Вестник Томского государственного университета. 2020. № 459. С. 221–229. DOI: 10.17223/15617793/459/27

ПРАВО

УДК 343.985, 343.132

О.Ю. Антонов

ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ В РОССИИ: СУЩНОСТЬ, ЭТАПЫ И ПУТИ СОВЕРШЕНСТВОВАНИЯ ТАКТИЧЕСКОГО ОБЕСПЕЧЕНИЯ

Раскрывается комплексная сущность получения информации о соединениях между абонентами и (или) абонентскими устройствами. Выделяются стадии его подготовительного этапа: процессуальная, организационная и организационно-техническая. Обосновывается проведение его рабочего этапа в рамках следственного осмотра. Даются рекомендации по реализации стадии оценки и использования результатов данного следственного действия.

Ключевые слова: информация о соединениях между абонентами и(или) абонентскими устройствами; следственное действие; криминалистическая тактика; тактический комплекс.

Среди законов развития криминалистики ее российский патриарх профессор Р.С. Белкин выделял ускорение ее развития в условиях научно-технического прогресса, а также активное творческое приспособление для целей судопроизводства достижений различных наук [1. С. 245–250, 259–261], предоставляющие новые возможности получения криминалистически значимой информации путем введения в уголовно-процессуальное законодательство современных технических способов получения доказательств. Одним из таких новых видов доказательств, рожденных в результате научно-технических достижений в области радиоэлектроники и компьютерной техники, является информация о соединениях между абонентами и (или) абонентскими устройствами.

В Соединенных Штатах Америки еще в 1996 г. Федеральная комиссия по связи (FCC) приняла решение об отражении сведений о регистрации местоположения вызывающего абонента диспетчерам экстренной связи 911. В связи с этим в 1999 г. сотовые операторы начали производить записи детализации вызовов (CDR) с информацией о местоположении сотового узла (CSLI), которые предоставлялись правоохранительным органам по решениям суда. Информация CDR / CSLI стала важным доказательством в судопроизводстве (CDR) [2].

В России практика получения от операторов связи сведений о соединениях средств электросвязи стала формироваться с начала 2000-х гг. путем проведения выемки, контроля и записи телефонных и иных переговоров или просто путем направления запросов без процессуальной регламентации. Получение информации о соединениях между абонентами и (или) абонентскими устройствами стало новым процессуальным действием после введения в 2010 г. в Уголовно-процессуальный кодекс Российской Федерации ст. 186.1 [3].

С учетом технической составляющей этого процессуального действия в российской уголовно-процессуальной и криминалистической литературе возникла дискуссия о его сущности.

Так, В.Ю. Стельмах относит получение информации о соединениях между абонентами и (или) абонентскими устройствами к условной группе технико-специальных следственных действий, выделяя в порядке их производства два относительно обособленных блока: процессуальную деятельность следователя и исследовательскую или техническую деятельность других лиц, результаты которой ему предоставляются [4. С. 44–45]. Действительно, следователь в судебном порядке запрашивает информацию; осуществляющая услуги связи организация в лице конкретного сотрудника ее формирует из автоматизированной базы данных и направляет в установленном виде следователю, который проводит ее осмотр. Соответственно, разработка тактических рекомендаций для указанного способа получения доказательств должна осуществляться с учетом его организационно-технических особенностей проведения. Однако эти особенности, определяющие специфическое содержание этого следственного действия, вызывают дискуссию в научной и учебной литературе.

Наиболее резко и критично к теоретической интерпретации сущности получения информации о соединениях между абонентами и (или) абонентскими устройствами как следственного действия подходит Б.Т. Безлепкин, считая, что «речь идет в сущности не о новом следственном действии (никаких процессуальных действий по обнаружению, «извлечению» и закреплению доказательств следователь не производит), а о представлении документальных доказательств по требованию органа расследования» [5]. Продолжая свою мысль, он полагает, что «истребовать и получить из соответствующей компетентной организации, будь то бухгалтерия фирмы или оператор сотовой связи, требуемую, надлежащим образом задокументированную, доказательственную информацию – это одно, а произвести лично регламентированное УПК следственное действие в целях личного извлечения такой информации – принципиально другое. Налицо два совершенно различных процессуальных способа уголовно-процессуального доказывания, сформировавшихся в историческом процессе развития уголовного судопроизводства. В ст. 186.1 УПК РФ они перепутаны» [6].

Аналогичной с Б.Т. Безлепкиным точки зрения придерживается С.А. Шейфер: «Закон преображает в следственное действие достаточно широко распро-

страненный в следственной практике прием детализации переговоров, ведущихся с мобильных и других телефонов… Но регламентация этого приема в УПК РФ не предусматривает каких-либо познавательных операций, присущих следственным действиям… При этом какие-либо процессуальные отношения между следователем и оператором отсутствуют, не предусмотрена и ответственность оператора за непредоставление сведений» [7. С. 122].

Действительно, в случае формирования информации о соединениях между абонентами и (или) абонентскими устройствами не непосредственно следователем, а сотрудником организации, являющимся оператором связи, возникает вопрос о полноте и объективности ее предоставления. Некоторые авторы в это не сомневаются, ссылаясь на технические возможности системы сотовой связи [8. С. 11]. С технической точки зрения все может быть надежно, поскольку данное программное обеспечение разрабатывается организациями, имеющими соответствующие лицензии Федеральной службы безопасности России (на осуществление разработки, производства и распространения шифровальных (криптографических) средств) и Федеральной службы по техническому и экспортному контролю России (на деятельность по технической защите конфиденциальной информации либо по разработке и производству средств защиты конфиденциальной информации). Однако нельзя забывать про «человеческий фактор»: сотрудник оператора связи вполне может вследствие халатного отношения к своим обязанностям, невнимательности либо технической ошибки предоставить информацию не в полном объеме (такие факты упоминаются в научной литературе [9. С. 144]), более того – способен внести в сформированные сведения какие-либо изменения. При этом он, в отличие от судебного эксперта, также действующего по поручению следователя, не несет уголовной ответственности за предоставление заведомо ложной информации, а доказать его корыстную или иную личную заинтересованность, а также преступный сговор с лицами, осуществляющими противодействие расследованию преступлений, практически невозможно. Кроме того, можно спрогнозировать совершение умышленных действий по внесению изменений в информацию, формируемую операторами связи, со стороны нового вида организованной преступности – хакерского сообщества [10] по заказу лиц, совершивших преступления, вину в совершении которых можно доказать путем получения и анализа информации о соединениях между абонентами и (или) абонентскими устройствами.

Таким образом, предусмотренный ст. 186.1 УПК РФ процессуальный порядок не позволяет в полном объеме обеспечить достоверность полученных сведений и затрудняет процесс оценки доказательств по требованиям, отраженным в ч. 1 ст. 88 УПК РФ. Зарубежные исследователи уже обратили на это внимание, разрабатывая методы определения того, являются ли сведения, формируемые операторами мобильной связи (MNO) и операторами мобильной виртуальной сети (MVNO), цифровыми доказательствами и поддерживается ли доказательственная целостность при их передаче следователям правоохранительных органов по уголовным делам [11].

Изложенное обусловливает необходимость определения места получения информации о соединениях между абонентами и (или) абонентскими устройствами в системе следственных действий в целях разработки криминалистических рекомендаций по тактике его производства. В связи с этим можно использовать позицию А.С. Князькова, который, основываясь на мнении С.А. Шейфера об организационно-распорядительном, обеспечительном характере некоторых процессуальных действий, относит получение информации о соединениях между абонентами и (или) абонентскими устройствами к числу таковых, ссылаясь на нормы УПК РФ, указывающие о проведении непосредственно за обеспечительными процессуальными действиями следственного осмотра [12. С. 131]. Действительно, проведение именно следственного осмотра сведений о соединениях между абонентами и (или) абонентскими устройствами вытекает из ч. 5 ст. 186.1 УПК РФ и соответствует сущности самостоятельного следственного действия – следственного осмотра, предусмотренной ст. 176–177, 180 УПК. Из этого можно сделать вывод, что рассматриваемое действие состоит из обеспечительных процессуальных и организационных процедур получения информации и собственного следственного осмотра полученных сведений, т.е. носит комплексный характер. Аналогичного мнения о сущности получения информации о соединениях между абонентами и (или) абонентскими устройствами придерживаются В.Ю. Стельмах [4. С. 58–59], Р.А. Дерюгин [13] и Н.А. Архипова [14. С. 10].

Такая нетрадиционная сущность деятельности по получению информации о соединениях между абонентами и (или) абонентскими устройствами ставит криминалистике относительно новую задачу – сформулировать тактику трех входящих в него взаимосвязанных между собой процессуального, организационного и следственного действий в рамках единого тактического комплекса:

1) направления в суд ходатайства следователя о производстве данного следственного действия (ч. 1, 2 ст. 186 УПК РФ);

2) направления следователем в соответствующую осуществляющую услуги связи организацию копии решения суда в случае принятия такого решения (ч. 3 ст. 186 УПК РФ);

3) осмотра документов, представленных соответствующей организацией, осуществляющей услуги связи и содержащих информацию о соединениях между абонентами и (или) абонентскими устройствами (ч. 5 ст. 186 УПК РФ) [15. С. 174].

В связи с этим в криминалистической литературе возникла дискуссия по этапам и стадиям данного комплексного следственного действия. Некоторые исследователи ставят во главу угла наименование следственного действия – «получение информации», относя его к первому рабочему этапу данного следственного действия [16. С. 24] или к первой стадии рабочего этапа [17. С. 129]. Однако, по нашему мнению, целью рассматриваемого следственного действия является ана-

лиз полученной информации, имеющей криминалистическое значение. Поэтому, на наш взгляд, более верной представляется точка зрения Д.В. Муленкова, А.Б. Соколова, О.Н. Лазаренко о том, что в подготовительный этап должны входить действия следователя по получению сведений о соединениях между абонентами и (или) абонентскими устройствами от организации, осуществляющей услуги связи [15. С. 173]. Действительно, этот этап оканчивается моментом направления следователем копии решения суда о получении информации о соединениях между абонентами и (или) абонентскими устройствами руководителю организации, осуществляющей услуги связи [17. С. 128]. Однако согласно ч. 3 ст. 186.1 УПК РФ сам следователь не может предпринимать действий по получению этой информации и лишь ожидает сопроводительное письмо с прилагаемой в опечатанном виде зафиксированной на любом материальном носителе информацией. Поэтому верной представляется точка зрения Е.С. Лапина, выделяющего среди этапов производства этого следственного действия (на наш взгляд, именно на этапе подготовки) отдельную техническую стадию по исполнению оператором связи действий по предоставлению соответствующей информации [9. С. 40].

Таким образом, подготовительный этап можно разделить на следующие стадии: процессуальную (подготовка и направление в суд ходатайства следователя о производстве следственного действия), организационную (направление следователем решения суда осуществляющей услуги связи организации) и организационно-техническую (действия оператора связи по формированию и предоставлению информации).

Первая стадия подготовительного этапа хотя и называется процессуальной, но требует не только процессуального, но и тактического обеспечения. Основные криминалистические рекомендации по принятию решения о проведении данного следственного действия и его подготовке достаточно подробно рассмотрены в литературе [9. С. 89–116; 15. С. 174–175; 18. С. 39–43], в том числе в зависимости от типичных следственных ситуаций [19], но требуют дальнейшего совершенствования по следующим направлениям.

1. В связи с имеющимися случаями отказа судов в удовлетворении ходатайств следователя, несмотря на наличие предложений с точки зрения уголовного процесса [4. С. 260–261, 286–287], возникает необходимость дальнейшей разработки тактических рекомендаций по составлению мотивировочной части таких ходатайств, в первую очередь в части обоснования значения для расследуемого преступления, учитываемого при принятии следователем решения о его проведении. В имеющейся в настоящее время криминалистической литературе иногда встречаются лишь рекомендации «более аргументированно излагать необходимость получения указанной информации за соответствующий период» [20. С. 24].

2. Большое значение имеет выверенное определение временного интервала, за который необходимо получить информацию о соединениях либо срок производства данного следственного действия. Такой период определяется не только предполагаемым временем совершения преступления, но зависит также от того, совершено ли преступление с внезапно возникшим умыслом или планировалось заранее (период подготовки также необходимо включать), местным жителем или заезжим преступником из другого региона (в таком случае для последующей грамотной выборке запрашивать период предшествующий преступлению и последующий период – несколько дней), единичный ли это преступный эпизод или длящееся преступление во времени и пространстве и т.п.

3. Отдельные следственные ситуации требуют проведения дополнительного подготовительного следственного действия – следственного осмотра с использованием датчиков оценки радиоэлектронной обстановки либо находящихся в свободном доступе программ Netmonitor, G-nettrack и других в целях установления в конкретном месте или по определенному маршруту базовых станций различных типов сети всех операторов связи одновременно. В результате проведения данного следственного действия определяются базовые станции, осуществляющие соединения в данном месте, а также их принадлежность к конкретным операторам связи, у которых следует запрашивать информацию о соединениях. Это позволяет сформулировать запрос в порядке ст. 186.1 УПК РФ каждой осуществляющей услуги связи организации с указанием идентификационных данных станций, которые необходимо проверить для подготовки интересующей следователя информации в данный период времени. Кроме того, результаты осмотра позволяют указать в ходатайстве не только стандартно запрашиваемые сведения об абоненте, собеседнике, типе соединения, его дате, времени и продолжительности, но и азимут (угол между направлением на север (нулевой показатель компаса) и направлением на место нахождения абонента), time energy (время прохождения сигнала от устройства абонента до базовой станции) [21. С. 28].

Тактика этого нового вида следственного осмотра, проводимого именно в целях подготовки к получению информации о соединениях между абонентами и (или) абонентскими устройствами, требует проведения дополнительных криминалистических исследований. Например, М.А. Гудкова полагает, что это следственное действие должно проводиться в то же время, что и проверяемое событие, поскольку в различные периоды в течение суток распределение нагрузки на каждую отдельную базовую станцию, зона покрытия каждой такой станции и, как следствие, возможности соединения устройства с каждой станцией весьма различаются [22. С. 157–158].

В любом случае, даже если данное следственное действие не проводится, на этой стадии подготовительного этапа нужно сформировать конкретные типы сведений о соединениях между абонентами и (или) абонентскими устройствами, имеющими потенциальное криминалистическое значение, которые необходимо отразить в ходатайстве в суд.

Переходя к последней, организационно-технической стадии подготовительного этапа получения информации о соединениях между абонентами и (или) абонентскими устройствами, на первый взгляд, можно признать, что она нуждается не в криминали-

стическом, а лишь в программно-техническом обеспечении. Однако в практике работы Следственного комитета Российской Федерации появилась возможность организации взаимодействия с операторами связи в целях получения информации об абонентах и их соединениях в рамках системы обработки запросов (СОЗ) – комплекса, переводящего процесс бумажного документооборота оператора с государственными уполномоченными органами в формат ЭДО [23]. Так, в отдельных следственных органах СК России в тестовом режиме с 2018 г. используется предоставленный ПАО «МегаФон» доступ к автоматизированной системе обработки запросов (АСОЗ), позволяющей по фамилии, имени, отчеству и дате рождения разыскиваемого лица оперативно получать сведения о зарегистрированных на него абонентских номерах [24. С. 638], а также соединениях между абонентами и (или) абонентскими устройствами и иной требуемой информации (по решению суда). Одним из направлений криминалистического обеспечения данного взаимодействия является разработка рекомендаций для программного обеспечения оператора связи в части формирования вида запрашиваемой информации в зависимости от типичных задач расследования преступлений. Например, Инструкция пользователя СОЗ ПАО «МегаФон» позволяет формировать 16 типов запросов: 4 по детализации, 2 по интернету, 9 по местоположению и регистрации, 1 по принадлежности [25], в то же время программное обеспечение ООО «Основа Лаб» предоставляет возможность обработки 24 уникальных типов запросов и получения аналитических данных [23].

Расширение данной практики получения информации об абонентах и их соединениях в рамках СОЗ, на наш взгляд, позволит нивелировать указанные ранее негативные моменты и обеспечить достоверность полученных сведений, поскольку их формирование будет осуществляться не физическим лицом – сотрудником оператора связи, а с помощью данного программного обеспечения. Такая возможность опровергает существующее мнение о том, что требование о проведении такой деятельности в обязательном порядке лично следователем является заведомо невыполнимым и попыткой блокировать достижения научно-технического прогресса в сфере расследования преступлений [4. С. 51]. В то же время сотрудник оператора связи в данном случае должен осуществить проверку наличия в решении суда всех типов сформированных следователем в рамках СОЗ запросов. В связи с этим требуется разработка соответствующих методических рекомендаций как для данных сотрудников по проведению этой проверки, так и для следователей по указанию в ходатайстве в суд сведений, соответствующих типам запросов оператора связи, предусмотренных в его СОЗ.

Рассмотренная практика взаимодействия фактически объединяет в одну стадию выделенные ранее организационную и организационно-техническую стадии подготовительного этапа получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Только после поступления данной информации начинается рабочий этап рассматриваемого тактического комплекса – ее следственный осмотр, включающий его последнюю стадию – фиксацию хода и результатов, тактика проведения которого также требует дальнейшего совершенствования, поскольку, по мнению Р.А. Дерюгина и А.А. Жижилевой, субъекты расследования уголовного дела не уделяют должного внимания криминалистическому значению сведений, получаемых от оператора сотовой связи (не производятся качественный анализ, обработка полученной информации, что приводит к утере значимых доказательственных сведений, имеющих значение для раскрытия и расследования преступления) [26. С. 221].

В следственных ситуациях, требующих анализа большого объема полученных сведений, а также решения сложных криминалистических задач, к следственному осмотру требуются привлечение специалиста в области компьютерной техники и применение соответствующих аппаратно-программных комплексов. Например, «в 2018 году производителем АПК “Сегмент” выпущена обновленная версия программной части, которая обладает расширенным функционалом, дающим возможность решать более сложные аналитические задачи… и способна автоматически в процессе обработки биллинга получать из открытых источников информацию о координатах, адресах установки, мощности, направлении действия и других параметрах базовых станций» [24. С. 638].

В практике работы следственных органов СК России такой следственный осмотр, как правило, проводится следователем-криминалистом по поручению следователя. Однако требуется разработка тактики взаимодействия указанных лиц как на этапе следственного осмотра, так и на этапе подготовки ходатайства в суд, поскольку формулировка всех возможных задач, которые решаются в ходе следственного осмотра, может быть осуществлена следователем только с учетом понимания технических возможностей анализа, знанием которого обладает сведущее лицо в области компьютерной техники, например, находящееся на должности следователя-криминалиста или эксперта СК России.

Замена такого следственного осмотра назначением так называемой информационно-аналитической судебной экспертизы или более того проведением «аналитического исследования» является на сегодняшний день не совсем приемлемым по следующим основаниям. Если готовить об информационно-аналитической судебной экспертизе, то упоминания о таком виде судебных экспертиз в учебной и научной литературе единично как в России [22], так и за рубежом, где она называется системой криминалистической экспертизы телефонных записей (TRFS) [27]. Фактически сущность данной формы использования специальных знаний – это не проведение исследования, позволяющего получить новые знания, имеющие доказательственное значение, а анализ приобретенных от оператора связи сведений с помощью аппаратно-программных комплексов (АПК), позволяющих выявить закономерности или связи. Для работы с данными АПК, как правило, специальных знаний в

области информатики и компьютерной техники не требуется, а необходимо обладать лишь навыками работы с их интерфейсом. Только в отдельных случаях, для решения сложных задач при применении АПК, необходимы специальные знания в области базовых принципов построения и функционирования сетей мобильной радиосвязи, которыми в следственных органах СК России обладают следователи-криминалисты. Однако в рамках создаваемой в разделе «Криминалистическая техника» российской криминалистики новой отрасли – «Криминалистическое исследование компьютерных средств и систем» [28] дальнейшее развитие криминалистического анализа цифровой информации так называемых больших данных (Big Data) [29], в которые входит информация о соединениях между абонентами и (или) абонентскими устройствами, а также достижений зарубежной цифровой криминалистики [30, 31] может привести к появлению данного вида судебных экспертиз. В то же время следует иметь в виду, что с процессуальной точки зрения и с постановлением о назначении такой судебной экспертизы, и с ее заключением требуется ознакомить участников уголовного процесса (ст. 206 УПК РФ), а ознакомившись с заключением эксперта, сторона защиты может организовать противодействие расследованию путем опровержения факта использования обвиняемым (подозреваемым) исследуемыми средствами связи.

Спецификой рабочего этапа данного следственного действия является то, что оно может проводиться несколько раз еженедельно (до 27 раз!), поскольку согласно ч. 4 ст. 186.1 УПК РФ получение следователем информации о соединениях между абонентами и (или) абонентскими устройствами может быть установлено на срок до шести месяцев. Соответственно, представляется необходимым разработка тактических рекомендаций по частоте и особенностям проведения каждого следственного осмотра в данный период.

Далее необходимо отметить, что в криминалистической тактике в этапы производства следственных действий не всегда включается оценка и использование полученных результатов. Так, особенности оценки результатов следственного действия рассматриваются в тактике следственного эксперимента [32. С. 177–179], а деятельность следователя, дознавателя и суда по оценке и использованию заключения эксперта прямо выделяется в тактике назначения и производства судебной экспертизы [33. С. 144–151]. При этом указывается, что после оценки могут приниматься решения о допросе эксперта либо назначении дополнительной или повторной судебной экспертизы, т.е. появляются дополнительные этапы деятельности следователя, связанной с производством судебной экспертизы. Применительно к рассматриваемому следственному действию оценку и использование в доказывании результатов получения информации о соединениях между абонентами и (или) абонентскими устройствами Н.А. Архипова относит к заключительному этапу его проведения, предлагая отдельные криминалистические рекомендации данного этапа [34. С. 5]. Обязательность данного этапа также обусловлена требованиями ч. 6 ст. 186.1 УПК РФ, предусматривающей приобщение к материалам уголовного дела полученных документов на основании постановления следователя в качестве вещественных доказательств.

Учитывая предложения Н.А. Архиповой, можно сформулировать следующие направления дальнейшего совершенствования этапа оценки и использования результатов рассматриваемого следственного действия, а также принимаемых следователем по ее итогам решений, проводя некоторую аналогию с оценкой и использованием заключения эксперта:

1. Оценка информации, полученной от оператора связи с точки зрения ее полноты, т.е. получения сведений по всем типам запросов, сформулированных в судебном решении.

Если оператор связи не представил все запрашиваемые сведения без указания причин (например, отсутствие технической возможности формирования и предоставления данный сведений), то необходимо повторно направлять запрос оператору связи на основании первичного решения суда.

2. Полнота и результативность проведенного следственного осмотра.

Как указано выше, в целях получения максимально возможной интересующей следователя информации в отдельных случаях недостаточно провести следственный осмотр полученных сведений, а требуется назначение судебной информационно-аналитической экспертизы.

3. Достаточность полученных в ходе следственного осмотра сведений для расследования преступления.

С учетом полученных сведений может возникнуть необходимость получения информации об анкетных данных абонентов, с которыми осуществлял соединение первоначальный абонент, или даже о соединениях между новыми абонентами и (или) абонентскими устройствами, например находившимися на месте происшествия или на определенном маршруте. То есть необходимо принятие решения о проведении нового аналогичного следственного действия.

4. Доказывание факта использования конкретным лицом зарегистрированного на него устройства связи.

Следует отметить, что результаты рассматриваемого следственного действия не являются прямым доказательством, поскольку анализу подвергается не непосредственная деятельность конкретного лица, а лишь принадлежащих ему средств связи. Поэтому для привязки этого лица к данному мобильному устройству требуется проведение дополнительных следственных действий: допрос его близких или родственников, а также разговаривавших с ним других абонентов, указанных в детализации; осмотр видеозаписей камер наблюдения, зафиксированных абонентами в зоне его выхода в сеть и т.д.

5. Проверка полученных сведений в сравнении с иными доказательствами, подтверждающими или опровергающими результаты следственного осмотра.

Например, согласно показаниям свидетелей абонент находился в конкретном месте, однако согласно ответу оператора связи находящиеся вблизи базовые станции не принимали сигнал от этого номера. Возможная причина этого – высокая загруженность данных станций, в связи с чем соединения может осу-

ществлять базовая станция, располагающаяся за несколько десятков километров от места нахождения абонента. В данном случае можно рекомендовать проведение следственного осмотра места происшествия с использованием датчика РЭО примерно в то же время суток, что и проверяемое событие, чтобы выявить все базовые станции, которые могут осуществлять соединения, и включить их в новый запрос оператору связи. То есть необходимо проведение дополнительного аналогичного следственного действия.

В отдельных случаях достаточно провести допрос сотрудника организации, предоставляющей услуги связи, который может пояснить технические особенности формирования информации и ее значение. Например, в ходе допроса представитель оператора связи, предоставившего в порядке ст. 186.1 УПК РФ сведения о соединениях абонента (обвиняемого) в зоне действия базовых станций, расположенных в г. Алушта, сообщил, что сигнал от базовой станции идет в виде лепестка примерно на 60 градусов справа и слева от ее азимута; однако существует и обратный лепесток с противоположной стороны от азимута [35].

Кроме того, можно отметить имеющиеся в практике случаи создания заведомо ложного алиби, подтверждаемые геопозиционированием мобильных устройств, принадлежащих подозреваемым или обвиняемым.

Соответственно, необходимо выявить все типичные следственные ситуации, возникающие в ходе оценки информации о соединениях между абонентами и (или) абонентскими устройствами, сформулировать типичные версии и предложить рекомендации по планированию расследования.

6. Направления использования полученных сведений в расследовании преступления (в качестве доказательств, разыскной или ориентирующей информации). Действительно, как справедливо отмечает В.А. Азаров, процесс доказывания завершается тогда, когда имеющиеся судебные доказательства систематизированы и «уложены» в обоснование процессуального решения, в том числе итогового, определяющего «судьбу» уголовного дела [36. С. 93].

Таким образом, после проведения оценки могут появляться новые факультативные этапы рассматриваемого процессуального комплекса:

1) направление повторного запроса оператору связи;

2) получение заключения эксперта по результатам производства информационно-аналитической экспертизы;

3) допрос представителя осуществляющей услуги связи организации.

Кроме того, могут приниматься решения о производстве новых следственных действий, в том числе связанных с получением новой информации о соединениях между абонентами и (или) абонентскими устройствами.

В заключение сформулируем следующие направления дальнейшего совершенствования тактического обеспечения получения информации о соединениях между абонентами и (или) абонентскими устройствами:

1) разработка тактических рекомендаций по составлению мотивировочной части ходатайств следователя о проведении данного следственного действия;

2) определение временного интервала, за который необходимо получить информацию о соединениях либо срок производства данного следственного действия;

3) разработка тактики производства дополнительного подготовительного следственного действия – следственного осмотра в целях установления в конкретном месте или по определенному маршруту базовых станций различных типов сети всех операторов связи одновременно;

4) формирование типов сведений о соединениях между абонентами и (или) абонентскими устройствами, имеющих потенциальное криминалистическое значение, которые необходимо отразить в ходатайстве в суд, в том числе с учетом возможностей программного обеспечения операторов связи в рамках системы обработки запросов;

5) конкретизация тактики проведения следственного осмотра сведений, полученных от оператора связи;

6) разработка тактических рекомендаций по частоте и особенностям проведения каждого следственного осмотра в течение возможных шести месяцев его производства;

7) совершенствование этапа оценки и использования результатов рассматриваемого следственного действия;

8) разработка тактики взаимодействия следователя со следователем-криминалистом или специалистом на всех этапах рассматриваемого тактического комплекса.

Представляется, что высказанное мнение о комплексном характере получения информации о соединениях между абонентами и (или) абонентскими устройствами, выделенные этапы его производства и направления совершенствования тактического обеспечения могут способствовать формированию полноценного тактического комплекса, направленного на получение, анализ и использование данных сведений в расследовании преступлений.

ЛИТЕРАТУРА

1. Белкин Р.С. Курс криминалистики : в 3 т. Т. 1: Общая теория криминалистики. М. : Юристъ, 1997. 408 с.
2. Minor J.B. Forensic Cell Site Analysis: A Validation & Error Mitigation Methodology // Journal of Digital Forensics, Security and Law. 2017. Vol. 12, № 2. Article 7. DOI: 10.15394/jdfsl.2017.1474
3. Федеральный закон «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» от 01.07.2010 № 143-ФЗ // СПС КонсультантПлюс.
4. Стельмах В.Ю. Следственные действия, ограничивающие тайну связи. М. : Юрлитинформ, 2016. 424 с.
5. Безлепкин Б.Т. Краткое пособие для следователя и дознавателя. М. : Проспект, 2011 // СПС КонсультатнтПлюс.
6. Безлепкин Б.Т. Уголовный процесс в вопросах и ответах : учеб. пособие. 9-е изд., перераб. и доп. М. : Проспект, 2018 // СПС КонсультатнтПлюс.
7. Шейфер С.А. Следственные действия – правомерны ли новые трактовки? // Lex russica (Русский закон). 2015. Т. 107, № 10. С. 115–127.

8. Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи. М., 2010. 192 с.
9. Лапин Е.С. Тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами. М. : Юрлитинформ, 2014. 192 с.
10. Бегишев И.Р., Хисамова З.И., Никитин С.Г. Организация хакерского сообщества: криминологический и уголовно-правовой аспекты // Всероссийский криминологический журнал. 2020. Т. 14, № 1. С. 96–105. DOI: 10.17150/2500-4255.2020.14(1).96-105
11. Minor J.B. Forensic Cell Site Analysis: Mobile Network Operator Evidence Integrity Maintenance Research // Journal of Digital Forensics, Security and Law. 2019. Vol. 14, № 2. Article 5. URL: https://commons.erau.edu/jdfsl/vol14/iss2/5 (дата обращения: 08.02.2020).
12. Князьков А.С. Признаки и система следственных действий // Вестник Томского государственного университета. 2011. № 352. С. 129–133.
13. Дерюгин Р.А. Криминалистические и процессуальные вопросы производства следственного действия, предусмотренного статьей 186.1 Уголовно-процессуального кодекса Российской Федерации // Вопросы безопасности. 2016. № 5. С. 43–48. DOI: 10.7256/2409-7543.2016.5.20396
14. Архипова Н.А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи : автореф. дис. … канд. юрид. наук. СПб., 2011. 25 с.
15. Муленков Д.В., Соколов А.Б., Лазаренко О.Н. Организационно-тактические особенности в деятельности следователя по получению информации о соединениях между абонентами и (или) абонентскими устройствами // Вестник экономической безопасности. 2016. № 1. С. 173–176.
16. Варданян А.А., Цыкора А.А. Правовая природа и тактико-криминалистические особенности производства следственных действий, связанных с получением и анализом информации о телекоммуникационных соединениях между абонентами и (или) абонентскими устройствами // Известия Тульского государственного университета. 2013. № 4-2. С. 21–26.
17. Архипова Н.А., Шебалин А.В. К вопросу об этапах получения информации о соединениях между абонентами и (или) абонентскими устройствами // Юридическая мысль. 2019. № 1 (111). С. 126–130.
18. 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. 176 с.
19. Антонов О.Ю. Тактика получения и использования криминалистически значимой информации от операторов связи // Российский следователь. 2020. № 4. С. 3–7. DOI: 10.18572/1812-3783-2020-4-3-7
20. Цыкора А.А. Тактико-криминалистические особенности производства следственных действий, связанных с получением и исследованием информации, передаваемой по техническим каналам связи : автореф. дис. ... канд. юрид. наук. Ростов н/Д, 2013. 28 с.
21. Скобелин С.Ю. Использование цифровых технологий при доказывании преступной деятельности // Российский следователь. 2019. № 3. С. 26–28.
22. Гудкова М.А. Актуальные вопросы информационно-аналитических исследований // Расследование преступлений. Проблемы и пути их решения. 2018. № 3. С. 155–160.
23. ООО «Основа Лаб». URL. https://osnovalab.ru/solutions/soz/ (дата обращения: 29.01.2020).
24. Чирков П.С. О практике оценки радиоэлектронной обстановки на месте происшествия, получения и анализа информации об абонентах, абонентских устройствах и их соединениях // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития : материалы Междунар. науч.-практ. конф. (Москва, 17 октября 2019 года) / под общ. ред. А.М. Багмета. М. : Московская академия Следственного комитета Российской Федерации, 2019. С. 636–639.
25. Инструкция пользователя. Сервис обработки запросов. Проект «СОЗ» / ООО «Основа Лаб», ПАО «МегаФон» // По материалам отдела криминалистики следственного управления Следственного комитета Российской Федерации по Архангельской области и Ямало-Ненецкому АО.
26. Дерюгин Р.А., Жижилева А.А. О некоторых проблемах производства получения информации о соединениях между абонентами и (или) абонентскими устройствами // Криминалистика – прошлое, настоящее, будущее: достижение и перспективы развития : материалы Междунар. науч.-практ. конф. (Москва, 17 октября 2019 года) / под общ. ред. А.М. Багмета. М. : Моск. академия Следственного комитета Российской Федерации, 2019. С. 219–223.
27. Abba E., Aibinu A.M., Alhassan J.K. Development of multiple mobile networks call detailed records and its forensic analysis // Digital Communications and Networks. Vol. 5, is. 4. P. 256–265. URL: https://doi.org/10.1016/j.dcan.2019.10.005 (дата обращения: 08.02.2020).
28. Россинская Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности // Известия Тульского государственного университета. Экономические и юридические науки. 2016. № 3-2. С. 109–117.
29. Гаврилин Ю.В. Технологии обработки больших объемов данных в решении задач криминалистического обеспечения правоохранительной деятельности // Российский следователь. 2019. № 7. С. 3–8.
30. Mane D., Shibe K. Big Data Forensic Analytics // Balas V., Sharma N., Chakrabarti A. (eds) Data Management, Analytics and Innovation. Advances in Intelligent Systems and Computing. Singapore : Springer, 2019. Vol. 839. DOI: 10.1007/978-981-13-1274-8_9
31. Sachdev H., Wimmer H., Chen L., Rebman C. A New Framework for Securing, Extracting and Analyzing Big Forensic Data // Journal of Digital Forensics, Security and Law. 2018. Vol. 13, № 2. Article 6. DOI: 10.15394/jdfsl.2018.1419
32. Криминалистика : учебник : в 3 ч. Ч. 2. М. : Проспект, 2020. 240 с.
33. Россинская Е.Р. Избранное. М. : Норма, 2019. 680 с.
34. Архипова Н.А. Оценка и использование в доказывании результатов получения информации о соединениях между абонентами и (или) абонентскими устройствами // Сборник материалов криминалистических чтений. 2018. № 15. С. 5–6.
35. Уголовное дело № 2016617152 // По материалам следственного отдела по городу Алушта Главного следственного управления Следственного комитета Российской Федерации по Республике Крым и г. Севастополю.
36. Азаров В.А. Отзыв официального оппонента на диссертацию Р.Я. Мамедова «Способы собирания вещественных доказательств в российском уголовном процессе» // Научный вестник Омской академии МВД России. 2017. № 4 (67). С. 89–93.

Статья представлена научной редакцией «Право» 26 мая 2020 г.

Acquiring Information on Connections Between Subscribers and/or Subscriber Devices in Russia: Essence, Stages and Ways to Improve Tactical Support

Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal, 2020, 459, 221–229.
DOI: 10.17223/15617793/459/27

Oleg Yu. Antonov, Moscow Academy of the Investigative Committee of the Russian Federation (Moscow, Russian Federation). E-mail: antonov@udm.ru

Keywords: information on connections between subscribers and/or subscriber devices; investigative action; forensic tactics; tactical complex.

After the introduction Article 186.1 into the Criminal Procedure Code of the Russian Federation in 2010, there was a discussion about the essence of acquiring information on connections between subscribers and/or subscriber devices in the Russian criminal

procedural and criminalistic literature. Based on the opinions of A.S. Knyazkov, S.A. Sheyfer, V.Yu. Stelmakh, R.A. Deryugin, and N.A. Arkhipova, the author formulates the conclusion that the acquisition of this information consists of provisional processual and organizational procedures for obtaining information and the investigative examination of the obtained information, i.e., it has a complex character. The author proposes to divide the preparatory stage of information acquisition into steps: processual (the investigator's request is prepared and submitted to the court), organizational (the investigator sends the court decision to the organization performing services of communication), and organizational technical (the communication operator collects and provides information). In some investigative situations, it is necessary to carry out an additional preparatory investigative action, investigative examination, in order to establish base stations of all communication operators' various network types simultaneously in a particular place or on a particular route. The existing practice of interaction between the Investigative Committee of the Russian Federation and telecommunication operators within the framework of the query processing system (in particular, with MegaFon, PJSC) actually combines organizational and organizational technical steps of the preparatory stage. On the basis of a study of the practice of the investigative bodies of the Investigative Committee of the Russian Federation, it is proposed that the working stage of the investigative action under consideration should be conducted within the framework of an investigative examination, including with the involvement of a specialist in the field of computer technology and the use of hardware and software systems, or of a forensic investigator on behalf of the investigator. Developing N.A. Arkhipova's opinion, the criteria for assessing the results of the considered investigative action are formulated. The assessment can result in new optional stages of information acquisition: sending a repeated request to the communication operator; obtaining an expert opinion on the results of the information and analytical examination; interrogating a representative of the organization providing communication services. Moreover, decisions on conducting new investigative actions, including those connected with the acquisition of new information on connections between subscribers and/or subscriber devices, can be made.

REFERENCES

1. Belkin, R.S. (1997) *Kurs kriminalistiki: v 3 t.* [A course in forensic science: In 3 volumes]. Vol. 1. Moscow: Yurist".
2. Minor, J.B. (2017) Forensic Cell Site Analysis: A Validation & Error Mitigation Methodology. *Journal of Digital Forensics, Security and Law*. 12 (2). Article 7. DOI: 10.15394/jdfsl 1474
3. Consultant Plus. (2010) *Federal'nyy zakon "O vnesenii izmeneniy v Ugolovno-protsessual'nyy kodeks Rossiyskoy Federatsii" ot 01.07.2010 № 143-FZ* [Federal Law "On Amendments to the Criminal Procedure Code of the Russian Federation" of 01 July 2010 No. 143-FZ]. Moscow: Consultant Plus.
4. Stel'makh, V.Yu. (2016) *Sledstvennye deystviya, ogranichivayushchie taynu svyazi* [Investigative actions limiting the secrecy of communication]. Moscow: Yurlitinform.
5. Bezlepkin, B.T. (2011) *Kratkoe posobie dlya sledovatelya i doznavatelya* [A short guide for the investigator and interrogator]. Moscow: Prospekt.
6. Bezlepkin, B.T. (2018) *Ugolovnyy protsess v voprosakh i otvetakh: ucheb. posobie* [Criminal procedure in questions and answers: A textbook]. 9th ed. Moscow: Prospekt.
7. Sheyfer, S.A. (2015) Nvestigative action – the legitimacy of new interpretation? *Lex Russica*. 107 (10). pp. 115–127. (In Russian).
8. Kozinkin, V.A. (2010) *Ispol'zovanie v rassledovanii prestupleniy informatsii, obnaruzhivaemoy v sredstvakh sotovykh sistem podvizhnoy svyazi* [Use of information found in the means of cellular mobile communication systems in the investigation of crimes]. Moscow: Yurlitinform.
9. Lapin, E.S. (2014) *Taktika polucheniya informatsii o soedineniyakh mezhdu abonentami i (ili) abonentskimi ustroystvami* [Tactic for obtaining information about connections between subscribers and (or) subscriber devices]. Moscow: Yurlitinform.
10. Begishev, I.R., Khisamova, Z.I. & Nikitin, S.G. (2020) The organization of hacking community: Criminological and criminal law aspects. *Vserossiyskiy kriminologicheskiy zhurnal – Russian Journal of Criminology*. 14 (1). pp. 96–105. (In Russian). DOI: 10.17150/2500-4255.2020.14(1).96-105
11. Minor, J.B. (2019) Forensic Cell Site Analysis: Mobile Network Operator Evidence Integrity Maintenance Research. *Journal of Digital Forensics, Security and Law*. 14 (2). Article 5. [Online] Available from: https://commons.erau.edu/jdfsl/vol14/iss2/5 (Accessed: 08.02.2020).
12. Knyaz'kov, A.S. (2011) Features and system of investigative actions. *Vestnik Tomskogo gosudarstvennogo universiteta – Tomsk State University Journal*. 352. pp. 129–133. (In Russian).
13. Deryugin, R.A. (2016) Criminalistic and procedural issues of investigating activities, specified in the article 186.1 of the Criminal Procedure Code of the Russian Federation. *Voprosy bezopasnosti – Security Issues*. 5. pp. 43–48. (In Russian). DOI: 10.7256/2409-7543.2016.5.20396
14. Arkhipova, N.A. (2011) *Organizatsionno-takticheskie aspekty raskrytiya i rassledovaniya prestupleniy v situatsiyakh ispol'zovaniya sredstv mobil'noy svyazi* [Organizational and tactical aspects of disclosing and investigating crimes in situations of using mobile communications]. Abstract of Law Cand. Diss. St. Petersburg.
15. Mulenkov, D.V., Sokolov, A.B. & Lazarenko, O.N. (2016) Organizational and tactical features of investigation aimed to acquiring data on subscribers and (or) subscriber units connections. *Vestnik ekonomicheskoy bezopasnosti*. 1. pp. 173–176. (In Russian).
16. Vardanyan, A.A. & Tsykora, A.A. (2013) Legal nature and basic features production forensic investiga tion regarding the receipt and analysis of information and telecommunication connection between the subscriber and (or) the subscriber device. *Izvestiya Tul'skogo gosudarstvennogo universiteta – Izvestiya Tula State University*. 4-2. pp. 21–26. (In Russian).
17. Arkhipova, N.A. & Shebalin, A.V. (2019) To the question about the stages of obtaining information about connections between subscribers and (or) subscriber devices. *Yuridicheskaya mysl'*. 1 (111). pp. 126–130. (In Russian).
18. Agafonov, V.V., Vazyulin, S.A. & Vasyukov, V.F. (2015) *Osobennosti formirovaniya dokazatel'stv s ispol'zovaniem informatsii o soedineniyakh mezhdu abonentami i (ili) abonentskimi ustroystvami: kriminalisticheskie i protsessual'nye aspekty* [Features of the formation of evidence using information about connections between subscribers and (or) subscriber devices: Forensic and procedural aspects]. Moscow: Yurlitinform.
19. Antonov, O.Yu. (2020) The tactics of receipt and use of criminalistically important information from communications service providers. *Rossiyskiy sledovatel' – Russian Investigator*. 4. pp. 3–7. (In Russian). DOI: 10.18572/1812-3783-2020-4-3-7
20. Tsykora, A.A. (2013) *Taktiko-kriminalisticheskie osobennosti proizvodstva sledstvennykh deystviy, svyazannykh s polucheniem i issledovaniem informatsii, peredavaemoy po tekhnicheskim kanalam svyazi* [Tactical and forensic features of the production of investigative actions related to the receipt and investigation of information transmitted through technical communication channels]. Abstract of Law Cand. Diss. Rostov-on-Don.
21. Skobelin, S.Yu. (2019) Use of digital technologies in proving of criminal activities. *Rossiyskiy sledovatel' – Russian Investigator*. 3. pp. 26–28. (In Russian).
22. Gudkova, M.A. (2018) Aktual'nye voprosy informatsionno-analiticheskikh issledovaniy [Topical issues of information and analytical studies]. *Rassledovanie prestupleniy. Problemy i puti ikh resheniya – Criminal Investigation: Problems and Ways of Their Solution*. 3. pp. 155–160.
23. Osnova Lab. (2020) *Obrabotka zaprosov* [Request processing]. [Online] Available from. https://osnovalab.ru/solutions/soz/ (Accessed: 29.01.2020).
24. Chirkov, P.S. (2019) [On the practice of assessing the radio-electronic situation at the scene of the incident, obtaining and analyzing information about subscribers, subscriber devices and their connections]. *Kriminalistika – proshloe, nastoyashchee, budushchee: dostizhenie i perspektivy*

razvitiya [Criminalistics – past, present, future: Achievement and development prospects]. Proceedings of the International Conference. Moscow 17 October 2019. Moscow: Moscow Academy of the Investigative Committee of the Russian Federation. pp. 636–639. (In Russian).
25. Osnova Lab & MegaFon. (n.d.) *Instruktsiya pol'zovatelya. Servis obrabotki zaprosov. Proekt "SOZ"* [User manual. Request processing service. Project SOZ]. Based on the materials of the Criminalistics Department of the Investigative Department of the Investigative Committee of the Russian Federation for Arkhangelsk Oblast and Yamalo-Nenets Autonomous Okrug.
26. Deryugin, R.A. & Zhizhileva, A.A. (2019) [Some problems of obtaining information on connection between subscribers and (or) subscriber devices]. *Kriminalistika – proshloe, nastoyashchee, budushchee: dostizhenie i perspektivy razvitiya* [Criminalistics – past, present, future: Achievement and development prospects]. Proceedings of the International Conference. Moscow 17 October 2019. Moscow: Moscow Academy of the Investigative Committee of the Russian Federation. pp. 219–223. (In Russian).
27. Abba, E., Aibinu, A.M. & Alhassan, J.K. (2019) Development of multiple mobile networks call detailed records and its forensic analysis. *Digital Communications and Networks.* 5 (4). pp. 256–265. DOI: 10.1016/j.dcan.2019.10.005
28. Rossinskaya, E.R. (2016) The issue of private theory of information and computer software criminalistics operations. *Izvestiya Tul'skogo gosudarstvennogo universiteta. Ekonomicheskie i yuridicheskie nauki – Izvestiya Tula State University. Economic and Legal Sciences*. 3-2. pp. 109–117. (In Russian).
29. Gavrilin, Yu.V. (2019) Technologies for processing big data in solution of tasks of criminalistic support of the law-enforcement activity. *Rossiyskiy sledovatel' – Russian Investigator.* 7. pp. 3–8. (In Russian).
30. Mane, D. & Shibe, K. (2019) Big Data Forensic Analytics. In: Balas V., Sharma N., Chakrabarti A. (eds) *Data Management, Analytics and Innovation. Advances in Intelligent Systems and Computing*. Vol. 839. Singapore: Springer. DOI: 10.1007/978-981-13-1274-8_9
31. Sachdev, H., Wimmer, H., Chen, L. & Rebman, C. (2018) A New Framework for Securing, Extracting and Analyzing Big Forensic Data. *Journal of Digital Forensics, Security and Law.* 13 (2). Article 6. DOI: 10.15394/jdfsl.2018.1419
32. Bagmet, A.M., Bychkov, V.V. & Antonov, O.Yu. (eds) (2020) *Kriminalistika: uchebnik: v 3 ch.* [Forensic science: A textbook: In 3 vols]. Vol. 2. Moscow: Prospekt.
33. Rossinskaya, E.R. (2019) *Izbrannoe* [Selected works]. Moscow: Norma.
34. Arkhipova, N.A. (2018) Otsenka i ispol'zovanie v dokazyvanii rezul'tatov polucheniya informatsii o soedineniyakh mezhdu abonentami i (ili) abonentskimi ustroystvami [Assessment of the results of obtaining information about connections between subscribers and (or) subscriber devices, and their use in proving]. *Sbornik materialov kriminalisticheskikh chteniy.* 15. pp. 5–6.
35. Investigation Department for Alushta of the Main Investigation Department of the Investigative Committee of the Russian Federation for the Republic of Crimea and Sevastopol. (n.d.) *Ugolovnoe delo № 2016617152* [Criminal case No. 2016617152].
36. Azarov, V.A. (2017) Official Opponent's Review of R.Ya. Mamedov's Dissertation "Methods of Collecting Evidence in the Russian Criminal Procedure". *Nauchnyy vestnik Omskoy akademii MVD Rossii – Scientific Bulletin of the Omsk Academy of the MIA of Russia*. 4 (67). pp. 89–93. (In Russian).

Received: 26 May 2020