонентами приобретает при проведении очной ставки следственного действия, направленного на устранение существенных противоречий в показаниях ранее допрошенных лиц. Очная ставка возможна только при

наличии у следователя достаточной совокупности доказательств для верной оценки показаний ее участников, что объективно повышает роль данных детализации как информации, подтверждающей или опровергающей субъективную сторону показаний.

При наличии в распоряжении следователя доказательств связи участников, в том числе детализации, свидетельствующей о неоднократных соединениях между ними, тактический алгоритм очной ставки, на наш взгляд, может быть представлен следующими взаимосвязанными элементами: постановка вопросов лицу, дающему, по мнению следствия, правдивые показания; соблюдение строгой логической последовательности вопросов; максимальная детализация вопросов, связанных с датами, адресами, временем и продолжительностью соединений; поэтапная конкретизация показаний; активное использование документально закреплённых доказательств - записей с камер видеонаблюдения, результатов экспертиз, аудиозаписей и собственно детализации; привлечение оперативных сотрудников к подготовительному этапу; проведение очной ставки по возможности непосредственно после задержания или в рамках единой тактической операции.

Обыск и выемка занимают самостоятельное место в системе следственных действий, в рамках которых возможно получение материальных носителей информации о телекоммуникационных контактах. Так, при обыске по месту жительства руководителя организованной преступной группы могут быть обнаружены боксы (упаковочные конверты) из-под SIM-карт сотовых телефонов, другие электронные носители, упаковочные материалы с записанными PIN-кодами и PUK-кодами. Криминалистическое значение подобных объектов заключается в том, что они подтверждают обстоятельства преступной деятельности организатора по координации действий соучастников и обеспечению членов группы средствами связи, в том числе для соблюдения мер конспирации.

В соответствии с частью 9.1 статьи 182 и частью 3.1 статьи 183 УПК РФ при изъятии электронных носителей информации в ходе выемки или обыска, к которым обоснованно относятся и абонентские устройства, обязательно участие специалиста. Изъятое абонентское устройство связи во всех случаях подлежит осмотру по правилам осмотра предметов с возможным последующим направлением на компьютерно-техническую экспертизу.

В качестве тактической рекомендации, заслуживающей закрепления в методических указаниях, следует выделить проведение группового осмотра объектов, изъятых в ходе различных следственных действий, проведенных в разных местах, но структурно дополняющих друг друга в рамках функционирования единого абонентского устройства. К таким объектам относятся сами сотовые телефоны, комплектующие, аксессуары, идентифицируемые по модели устройства, а также упаковки от SIM-карт с абонентским номером пользователя. Совокупный анализ таких объектов позволяет установить контроль за телекоммуникационной активностью конкретного абонентского устройства и разоблачить попытки виновных лиц инсценировать неосведомленность о контактах соучастников.

Теоретически средства связи могут быть обнаружены и в ходе таких следственных действий, как проверка показаний на месте (часть 1 статьи 194 УПК РФ) и следственный эксперимент. Показывая место совершения преступления или сокрытия похищенного имущества, подозреваемый (обвиняемый) может указать на находящийся там сотовый телефон, принадлежавший потерпевшему. Независимо от процессуальной формы изъятия абонентское устройство во всех случаях подлежит тщательному осмотру.

Проведенный анализ позволяет констатировать, что результаты получения информации о соединениях между абонентами и (или) абонентскими устройствами интегрированы в систему отдельных следственных действий двояким образом. С одной стороны, другие

следственные действия (осмотр места происшествия, осмотр предмета, обыск, выемка, личный обыск, допрос) предоставляют следователю первичные сведения об абоненте, абонентском номере, IMEI-коде устройства, необходимые для подготовки и направления ходатайства в порядке статьи 186.1 УПК РФ. С другой стороны, информация, уже полученная от оператора связи, служит надёжным инструментом организации и тактического обеспечения последующих следственных действий — допроса, очной ставки, проверки показаний на месте.

Гораздо меньше в литературе освещаются возможности использования рассматриваемой информации при расследовании преступлений, не связанных напрямую с использованием средств связи. Между тем сведения о соединениях нередко выступают в качестве косвенных доказательств причастности лица к преступлению по делам о дорожно-транспортных происшествиях (для проверки факта нахождения водителя на месте происшествия) [5, с. 10], о террористических актах (для установления круга абонентов, которые в момент совершения преступления обслуживались базовой станцией в районе происшествия), о налоговых и иных экономических преступлениях (для установления факта пребывания обвиняемых на территории, где совершались юридически значимые действия).

В связи с этим следует согласиться с тем, что информация о соединениях между абонентскими устройствами по своей доказательной природе чаще выступает в качестве косвенных, а не прямых улик. Это обусловлено двумя обстоятельствами: во-первых, сведения, получаемые в порядке статьи 186.1 УПК РФ, фиксируют сам факт соединения, но не его содержание; во-вторых, абонент, указанный в договоре с оператором связи, не всегда совпадает с фактическим пользователем абонентского устройства. Ю. Н. Соколов справедливо отмечает, что отсутствие в настоящее время отработанных методик определения подлинности и авторства цифровых сообщений является основной проблемой при преобразовании соответствующих данных в

доказательства [6, с. 130]. Из этого следует методологически важный вывод: одновременно с анализом детализации следователь обязан устанавливать принадлежность конкретного абонентского устройства определенному лицу — путем допроса с уточнением обстоятельств использования сотового телефона или SIM-карты, а также путем фиксации факта отсутствия доступа к устройству посторонних лиц.

Литература:

1. Агафонов В.В., Вазюлин С.А., Васюков В.Ф. Особенности формирования доказательств с использованием информации о соединениях между абонентами и (или) абонентскими устройствами: криминалистические и процессуальные аспекты. М.: Юрлитинформ, 2015. 168 с.
2. Васюков В.Ф. Получение информации о соединениях между абонентами и (или) абонентскими устройствами: дис. … канд. юрид. наук. М., 2015. Прил. 1.
3. Бурцева Е.В., Рогова И.А. Проблемы получения информации, содержащейся в электронных мобильных устройствах, с применением универсального устройства извлечения судебной информации (УУСИ) // Материалы X Международной научно-практической конференции «Эффективные инструменты современных наук». 2014. Т. 11. Прага. С. 54—56.
4. Драпкин Л.Я. Тактика следственных действий: учеб. пособие. Екатеринбург: Уральский юридический институт МВД России, 2014. 135 с.
5. Куприянов А.А. Суд свяжет следствие «проводами» // Уголовный процесс. 2010. № 6. С. 10-15.
6. Соколов Ю.Н. Электронное наблюдение в уголовном судопроизводстве и оперативно-розыскной деятельности. Екатеринбург, 2006. 175 с.