Федеральное государственное казенное образовательное учреждение высшего образования «Уральский юридический институт Министерства внутренних дел Российской Федерации»

На правах рукописи

ДЕРЮГИН РОМАН АЛЕКСАНДРОВИЧ

ПОЛУЧЕНИЕ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ: ТАКТИКА СЛЕДСТВЕННОГО ДЕЙСТВИЯ И ИСПОЛЬЗОВАНИЕ ЕГО РЕЗУЛЬТАТОВ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Специальность 12.00.12 – криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность

Диссертация на соискание ученой степени

кандидата юридических наук

Научный руководитель –

доктор юридических наук,

профессор А.А. Беляков

Екатеринбург, 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4

ГЛАВА 1. ПОНЯТИЕ И ПРОЦЕССУАЛЬНЫЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ 17

§ 1. Организационные аспекты работы оператора сотовой связи по предоставлению информации о соединениях между абонентами и (или) абонентскими устройствами правоохранительным органам 17

§ 2. Получение информации о соединениях между абонентами и (или) абонентскими устройствами: понятие и значение следственного действия 34

§ 3. Процессуальные особенности и отличие получения информации о соединениях между абонентами и (или) абонентскими устройствами от иных следственных действий и оперативно-розыскных мероприятий 58

ГЛАВА 2. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ АСПЕКТЫ ПРОИЗВОДСТВА ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ 71

§ 1. Типичные следственные ситуации, требующие производства следственного действия «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» и программа действий следователя 71

§ 2. Тактика производства получения информации о соединениях между абонентами и (или) абонентскими устройствами 99

§ 3. Получение информации о соединениях между абонентами и (или) абонентскими устройствами в структуре тактических операций 120

ГЛАВА 3. ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ 146

§ 1. Организация и тактика проведения отдельных следственных действий с учетом информации о соединениях между абонентами и (или) абонентскими устройствами 146

§ 2. Использование результатов следственного действия, предусмотренного статьей 186.1 УПК РФ, при расследовании отдельных видов преступлений 175

ЗАКЛЮЧЕНИЕ 207

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ 211

ПРИЛОЖЕНИЯ 229

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования. Начало XXI века ознаменовано компьютеризацией населения, а также развитием информационно-телекоммуникационных технологий. Современные средства сотовой связи, к которым относятся мобильные (сотовые) телефоны, смартфоны, планшеты и т.п. приобрели огромную популярность, повсеместно распространены и в настоящее время являются одной из самых быстроразвивающихся и перспективных областей радиосвязи. Исходя из данных Международного союза электросвязи, в мире насчитывается больше 6,1 млрд. пользователей сотовой связи. В России за 2016 год количество абонентов (активных SIM-карт[1]) увеличилось до 257 млн., что на 2% больше чем в 2015 году. Аналитиками российского рынка сотовой связи отмечается рост указанных показателей и в 2017 году[2].

Безусловно, достижения научно-технического прогресса и динамичный рост потребительского спроса на услуги связи в стране привел к тому, что практически каждый человек имеет сотовый телефон с широким функционалом, включающим не только обеспечение коммуникации между людьми, доступ к сети Интернет, но и многообразие различных по предназначению приложений. Наряду с положительными моментами, связанными с расширением возможностей средств сотовой связи, отмечаются и негативные факторы. Так, преступность, являясь неотъемлемой частью нашего общества, не могла не отреагировать на перечисленные глобальные феномены. С использованием средств сотовой связи совершаются мошенничества, вымогательства, преступления в сфере компьютерной информации и преступления, связанные с незаконным оборотом наркотических средств, передаются заведомо ложные сообщение об акте

[1] SIM - карта (Subscriber Identification Module (в пер. с англ.) - идентификационный модуль подключения) - карта, с помощью которой обеспечивается идентификация абонентской станции (абонентского устройства), ее доступ к сети подвижной связи, а также защита от несанкционированного использования абонентского номера.

[2] Статистические данные 2015-2016 // URL: http://www.amobile.ru/info.

терроризма, высказываются угрозы и т.п. При помощи сотовой связи координируются действия в преступной группе, совершенствуются схемы и способы совершения преступлений и в целом, происходит расширение границ преступной деятельности. К тому же, сотовые телефоны стали не только средством совершения преступления, но предметом преступных посягательств, увеличив тем самым, долю всех хищений.

Именно негативные последствия распространения средств сотовой связи, стали предпосылкой появления нового следственного действия, предусмотренного статьей 186.1 Уголовно-процессуального кодекса Российской Федерации (Далее УПК РФ) «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». Анализ следственной практики свидетельствует об объективной необходимости совершенствования имеющихся тактических приемов и разработки тактических рекомендаций, обеспечивающих эффективное и рациональное использование возможностей данного следственного действия.

Опыт правоприменительной деятельности позволил выявить проблемы, связанные с получением информации о соединениях между абонентами и (или) абонентскими устройствами.

Во-первых, прослеживается низкий уровень взаимодействия следователя (дознавателя) с оператором сотовой связи. В связи с этим, операторы сотовой связи не всегда предоставляют запрашиваемые сведения в срок, что в свою очередь негативно влияет на раскрытие преступлений по горячим следам;

Во-вторых, возникают сложности в получении судебного решения на производство следственного действия, предусмотренного статьей 186.1 УПК РФ, которое напрямую связано с ограничением конституционных прав граждан на тайну связи. Судами, в одном случае, безосновательно отказывалось в производстве указанного следственного действия, в другом – предполагая получение следователем информации о соединениях между абонентами и (или) абонентскими устройствами, давалось разрешение на производство иных следственных действий (выемка, контроль и запись переговоров);

В-третьих, недостаточная теоретическая разработанность методических рекомендаций, касающихся организации и тактики получения информации о соединениях между абонентами и (или) абонентскими устройствами обусловила появление проблем, связанных с обработкой, систематизацией и закреплением результатов данного следственного действия;

В-четвертых, субъектами расследования уделяется недостаточное внимание криминалистическому значению сведений, получаемых от оператора сотовой связи. Такая информация требует особого анализа, так как является ориентирующей, может повлиять на ход дальнейшего расследования и нередко используется при производстве других следственных действий.

В-пятых, несмотря на высокий технический потенциал получения информации о соединениях между абонентами и (или) абонентскими устройствами, важной проблемой остается установление принадлежности абонентского номера и (или) абонентского устройства конкретному лицу. Данный факт обусловлен тем, что преступники активно конспирируют свою деятельность, используя не один, а несколько сотовых телефонов, с разными SIM-картами, избавляются от них после совершения преступления, путем специального программного обеспечения изменяют уникальные идентификационные номера устройств и т.п.

Вышеперечисленное предопределяет необходимость создания и внедрения в практику расследования преступлений соответствующих теоретических и прикладных рекомендаций, связанных с тактико-криминалистическими и организационными аспектами получения информации о соединениях между абонентами и (или) абонентскими устройствами и свидетельствует об актуальности и высоком уровне научно-практической значимости настоящего исследования.

Степень научной разработанности темы. Анализ научной литературы свидетельствует о том, что вопросам, касающимся получения информации о соединениях между абонентами и (или) абонентскими устройствами частично посвящены диссертации Н.А. Архиповой, А.А. Нуждина, Д.А. Ширева,

А.А. Цыкоры, Л.Г. Юриной, А.В. Ярцевой. Вопросам тактики указанного следственного действия посвящена работа Е.С. Лапина. Процессуальные и организационные аспекты производства следственного действия, предусмотренного статьей 186.1 УПК РФ, нашли отражение в диссертационном исследовании В.Ю. Стельмаха, а также в монографии и учебном пособии Ю.Н. Соколова.

Отдельным аспектам производства получения информации о соединениях между абонентами и (или) абонентскими устройствами посвящены труды ученых и исследователей, которые отражены в статьях и публикациях, учебных пособиях и тезисах выступлений, раскрывающих некоторые проблемные вопросы использования рассматриваемого следственного действия. Это работы В.В. Агафонова, Т.В. Астишиной, Б.Т. Безлепкина, А.А. Белякова, С.А. Вазюлина, В.Ф. Васюкова, А.А. Варданян, О.В. Волынской, Л.Я. Драпкина, В.В. Кальницкого, В.А. Козинкина, Е.В. Маркеловой, С.А. Невского, А.П. Рыжакова, В.А. Семенцова, С.Ю. Скобелина, И.В. Тишутиной, А.В. Ткачева, А.В. Шампорова, А.В. Шебалина, В.С. Шишкина, Н.П. Яблокова, Н.В. Яджина и других российских ученых криминалистики и уголовного процесса, посвятивших свои работы вопросам тактики отдельных следственных действий, тактическим операциям и следственным ситуациям. Безусловно, все работы, посвященные правовым, процессуальным и тактико-криминалистическим аспектам получения информации о соединениях между абонентами и (или) абонентскими устройствами интересны как в теоретическом, так и в практическом отношении. Однако, во-первых, они не исчерпывают всех проблемных аспектов, характеризующих актуальность указанной проблематики; во-вторых, отчасти не лишены дискуссионного характера. Таким образом, уровень научной разработанности темы исследования явно не соответствует реальной степени вовлеченности различных средств сотовой связи в противоправную деятельность виновных лиц, а потому не вполне удовлетворяет потребности правоприменительной практики в сфере расследования преступлений.

Цели и задачи исследования. Целью исследования является научный анализ проблем, связанных с правовыми и тактико-криминалистическими аспектами производства следственного действия, предусмотренного статьей 186.1 УПК РФ, и разработка на этой основе методических рекомендаций по получению информации о соединениях между абонентами и (или) абонентскими устройствами, а также его проведения в структуре тактической операции.

Для достижения указанной цели определены следующие задачи:

- изучить и обобщить нормативную, монографическую и иную литературу по криминалистике, уголовному процессу, оперативно-розыскной деятельности, посвященную особенностям производства следственных действий и оперативно-розыскных мероприятий, направленных на получение и исследование информации, передаваемой с помощью средств сотовой связи;

- исследовать законодательство в области связи и основных принципов работы организаций связи, которые имеют техническую возможность и обязаны в установленном законом порядке, предоставлять следствию информацию о соединениях между абонентами и (или) абонентскими устройствами;

- проанализировать практическую деятельность органов расследования в сфере получения, исследования и использования в уголовном судопроизводстве информации, передаваемой с помощью средств сотовой связи;

- установить и уточнить перечень следственных ситуаций, в которых целесообразно проведение указанного следственного действия и разработать в связи с этим алгоритмы действий следователя;

- рассмотреть получение информации о соединениях между абонентами и (или) абонентскими устройствами в структуре тактических операций в условиях различных следственных ситуаций;

- рассмотреть тактико - криминалистические аспекты производства, а также тактические особенности и специфические проблемы подготовительного, рабочего и заключительного этапа данного следственного действия;

- разработать практические рекомендации по тактике проведения получения информации о соединениях между абонентами и (или) абонентскими

устройствами и использованию его результатов в раскрытии и расследовании преступлений;

- установить и разграничить криминалистическое и доказательственное значение результатов рассматриваемого следственного действия при расследовании различных видов преступлений;

- проанализировать особенности оценки полученной от оператора сотовой связи информации о соединениях между абонентами и (или) абонентскими устройствами и использования ее при расследовании и раскрытии преступлений.

Новизна научного исследования предопределена тем фактом, что получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие существует около семи лет, однако комплексных и масштабных исследований, посвященных криминалистическим аспектам его проведения сравнительно немного.

Впервые на монографическом уровне проведен комплексный анализ проблем, связанных с тактическими и организационными аспектами получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Автором предложено и обосновано определение получения информации о соединениях между абонентами и (или) абонентскими устройствами, выделены цели, задачи следственного действия, дана классификация получаемых сведений; описаны типичные следственные ситуации, в которых целесообразно проведение получения информации о соединениях между абонентами и (или) абонентскими устройствами и разработан соответствующий алгоритм действий следователя; всесторонне исследована тактика данного следственного действия, как на этапе принятия решения, так и при подготовке, непосредственном проведении, фиксации результатов и их использовании в процессе расследования преступлений.

Алгоритмы действий следователя, включающие получение информации о соединениях между абонентами и (или) абонентскими устройствами, разработаны с учетом характера предложенных следственных ситуаций, которые могут быть

простыми, проблемными, конфликтными или мнимо простыми. Также, установлено, что при производстве указанного следственного может возникать организационно-неупорядоченная ситуация.

Подробно исследован вопрос о месте и роли получения информации о соединениях между абонентами и (или) абонентскими устройствами в структуре отдельных тактических операции, а также разработаны соответствующие схемы их реализации с учетом использования указанного следственного действия.

В рамках тактики указанного следственного действия автор обосновал и выделил на подготовительном этапе стадию изучения и систематизации необходимых материалов уголовного дела и стадию подготовки постановления о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами, на основном этапе – техническую и исследовательскую стадии.

Соискателем разработаны практические рекомендации по применению тактических приемов при производстве рассматриваемого следственного действия, а также иных следственных действий с учетом использования результатов получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Теоретическая и практическая значимость исследования заключается в том, что, развивая в теоретическом и практическом аспекте одну из наиболее сложных юридических проблем, носящих междисциплинарный характер, связанных с законодательным ограничением отдельных фундаментальных гарантий защиты прав личности в результате деятельности по расследованию преступлений, данная диссертационная работа содержит элементы нового знания, направленного на повышение эффективности получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Отдельные теоретические положения и выводы, сделанные автором, не только дополняют соответствующие разделы криминалистики, но и способствуют развитию криминалистической тактики отдельных следственных действий, в

особенности получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Выделение автором следственных ситуаций, требующих производство следственного действия, предусмотренного статьей 186.1 УПК РФ, позволяет конкретизировать раздел криминалистической методики расследования отдельных видов и групп преступлений.

Практическое значение диссертационного исследования состоит в том, что сформулированные рекомендации могут быть применены в деятельности следственных органов по раскрытию и расследованию преступлений, связанных с использованием средств сотовой связи, а также при проведении получения информации о соединениях между абонентами и (или) абонентскими устройствами и иных следственных действий.

Результаты настоящего диссертационного исследования могут найти применение в дальнейших монографических и иных научных исследованиях фундаментального и прикладного характера, посвященных аналогичной либо смежной тематике, в учебном процессе вузов и факультетов юридического профиля, особенно юридических вузов МВД России. Отдельные выводы диссертанта могут быть полезны в нормотворческой деятельности по совершенствованию действующего законодательства.

Методология и методика исследования. Методологическую основу диссертационного исследования составили: диалектический метод познания и базирующиеся на нем общенаучные и специальные криминалистические методы, а также труды специалистов в области системных исследований.

Были использованы исходные положения теории познания, а также методы обобщения, систематизации, моделирования, статистический, исторический и формально-логические методы.

Составной частью методологической базы исследования явились конкретно-социологические методы, в соответствии с которыми исследовалась практика досудебного производства, проводились анкетирования, интервьюирования и опросы.

В процессе исследования использовалось конституционное, уголовное, уголовно-процессуальное и иное федеральное законодательство России.

Объяснение, обоснование и развитие положений диссертации осуществлялось на теоретической базе, в основе которой лежат научные исследования, представленные в трудах отечественных криминалистов: Т.В. Аверьяновой, И.В. Александрова, О.Я. Баева, А.Р. Белкина, Р.С. Белкина, А.А. Белякова, И.А. Возгрина, А.Ф. Волынского, Т.С. Волчецкой, В.К. Гавло, И.Ф. Герасимова, Л.Я. Драпкина, А.В. Дулова, В.Н. Долинина, В.Д. Зеленского, Е.П. Ищенко, В.Н. Карагодина, В.П. Лаврова, А.С. Подшибякина, Е.Р. Россинской, А.В. Руденко, В.А. Савельева, А.Г. Филиппова, Е.Е. Центрова, С.А. Шейфера, А.В. Шмонина, Н.П. Яблокова.

Основные положения, выносимые на защиту:

1. Разработано авторское понятие следственного действия получение информации о соединениях между абонентами и (или) абонентскими устройствами, под которым предложено понимать комплексное следственное действие, состоящее в получении от оператора сотовой связи по судебному решению интересующих следствие сведений об абонентах, абонентских устройствах и их соединениях. Предлагается классификация информации, получаемой в ходе производства данного следственного действия, по ее содержанию и в зависимости от использования указанных сведений в процессе расследования по уголовному делу.

2. В рамках получения информации о соединения между абонентами и (или) абонентскими устройствами, кроме характерных для всех следственных действий целей, таких как получение сведений о неустановленных обстоятельствах, а также данных подтверждающих либо опровергающих уже известные факты совершенного преступного деяния, реализуется специальная цель, которая заключается в получение криминалистически значимой информации, отражающей совокупность данных об использовании конкретного абонентского устройства и (или) абонентского номера проверяемым лицом в определенный период времени.

Достижение указанных целей определяет необходимость постановки и решения следующих **задач**:

1. Установление оператора сотовой связи, принадлежность к которому имеет проверяемый абонентский номер;

2. Установление принадлежности абонентского номера и (или) абонентского устройства конкретному лицу;

3. Определение периода времени, за который необходимо получить сведения о соединениях между абонентами и (или) абонентскими устройствами;

4. Подготовка необходимых процессуальных документов, выступающих юридическим основанием для получения информации о соединениях между абонентами и (или) абонентскими устройствами;

5. Обращение к оператору сотовой связи в целях технического исполнения рабочего этапа следственного действия;

6. Анализ полученных результатов, определение объема данных, представляющих доказательственное значение и сведений, носящих информационный характер.

3. Обосновано, что получение информации о соединениях между абонентами и (или) абонентскими устройствами является не только источником сведений, подлежащих доказыванию при производстве по уголовному делу, но и криминалистически значимой (ориентирующей) информации.

4. Автором выработан перечень ситуаций расследования, и соответствующие типичные следственные ситуации. В зависимости от того, как характеризуется каждая следственная ситуация, является ли она простой, проблемной, конфликтной или мнимо простой, разработан алгоритм действий следователя, в котором с учетом обстоятельств используется получение информации о соединениях между абонентами и (или) абонентскими устройствами.

5. Установлено, что некоторые простые следственные ситуации, для успешного разрешения которых в рамках следственного действия, предусмотренного статьей 186.1 УПК РФ, получена информация от оператора

сотовой связи, могут оказаться мнимо простыми. В таком случае алгоритм действий следователя усложняется дополнительными следственными действиями и иными мероприятиями.

6. Аргументирована необходимость включения получения информации о соединениях между абонентами и (или) абонентскими устройствами в структуру тактических операций по установлению лиц, причастных к совершению преступления, по изобличению подозреваемых, обвиняемых, проверке алиби лица, по проверке признательных показаний подозреваемого, обвиняемого и других лиц.

7. Обосновано, что получение информации о соединениях между абонентами и (или) абонентскими устройствами в структуре тактических операции может играть роль вспомогательного звена, а также иметь центральное значение в зависимости от сложившейся следственной ситуации.

8. В целях повышения эффективности производства получения информации о соединениях между абонентами и (или) абонентскими устройствами, в рамках существующей системы поэтапного проведения следственных действий, предлагается на подготовительном и основном (рабочем) этапах выделить самостоятельные стадии. В связи с этим, подготовительный этап включает стадию изучения и систематизации необходимых материалов уголовного дела и стадию подготовки постановления о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами, а основный (рабочий) этап – техническую и исследовательскую стадии.

9. Определено, что на отдельных этапах проведения получения информации о соединениях между абонентами и (или) абонентскими устройствами используются тактические приемы, присущие выемке предметов и документов, составляющих охраняемую законом тайну, контролю и записи переговоров, а также следственному осмотру предметов и документов, при этом необходимость применения конкретного тактического приема обусловлена соответствующей стадией рассматриваемого следственного действия.

10. Разработан комплекс тактических рекомендаций по повышению результативности следственных действий, в ходе которых с учетом различных ситуаций, осуществляется получение и анализ информации об абонентах и их соединениях (выемка, обыск, осмотр сотового телефона, очная ставка, осмотр места происшествия). Определено, что результаты получения информации о соединениях между абонентами и (или) абонентскими устройствами, могут повлиять на принятие решения о последующих следственных действиях или тактику их проведения.

Степень достоверности и апробация результатов исследования.

В процессе исследования было проведено анкетирование 129 сотрудников правоохранительных органов, в числе которых следователи, дознаватели, а также руководители следственных подразделений и отделов дознания, расположенных на территории Свердловской области, Пермского края, Тюменской области, Челябинской области, Ямало-Ненецкого автономного округа. Автором было изучено 174 уголовных дела, расследовавшихся в период с 2011 по 2018 г.г., при расследовании которых применялось следственное действие, предусмотренное статьей 186.1 УПК РФ, либо использовалась информация об абонентах или их соединениях.

Основные положения диссертационного исследования докладывались на научно-практических конференциях международного и всероссийского уровня: «Актуальные проблемы правоохранительной деятельности органов внутренних дел» (г. Екатеринбург, 2016), «Актуальные проблемы раскрытия и расследования преступлений» (г. Екатеринбург, 2016), «Оптимизация деятельности органов предварительного следствия и дознания: правовые, управленческие и криминалистические проблемы» (г. Москва, 2017), «Актуальные вопросы противодействия преступности в России и зарубежом» (г. Екатеринбург, 2016), «Правовые проблемы информационной безопасности теория и практика» (г. Екатеринбург, 2016), «Проблемы современной криминалистики и основные направления ее развития в XXI веке» (г. Екатеринбург, 2016), «Криминалистика и судебно-экспертная деятельность: теория и практика» (г. Краснодар, 2017),

«Деятельность правоохранительных органов в современных условиях» (г. Иркутск, 2017), «Актуальные проблемы криминалистической теории и практики» (г. Калининград, 2017), «59-е ежегодные криминалистические чтения» (г. Москва, 2018), «Деятельность правоохранительных органов в современных условиях» (г. Иркутск, 2018).

Некоторые положения, сделанные соискателем, внедрены в деятельность следственных подразделений и отделов дознания (СО МО МВД России «Южноуральский» Челябинской области, ОМВД России по Еманжелинскому району Челябинской области, ОП №7 УМВД России по г. Тюмени, Сургутский ЛО МВД России на транспорте).

Результаты диссертационного исследования нашли отражение в 18 научных статьях, 5 из которых опубликованы в изданиях, рекомендованных ВАК Минобрнауки России.

Структура диссертации соответствует теме и логике проведенного исследования и представлена введением, тремя главами, включающими восемь параграфов, заключением, списком использованных источников и литературы, приложений.

ГЛАВА 1. ПОНЯТИЕ И ПРОЦЕССУАЛЬНЫЕ ОСОБЕННОСТИ ПРОИЗВОДСТВА ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ

§ 1. Организационные аспекты работы оператора сотовой связи по предоставлению информации о соединениях между абонентами и (или) абонентскими устройствами правоохранительным органам

Современное общество можно по праву считать информационным, так как за последние годы его развития значительно расширились возможности технических средств, а в особенности средств сотовой связи. Информационное общество – это первое приближение к информационным знаниям, которое отражает современное состояние информационной эпохи, сквозь его призму происходит осознание и понимание правоведами той самой информационной парадигмы развития общества[3]. В литературе последнего времени данному понятию уделяется довольно много внимания. Для понимания феномена информационного общества важно раскрыть его признаки. Данный вопрос подробно освещен Кузнецовым П.У., Волковым Ю.В., Морозовым А.В., Стрельцовым А.А., Соколовым Ю.Н., Ниесовым В.А., Паршуковым М.И., которые выделяют следующие признаки информационного общества:

1. Высокоразвитая информационная инфраструктура и массовая глобальная информатизация. К инфраструктуре относятся такие компоненты как персональные компьютеры, системы связи, средства связи, цифровые системы передачи данных, высокие информационные технологии и др.

2. Широкий доступ к информационным ресурсам. Технические и технологические возможности общества в использовании информации остаются всего лишь возможностями. Для реализации информационных потребностей необходимо создавать условия доступности к информационным ресурсам.

---

[3] Кузнецов П.У. Информационные технологии в юридической деятельности: учебник для академического бакалавриата – 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2017. –. С. 111.

3. Рынок информационных продуктов. Общество, основанное на знаниях, требует цивилизованного процесса оборота информационных продуктов, т е материальных и нематериальных объектов информационного характера имеющих потребительские свойства. Информационный рынок – это свободный оборот информационных продуктов и услуг производство и реализация, которых зависит от общественных потребностей в рамках, определяемых государством.

4. Информационный сектор экономики. ИКТ – сектор экономики – это та ее сфера, которая связана с производством финансированием и потреблением информационных продуктов, включая программные продукты и технологии электронной техники телефонии и электросвязи телекоммуникаций и многих других товаров и услуг, которые пользуются все большим спросом у потребителей.

5. Высокий уровень информационной культуры. Основной критерий развития информационного общества тесно связан с самим человеком с его духовным содержанием с его поступками в новом, технологически обустроенном мире. Поэтому проблемы нравственности и этики будут определяющими[4].

ИКТ – сектор экономики – один из признаков информационного общества, который кроме всего прочего включает в себя сотовую связь. Она же в свою очередь представляет собой целую систему, которая обеспечивает возможность общения людей всех социальных слоев населения, любого возраста, пола, профессии. Следует отметить, что в Постановлении Правительства Российской Федерации от 23 января 2006 г. № 32 г. Москва «Об утверждении Правил оказания услуг связи по передаче данных» и Постановлении Правительства Российской Федерации от 9 декабря 2014 г. № 1342 г. Москва «О порядке оказания услуг телефонной связи» такой термин как сотовая связь отсутствует. В законе это услуга подвижной радиотелефонной связи. Однако, для упрощения некоторых формулировок в исследовании будет использовано более

---

[4] Кузнецов П.У. Информационные технологии в юридической деятельности: учебник для академического бакалавриата – 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2017. – С. 112 - 116.

обыденное и привычное словосочетание «сотовая связь». Аналогично, в диссертационном исследовании соискатель использует бытовые названия абонентских устройств или абонентских терминалов[5]: мобильные (сотовые) телефоны, смартфоны, коммуникаторы, абонентские средства связи.

Примечательно, что термин «мобильный телефон» (сотовый телефон) широко используется не только в повседневном обиходе, но и в специальной литературе, а также в правоприменительной деятельности, но законодательно до сегодняшнего дня не закреплен. Исходя из смысла понятий абонентская станция (абонентское устройство)[6] и пользовательское оконечное оборудование[7] следует, что к ним относятся и мобильные (сотовые) телефоны. Данные термины имеют схожую смысловую нагрузку и связаны между собой, так как представляют технические средства связи, предназначенные для передачи или приема сигналов электросвязи, находящиеся в пользовании абонентов. В связи с этим, нами поддерживается позиция Н.А. Архиповой, о законодательном закреплении «мобильного (сотового) телефона» как термина, относящегося к законодательству о связи[8]. К тому же, данные о технических возможностях и характеристиках сотового телефона, имеют криминалистическое значение и способствуют установлению механизма преступления.

Мобильные телефоны, смартфоны и коммуникаторы, обладающие многофункциональным интерфейсом, являются наиболее популярными среди технических средств связи. Анализ следственной и судебной практики показывает, что сотовая связь стала основным средством передачи информации между

---

[5] Абонентский терминал - пользовательское (оконечное) оборудование, используемое абонентом и (или) пользователем для подключения к узлу связи сети передачи данных с помощью абонентской линии.

[6] Об утверждении Правил оказания услуг подвижной связи: постановление правительства Российской Федерации от 25 мая 2005 г. № 328. – [Электронный ресурс]. − URL: http:// www.consultant.ru.

[7] О связи: федеральный закон от 07.07.2003 № 126-ФЗ. (действующая редакция). – [Электронный ресурс]. − URL: http:// www.consultant.ru.

[8] Архипова Н.А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи: автореф. дис. … канд. юрид. наук / Н.А. Архипова. – СПб.: Санкт-Петербургский университет МВД России, 2011. С. 12.

преступниками. Последние используют возможности сотовой связи в целях координации преступной деятельности, установления и поддержание связи в преступной группе, при подготовке, совершении и сокрытии преступлений, а также оказания противодействия правоохранительным органам.

В действующем УПК РФ «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» закреплено как следственное действие, которое представляет собой процессуальное средство получения интересующих следствие сведений об абонентах и абонентских устройствах. В целях уяснения сущности и правовой природы указанного следственного действия, считаем необходимым, рассмотреть понятие информации, технические возможности оператора сотовой связи, информационные свойства и принцип работы средств сотовой связи.

Обратим внимание на тот факт, что информация, получаемая путем производства следственного действия, предусмотренного статьей 186.1 УПК РФ, может быть как опосредствованной, так и непосредственно-составляющей способ совершения преступления, а соответственно, используемой для целей раскрытия и расследования преступлений в качестве ориентирующей и доказательственной информации. Так, согласно данным опроса, указанная информация использовалась в качестве доказательственной в 44,2% случаев; ориентирующей – в 30,2%, результаты позволили определить дальнейший ход расследования – 22,5 % и послужили предпосылкой последующих следственных действий – 38% от общего количества случаев ее использования[9].

Информация, сосредоточенная в базе данных оператора сотовой связи, может иметь значение для следствия при фактически любом преступлении (убийство, разбой, вымогательство, незаконный оборот наркотических средств и др.), в том числе преступлениях, совершаемых в сфере мобильных телекоммуникаций (неправомерный доступ к компьютерной информации; незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств и программного обеспечения и др.). По результатам опроса

[9] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

следователей (дознавателей) было отмечено, что получение информации о соединениях между абонентами и (или) абонентскими устройствами применяется практически по всем категориям уголовных дел[10].

В.А. Козинкин сформулировал определение информации, сосредоточенной в средствах сотовых систем подвижной связи – это информация, возникающая в ходе эксплуатации пользовательского оборудования непосредственно в нем самом, а также в операционно-информационных системах и центрах коммутации оператора подвижной связи[11].

Вышесказанное позволяет нам предложить классификацию сведений, имеющих криминалистическое значение, получаемых посредством производства получения информации о соединениях между абонентами и (или) абонентскими устройствами. В зависимости от места накопления информации выделим:

- сосредоточенную в пользовательском оборудовании (абонентское устройство связи);

- сосредоточенную в базе данных, информационных системах оператора сотовой связи.

К первой группе относится информация созданная абонентом в процессе пользования услугами, предоставляемыми оператором связи. Основными из них в настоящее время являются: данные о входящих (исходящих) вызовах (телефонная книга вызовов); телематические услуги связи (передача сообщений, использование интернет-трафика)[12].

Ко второй группе – входящие/исходящие вызовы, сообщения, с указание времени, длительности соединения, данные о местоположении абонентского устройства, точные дата время совершения действий с абонентским терминалом и сведения об устройстве, об абоненте, данные SIM-карты, идентификационный

---

[10] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

[11] Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи: дисс. …канд. юрид. наук. Ижевск, 1998. С.44.

[12] Об утверждении Правил оказания телематических услуг связи: постановление правительства Российской Федерации от 10 сентября 2007 г. № 575 г. Москва // Российская газета - № 622 (0). – [Электронный ресурс]. – https://rg.ru/2007/09/25/svyaz-pravila-dok.html.

номер IMEI[13], а также дублируется, систематизируется и хранится информация созданная абонентом.

В процессе обобщения практики раскрытия и расследования преступлений были выявлены следующие категории информации, полученной от операторов сотовой связи:

- персональные данные абонента (фамилия, имя, отчество, паспортные данные, адрес места жительства), определяемые по номеру телефона;
- IMEI-код пользовательского оборудования, устанавливаемый по номеру телефона;
- протокол соединений фиксированного номера абонента за определенный период времени (протокол или детализация соединений);
- протокол соединений абонентов оператора связи через конкретную базовую станцию за определенный период времени (контрольный звонок);
- данные о местонахождении абонента или аппарата мобильной связи в зоне действия той или иной базовой станции данного оператора сотовой связи в указанное время. Эти сведения позволяют установить точное местонахождение звонившего (или получившего входящий звонок) в интересующее следствие время;
- протокол соединений абонента с фиксированным IMEI-кодом телефонного аппарата за определенный период времени;
- IMEI-код пользовательского оборудования и перечень абонентов, его использовавших по абонентскому номеру.

Указанные сведения, обобщенные в детализации телефонных соединений абонента, формируются и накапливаются в информационных банках операторов сотовой связи, разумеется, вне связи с каким-либо общественно опасным деянием, но в ряде случаев, при условии использования участником уголовного

---

[13] IMEI - International Mobile Equipment Identifier (международный идентификатор мобильного оборудования). // Приказ Министерства информационных технологий и связи РФ от 19 февраля 2008 г. № 21 «Об утверждении Правил применения абонентских станций (абонентских радиостанций) сетей подвижной радиотелефонной связи стандарта GSM-900/1800»

судопроизводства, средства сотовой связи являются значимыми для раскрытия и расследования преступления.

Для полноты исследования актуальным представляется изучение процесса формирования и хранения данных об абонентах и абонентских устройствах как источника получения доказательственной и криминалистически значимой информации.

Итак, деятельность операторов сотовой связи, кроме уже затронутых нормативно-правовых актов, регулируется Федеральным законом от 7 июля 2003 года № 126-ФЗ «О связи». Федеральный закон определяет правовые основы деятельности, полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи. В соответствие с п. 12 ст. 2 Федерального закона «О связи» оператор связи – это юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии[14]. Под юридическим лицом следует понимать коммерческую организацию (телефонную компанию), которая предоставляет мобильные услуги для своих абонентов. Все функционирующие на территории России операторы сотовой связи можно разделить на две группы (по признаку зоны фактического покрытия). К первой группе отнесем операторы федерального значения - МегаФон, МТС (Мобильные ТелеСистемы), ВымпелКом (бренд Билайн), Т2 Мобайл (бренд Tele2). Вторая группа включает в себя операторов регионального уровня: МОТИВ (Екатеринбург-2000), Смартс, Скай Линк, Ю-тел (УралСвязьИнформ) и другие. По данным интернет портала 8sot.su в Российской Федерации насчитывается 18 операторов сотовой связи[15].

Вышеуказанные операторы оказывают услуги связи пользователям на основании договора об оказании услуг связи, который заключается в соответствие с гражданским законодательством и правилами оказания услуг подвижной связи

---

[14] О связи: федеральный закон от 07.07.2003 № 126-ФЗ. (действующая редакция). – [Электронный ресурс]. − URL: http:// www.consultant.ru.

[15] Сотовые операторы России - 8sot – [Электронный ресурс]. − URL: http://8sot.su/ru/operators.

(Далее Правила)[16]. Договор заключается в письменной форме в двух экземплярах. Заключение договора путем осуществления конклюдентных действий допускается в порядке исключения, только при оказании разовых услуг по передаче данных в пунктах коллективного доступа.

В договоре должны быть указаны следующие данные об абоненте:

а) дата и место заключения договора;

б) наименование (фирменное наименование) оператора связи;

в) реквизиты расчетного счета оператора связи;

г) сведения об абоненте – фамилия, имя, отчество (при наличии), место жительства, реквизиты основного документа, удостоверяющего личность для гражданина; наименование (фирменное наименование) организации, место нахождения (юридический адрес и адрес фактического нахождения), номер свидетельства о государственной регистрации юридического лица, индивидуальный номер налогоплательщика для юридического лица;

д) адрес, порядок и способ предоставления счета за оказанные услуги телефонной связи;

е) срок обеспечения доступа к сети местной или подвижной связи[17].

Оператор связи обязан осуществлять проверку достоверности сведений об абоненте (ч. 6 ст. 44 Федерального закона «О связи»).

Пользователь, заключивший такой договор, именуется абонентом. Понятие абонента находит отражение как в федеральном законе «О связи», так и в вышеуказанных правилах, и принципиальных отличий не имеет. Абонент – это физическое лицо (гражданин) или юридическое лицо, с которым заключен договор об оказании услуг подвижной связи при выделении для этих целей абонентского номера или уникального кода идентификации. В соответствие с п. 2 указанных Правил, под абонентским устройством (абонентской станцией)

---

[16] Об утверждении Правил оказания услуг подвижной связи: постановление правительства Российской Федерации от 25 мая 2005 г. № 328. – [Электронный ресурс]. − URL: http://www.consultant.ru.

[17] О порядке оказания услуг телефонной связи: постановление правительства Российской Федерации от 9 декабря 2014 г. № 1342 г. Москва. – [Электронный ресурс]. − URL: http://www.consultant.ru.

понимается - пользовательское (оконечное) оборудование, подключаемое к сети подвижной связи. Установление в результате вызова взаимодействия между средствами связи, позволяющее абоненту передавать и (или) принимать голосовую и (или) неголосовую информацию понимается как соединение по сети подвижной связи (установление соединения между абонентскими устройствами). Интересен тот факт, что в Федеральном законе «О связи» не используется понятие абонентского устройства, альтернативой выступают средства связи, под которыми понимаются технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи, включая технические системы и устройства с измерительными функциями. На наш взгляд, это более полное и достаточно подробное определение, так как охватывает весь комплекс технических устройств, которые посредством сотовой сети позволяют обеспечить связь между абонентами.

Исходя из п. 24 ст. 2 Федерального закона «О связи», все средства связи функционируют не изолированно, а во взаимодействии, образуя единую сеть электросвязи, то есть технологическую систему, включающую в себя средства и линии связи и предназначенную для электросвязи[18]. По смыслу уголовно-процессуального закона, путем производства следственного действия, предусмотренного статьей 186.1 УПК РФ, получаются сведения, переданные средствами электросвязи.

Согласно ст. 12 Федерального закона «О связи» к электросвязи относятся:

- сеть связи общего пользования;

- выделенные сети связи;

- технологические сети связи, присоединенные к сети связи общего пользования;

---

[18] О связи: федеральный закон от 07.07.2003 № 126-ФЗ. (действующая редакция). – [Электронный ресурс]. − URL: http:// www.consultant.ru.

- сети связи специального назначения и другие сети связи для передачи информации при помощи электромагнитных систем[19].

Правила оказания услуг телефонной связи регулируют отношения между абонентом и пользователем услуг телефонной связи и оператором связи при оказании услуг местной, внутризоновой, междугородной и международной телефонной связи в сети связи общего пользования[20]. Исходя из закона это виды телефонной связи.

Для уяснения сущности процедуры получения информации о соединениях между абонентами и (или) абонентскими устройствами представляется необходимым подробнее рассмотреть телефонную связь, которая в свою очередь подразделяется на связь с подвижными объектами.

Под подвижной (мобильной) связью понимается такая связь между абонентами, при осуществлении которой доступ к абонентским линиям с абонентским устройством осуществляется по радиоканалу, а месторасположение абонентов может меняться. Одной из разновидностей (подвижной) мобильной связи является сотовая связь. Главная отличительная особенность этого вида связи состоит в том, что общая зона покрытия делится на ячейки (соты), определяющиеся зонами покрытия отдельных базовых станций. Соты частично перекрываются и вместе образуют сеть. Совокупность ячеек образует зону обслуживания.

В мире существует несколько стандартов сотовой связи, из которых в Российской Федерации наиболее распространены GSM нескольких модификаций, и ограниченно используются CDMA, однако на данный момент она устарела. Стандарт GSM в России использует частоты в 900 и 1800 МГц. Крупнейшие сети 3G в стране работают на технологии WCDMA и работают на частотах 2000-2100 МГц. Скорости передачи данных в таких сетях несравненно выше, чем в сети

---

[19] О связи: федеральный закон от 07.07.2003 № 126-ФЗ. (действующая редакция). – [Электронный ресурс]. − URL: http:// www.consultant.ru.

[20] О порядке оказания услуг телефонной связи: постановление правительства Российской Федерации от 9 декабря 2014 г. № 1342 г. Москва. – [Электронный ресурс]. − URL: http:// www.consultant.ru.

GSM. В настоящее время большая часть устройств поддерживает 4G, которая представлена двумя стандартами — LTE (791-862 МГц) и Wi-Max (2500-2600 МГц).

Сотовые сети разных операторов соединены друг с другом, а также со стационарной телефонной сетью. Это позволяет абонентам одного оператора делать звонки абонентам другого оператора, с мобильных телефонов на стационарные и со стационарных на мобильные. Кроме того, операторы сотовой связи активно заключают между собой договоры роуминга, благодаря которым абонент, находясь вне зоны покрытия своей сети, может совершать и принимать звонки через сеть другого оператора.

Таким образом, основными составляющими сотовой сети выступают базовый коммутатор («сердце»), базовые станции и абонентские устройства (оконечное оборудование).

Базовая станция применительно к сотовой связи – это комплекс радиопередающей аппаратуры (ретрансляторы, радиоприемники), осуществляющий связь с оконечным абонентским оборудованием – сотовым телефоном. Сети мобильной связи между собой делятся на географические области, зоны покрытия от антенн базовой станции, которые именуются сотами. Таким образом, между мобильными телефонами и сетью поддерживается постоянный контакт, в зависимости от перемещения абонентов в ту или иную соту.

Каждый сотовый телефон, находясь в режиме ожидания, с определённой периодичностью, активно, без непосредственного участия абонента, отслеживает сигналы базовых станций и передаёт сигнал с оконечного устройства на базовую станцию. Далее информация о поступивших сигналах фиксируется в базе данных оператора связи и оперативно используется для подключения входящих звонков. Последующая регистрационная информация уничтожает предыдущую, оставляя для работы актуальную, полученную в последний момент времени. Использование данного принципа даёт возможность в режиме реального времени оперативно устанавливать местонахождение абонентского устройства

(конкретного сотового телефона, используемого преступником) с привязкой к той или иной местности с точностью до нескольких метров, зависящей от размера самой соты, которая, в свою очередь, зависит от количества абонентов и интенсивности радиообмена. Отметим, что современный пользователь нуждается в постоянном доступе к сети Интернет и оставляет данную функцию на устройстве включенной по умолчанию. Таким образом, даже без осуществления звонков, сотовый телефон автоматически с некоторой периодичностью передает сигнал на базовую станцию об использовании интернет трафика, что отражает его перемещение на местности и фиксируется в геопозиции. Данный факт в очередной раз подтверждает, что технические возможности оператора связи, позволяют правоохранительным органам получить криминалистически важные сведения, представляющие интерес для следствия.

Сотовые телефоны являются оконечным оборудованием, непосредственно с которого и ведутся переговоры. Первоначально, на ранних стадиях развития сотовой связи, идентификацию абонента в сети проводили по заводскому номеру сотового телефона – ESN (англ. Electronic Serial Number). Таким образом, и абонентское устройство (сотовый телефон), и абонент идентифицировались единым кодом. Данный подход порождал полную зависимость номера абонента и пакета, предоставляемых ему услуг от конкретного экземпляра телефона. Поменяв, в том числе вынужденно, сотовый телефон, абонент должен был обращаться в офис оператора связи для перепрограммирования сотового телефона и внесения его нового серийного номера в базу данных оператора.

Со временем, исходя из интересов абонентов, сформировалась точка зрения, что более удобна идентификация абонента, независимая от телефона. В стандарте GSM было предложено выделить аутентификацию[21] абонента с помощью съемного модуля SIM (SIM-карты[22]) и оборудования, которому свойственен

[21] Аутентификация (англ. Authentication), или подтверждение подлинности – процедура проверки соответствия субъекта и того, за кого он пытается себя выдать, с помощью некой уникальной информации, в простейшем случае – с помощью имени и пароля. – Словарная статья. – [Электронный ресурс] − URL: http://ru.wikipedia.org.

[22] SIM - карта (Subscriber Identification Module (в пер. с англ.) - идентификационный модуль подключения) - карта, с помощью которой обеспечивается идентификация абонентской станции

уникальный код IMEI (англ. International Mobile Equipment Identifier – Международный идентификатор мобильного оборудования).

С помощью SIM-карты обеспечивается идентификация абонентской станции (абонентского устройства), ее доступ к сети подвижной связи, а также защита от несанкционированного использования абонентского номера[23]. Основная функция SIM-карты – это хранение идентификационной информации об аккаунте (совокупности знаков, набор которых дает возможность выйти в сеть). SIM-карта состоит из микрочипа, включенного в пластиковый корпус. В зависимости от размера и применимости к различным модификациям сотовых телефонов SIM-карты бывают четырех видов: классическая, мини SIM-карта, микро-SIM-карта и нано- SIM-карта. В настоящий момент распространение получает мульти-SIM-карта, отличительной особенностью которой, является возможность сочетания в себе нескольких абонентских номеров одного или более операторов связи. Чип, установленный в SIM-карту, состоит из микросхем микропроцессора и памяти (ROM и RAM). В память ROM оператор связи записывает код абонента IMSI, который уникален и является идентификатором SIM-карты в сети. Данный код содержит в себе следующие составляющие:

- MCC (код страны) – первые три цифры;
- MNC (код мобильной сети) – четвертая и пятая цифры;
- MSIN (идентификационный номер абонента) – остальные цифры.

В память RAM записываются пользовательские данные: телефонные номера, SMS-сообщения, коды PIN и PUK. Криминалистическое значение представляет то, что на SIM-карте может быть отражена информация об операторе связи, о последних набранных номерах, контактах других абонентов, сохраненных в памяти, сведения об отправленных и полученных SMS, об оплате услуг, о примерном местонахождении абонента, а также о номере IMSI.

(абонентского устройства), ее доступ к сети подвижной связи, а также защита от несанкционированного использования абонентского номера.

[23] Об утверждении Правил оказания услуг подвижной связи: постановление правительства Российской Федерации от 25 мая 2005 г. № 328. – [Электронный ресурс]. − URL: http:// www.consultant.ru.

Частично согласимся с мнением В.Ф. Васюкова о том, что SIM-карта по своей сути является полноценным абонентским устройством, так как обладает микрокомпьютером с операционной и файловой системой[24]. Хотя правильнее сказать, что SIM-карта – техническое устройство с собственной операционной системой, обеспечивающее работу абонентского терминала в сетях связи. Но бесспорным остается то, что при обнаружении SIM-карты на месте происшествия, для получения от оператора связи информации, находящейся на ней, несомненно, после осмотра, необходимо производство следственного действия, предусмотренного статьей 186.1 УПК РФ. Вышесказанное подтверждается данными проведенного анкетирования следователей, дознавателей (96,9% ответивших, указали, что в случае обнаружения на месте происшествия SIM-карты или абонентского устройства связи далее ими проводилось получение информации о соединениях между абонентами и (или) абонентскими устройствами)[25].

Сведения запрашиваются по коду IMSI, находящегося на корпусе SIM-карты. SIM-карта выдается оператором связи, обязанностью которого, оформляя договор об оказании услуг сотовой связи, является формирование базы данных из сведений, полученных при подключении абонента-гражданина (фамилия, имя, отчество, место жительства и реквизиты основного документа удостоверяющего личность, представленные при личном предъявлении абонентом указанного документа), а также юридического лица (наименование (фирменное наименование) юридического лица, его местонахождение, а также список лиц, использующих оконечное оборудование юридического лица, заверенный уполномоченным представителем юридического лица, в котором указаны их фамилии, имена, отчества, места жительства и реквизиты основного документа удостоверяющего личность)[26].

---

[24] Васюков В.Ф. Особенности раскрытия и расследования грабежей и разбоев, совершаемых на открытой местности: дисс. …канд. юрид. наук. Орел, 2009. С.106.

[25] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

[26] Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность:

Установить абонента кроме как по SIM-карте, можно при помощи IMEI-кода оборудования и абонентскому номеру. Идентификационный код IMEI присваивается каждому устройству связи фирмой производителем и является уникальным для отдельного средства связи. Как правило, IMEI указывается в четырёх местах: в абонентском устройстве (в большинстве случаев его можно вывести на экран набором *#06# на клавиатуре), под аккумуляторной батареей, на упаковке и в гарантийном талоне. IMEI играет роль серийного номера аппарата при авторизации в сети, передаётся в эфир при авторизации в сети. Современная структура IMEI (Таблица 1).

Таблица 1.

TAC — Type Allocation Code		**Serial No**	**Check Digit**
Reporting Body Identifier	**Type Identifier**	**Serial number**	**Check Digit**
NN	**XXXX XX**	***ZZZZZZ***	**A**
Типовой код распределения		Серийный номер	Проверочный код

IMEI код является уникальным и при работе средств сотовой связи остается неизменным, поэтому в случае хищений мобильных телефонов, его установление является важной составляющей успешного поиска и раскрытия преступления.

Оператор сотовой связи может также предоставить интересующую следствие информацию на основании судебного решения, если известен абонентский номер. Абонентский номер - номер, однозначно определяющий (идентифицирующий) подключенную к сети подвижной связи абонентскую станцию (абонентское устройство) с установленной в ней SIM-картой[27]. Он присваивается при заключении договора с оператором сотовой связи и, как правило, является уникальным. Изменения в Федеральный закон «О связи»,

---

постановление правительства Российской Федерации от 27 августа 2005 г. № 538 (ред. от 10.04.2013) // Собрание законодательства Российской Федерации. 2005. – № 36 ст. 3704.

[27] Об утверждении Правил оказания услуг подвижной связи: постановление правительства Российской Федерации от 25 мая 2005 г. № 328. – [Электронный ресурс]. − URL: http:// www.consultant.ru.

вступившие в силу с 1 декабря 2013 года, позволяют абонентам сохранять свой номер даже при смене оператора сотовой связи, при условии, отсутствия задолжности на счету и расторжения договора со старым оператором связи, и заключением договора с новым оператором.

По абонентскому номеру устанавливаются: сведения о номере IMEI похищенного мобильного телефона; о том, использовался ли мобильный телефон после хищения; были ли произведены с него звонки, отосланы сообщения. Если да, то, по каким номерам происходили соединения с похищенного телефона, их продолжительность, а также персональные данные абонентов, с которыми происходили соединения.

Таким образом, оператор сотовой связи, имея технические возможности по доступу к информации, сформированной в его базах данных, может отслеживать и предоставлять следствию данные о соединения между абонентами телефонной связи по IMEI-коду телефона, по номеру SIM-карты, или по абонентскому номеру. При этом базы данных операторов связи содержат сведения обо всех этих параметрах, поэтому, установив абонентский номер, можно выяснить IMEI телефона, а по нему – номера всех SIM-карт, которые когда-либо устанавливались в данном телефоне.

Информацию о соединениях между абонентами и (или) абонентскими устройствами, оператор связи предоставляет следователю в виде **детализации**. Исходя из УПК РФ, она представляет сведения о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведения о номерах и месте расположения приемопередающих базовых станций[28].

Получение и накопление операторами связи данных об абонентах, в том числе фиксация соединений между абонентами, производится не для потребностей правоохранительных органов, а в целях упорядоченного

[28] Уголовно-процессуальный кодекс Российской Федерации (действующая редакция). – [Электронный ресурс]. − URL: http:/www.consultant.ru.

регулирования гражданских правоотношений, возникающих при осуществлении услуг связи, и должного исполнения заключенных договоров (прежде всего – правильности расчетов за услуги связи). Комплекс процессов и решений на предприятиях связи, ответственных за сбор информации об использовании телекоммуникационных услуг, их тарификацию, выставление счетов абонентам, обработку платежей именуется биллингом[29]. Биллинг, имея основным назначением расчет стоимости услуг связи, объективно позволяет собрать информацию об абонентах и соединениях используемых абонентских устройств, которая дает возможность установить принадлежность абонентского номера, зафиксировать соединения между абонентскими устройствами и ограничить примерное местонахождение абонентского устройства в момент соединения в зоне обслуживания базовой станции[30].

Данная информация может использоваться и в процессе доказывания при расследовании уголовных дел, поскольку современные системы фиксации переговоров позволяют фиксировать в базе данных речевую и служебную информацию о переговорах (дата, время, длительность, входящие и исходящие номера); автоматически определять номер; осуществлять автоматическую архивацию записанной информации[31].

Рассмотрев организационные вопросы работы оператора подвижной радиотелефонной связи, некоторые технические характеристики электросвязи, построение сотовой сети, можно констатировать, что оператор сотовой связи имеет возможность по судебному решению предоставить полный доступ к информации о соединениях между абонентами и (или) абонентскими устройствами. Следственные органы вправе запросить сведения, хранящиеся в базах оператора связи путем использования известных коду IMEI оборудования, номеру SIM-карты или абонентскому номеру пользователя. При производстве

---

[29] Billing (англ. биллинг) есть «тарификация, составление и выписывание счетов за предоставление телекоммуникационных услуг»

[30] Черенков А.В. Использование контроля и записи переговоров в раскрытии и расследовании преступлений: автореф. дис. … канд. юрид. наук. М., 2005. С. 9.

[31] Гаврилин Ю.В., Дубоносов Е.С. Использование контроля и записи телефонных и иных переговоров в раскрытии и расследовании преступлений: учебное пособие. – М., 2003. С. 38.

следственного действия, предусмотренного статьей 186.1 УПК РФ, оператор обязан предоставить следствию запрашиваемые сведения, к которым можно отнести дату, время, продолжительность входящих/исходящих вызовов, передачи SMS, MMS, EMS-сообщения, данные SIM-карты (сведения об абоненте), геолокацию абонентского устройства, идентификационный код IMEI, услуги связи, предоставляемые оператором связи. Таким образом, абонентские устройства с учетом принципов функционирования операторов сотовой связи и сведений об обстоятельствах использования конкретного абонента являются источником получения криминалистически значимой информации.

§ 2. Получение информации о соединениях между абонентами и (или) абонентскими устройствами: понятие и значение следственного действия

Понятие и необходимость правовой регламентации процесса получения информации о соединениях между абонентами и (или) абонентскими устройствами начали формироваться еще до закрепления следственного действия в УПК РФ. Именно с появлением этой процессуальной нормы появились четкие границы того, что можно относить к данному понятию, а что к нему не имеет значения.

Несмотря на то, что следственное действие, предусмотренное статьей 186.1 УПК РФ, с 2010 года нормативно закреплено, до сегодняшнего дня среди ученых и исследователей не сформировалось единой точки зрения относительно его правовой сущности. Некоторые ученые считают, что получение информации о соединениях между абонентами и (или) абонентскими устройствами это даже не следственное действие. Примечательно, что законодатели отдельных стран СНГ называют аналогичное в правовом плане следственное действие иначе: розыскное мероприятие (УПК Республики Молдова); негласное (розыскное) действие – разновидность следственных действий, не подлежащих разглашению (УПК

Украины)[32]. В.В. Кальницкий утверждает, что получение информации о соединениях между абонентами и (или) абонентскими устройствами нельзя относить к следственным действиям, так как оно имеет иную правовую природу[33]. По его мнению, получение информации о соединениях между абонентами и (или) абонентскими устройствами следует рассматривать как квалифицированное (осуществляемое по судебному решению) истребование соответствующей информации у оператора связи. Эта информация не имеет признаков вещественного доказательства и должна приобщаться к делу по правилам работы с иными документами. Б.Т. Безлепкин также не согласен с введением новой нормы в УПК РФ и пишет, что из содержания ст. 186.1 УПК РФ «вытекает следующая теоретическая интерпретация нового процессуального действия. Информация (на языке УПК РФ (ст.74) – «сведения о фактах», а по теории доказательств – «фактические данные»), о которой идет речь, фиксируется компетентным специалистом учреждения связи, которому поручено исполнение судебного решения по конкретному уголовному делу, излагается в общепонятной письменной форме (распечатке), удостоверяется подписью ответственного лица, словом, документируется, а составленный и оформленный документ представляется органу расследования. Таким образом, – заключает Б.Т. Безлепкин, – 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. Подобное процессуальное правоотношение нормально испокон веков широко применимо как в досудебной,

---

[32] Статья 268 кримінального процессуального кодекса Украіни предусматривает установление местонахождения радиоэлектронного средства. Это действие проводится оперативным работником на основании решения следственного судьи и заключается в применении технического оборудования для локализации местонахождения радиоэлектронного средства, в том числе мобильного терминала, систем связи и других радиоизлучающих устройств, активированных в сетях операторов подвижной связи, без раскрытия содержания передаваемых сообщений, если в результате его проведения можно установить обстоятельства, имеющие значение для уголовного дела.

[33] Кальницкий В.В. Вопросы правовой регламентации следственных действий на современном этапе // Законы России: опыт, анализ, практика. 2015. № 2. С. 34.

так и в судебной практике уголовного судопроизводства. Так что диктуемое техническим прогрессом, но лишенное достаточной теоретической основы изобретательство новых суррогатов следственных действий продолжается»[34].

В противовес такой точки зрения выступает В.Ю. Стельмах. По поводу правовой природы получения информации о соединениях между абонентами и (или) абонентскими устройствами, автор утверждает, что необходимо его квалифицировать как следственное, без каких-либо оговорок и с учетом специфических особенностей сосредоточить усилия на совершенствовании процессуальной регламентации и обеспечении гарантий прав граждан при его проведении[35]. Аналогичного мнения придерживается Е.С. Лапин[36].

На наш взгляд, необходимо руководствоваться действующим уголовно-процессуальным законом. Законодатель в п. 24.1 ст. 5 УПК РФ определил, что под получением информации о соединениях между абонентами и (или) абонентскими устройствами понимается получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, а также сведений о номерах и месте расположения приемопередающих и базовых станций. Очевидно, что получение информации о соединениях между абонентами и (или) абонентскими устройствами важное следственное действие, которое выделил законодатель в целях упрощения работы следователя со сведениями, предоставляемыми оператором связи, а также для наиболее эффективного их закрепления в качестве вещественных доказательств. Однако, Е.С. Лапин справедливо отмечает, что наличие сформулированного в законе понятия получения информации о соединениях между абонентами и (или) абонентскими

---

[34] Безлепкин Б.Т. Краткое пособие для следователя и дознавателя / Б.Т. Безлепкин.– М., 2011. – С. 80. См. также: Шейфер С.А. Следственные действия. Основания, процессуальный порядок и доказательственное значение / С.А. Шейфер. – М.: Юрлитинформ, 2004.

[35] Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: монография / В.Ю. Стельмах. – Екатеринбург: Уральский юридический институт МВД России, 2014. С.40.

[36] Лапин Е.С. Тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами: монография. – Юрлитинформ, 2014. С. 37-38.

устройствами не препятствует тому, что ученые-криминалисты продолжают предлагать свои новые определения данному следственному действию. Действительно, указанное в УПК РФ определение рассматриваемого следственного действия, казалось бы, перечисляет все виды информации, которые можно получить, используя возможности ст. 186.1 УПК РФ, но, тем не менее, является достаточно пространным, что создало почву для дискуссий среди исследователей по данному вопросу.

Проанализировав некоторые исторические факты и документы, можно сделать вывод о том, что формирование понятия получения информации о соединениях между абонентами и (или) абонентскими устройствами началось задолго до введения в уголовно-процессуальный закон статьи 186.1, закрепившей данную норму права. Еще в 2003 году, было вынесено Определение Конституционного Суда Российской Федерации от 2 октября 2003 г. № 345-О «Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года «О связи»», в котором как рассматривался вопрос законности и правомерности предоставления оператором сотовой связи правоохранительным органам сведений об абонентских соединениях лица, совершившего мошеннические действия[37].

Основными предпосылками формирования нового процессуального средства получения сведений об абонентах и абонентских устройствах, с одной стороны стали спорные ситуации, возникшие в следственной и судебной практике, а с другой - труды ученых и исследователей, в которых отмечался непрерывный научно-технический прогресс, повсеместное развитие телекоммуникаций, модернизация сотовых сетей, а также мобильных устройств связи, и отставание от современных реалий норм уголовно-процессуального закона. Многие ученые в рамках своих работ обращались к законодателю с

[37] Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 г. «О связи: определение Конституционного Суда РФ от 2 октября 2003 г. № 345-0 // Вестник Конституционного Суда РФ. 2004. № 1. С. 48.

инициативой внесения изменений в УПК РФ, а в частности, предполагали введение новой нормы, которая бы позволила органам следствия максимально эффективно использовать информацию, источниками которой являются технические устройства связи. Так, Соколов Ю.Н. предлагает ввести новое следственное действие именуемое «Электронным наблюдением», в рамках которого необходимо объединить все случаи получения сведений, передаваемых с помощью средств электросвязи, в рамках одного следственного действия[38]. А.Н. Иванов выступал с предложением ввести в УПК РФ статью 186.1 «Контроль детализации абонентов оператора связи». Новая статья содержала следующее: «При наличии достаточных оснований полагать, что имеются достоверные данные о факте использования телефона в период, предшествовавший совершению преступления, в момент совершения преступления, а также в период непосредственно после окончания преступления подозреваемым, обвиняемым и другими лицами, в графиках соединений (детализациях) которых могут содержаться сведения, имеющие значение для уголовного дела, их контроль допускается на основании судебного решения, принимаемого в порядке, установленном статьей 165 УПК РФ. В ходатайстве следователя о получении детализации сигналов электросвязи указываются: уголовное дело, при производстве которого необходимо применение данной меры; основания, по которым производится данное следственное действие; фамилия, имя, отчество абонента и (или) его абонентский номер; конкретный абонентский номер или серийный номер сотового телефона, по которому необходима детализация; период времени, за который необходимо получение детализации; наименование оператора связи, у которого запрашивается предоставление детализации. Период времени, за который предоставляется детализация, не должен превышать календарного года до указанного события. Детализация абонентских соединений предоставляется на бумажном носителе или в электронном виде. О результатах осмотра и анализа графика соединения абонентов следователь с участием понятых составляет

[38] Соколов Ю.Н. Электронное наблюдение в уголовном судопроизводстве и оперативно-розыскной деятельности. Екатеринбург, 2006. С. 120 – 124.

протокол»[39]. Несколько позже В.Ф. Васюков предложил дополнить УПК РФ новой статьей 186.1 «Контроль сведений о пользователях связи и об оказанных им услугах связи» следующего содержания:

1. При наличии достаточных оснований полагать, что у организации связи содержатся сведения, имеющие значение для уголовного дела, их получение допускается на основании судебного решения, принимаемого в порядке, установленном статьей 165 настоящего Кодекса.

2. В ходатайстве следователя указываются: 1) уголовное дело, при производстве которого необходимо применение данной меры; 2) персональные данные и (или) абонентский номер пользователя; 3) идентификационный номер средства связи, если он известен; 4) основания, по которым производится данное следственное действие; 5) срок осуществления контроля; 6) наименование организации, на которую возлагается обязанность по предоставлению сведений.

3. Постановление о производстве контроля сведений о пользователях связи и об оказанных им услугах связи направляется следователем для исполнения в соответствующую организацию.

4. Сведения о входящих и исходящих сигналах соединения в сети конкретных пользователей связи с момента вынесения постановления могут быть истребованы не более чем за 12 месяцев до срока окончания предварительного расследования по данному уголовному делу. Решение об истребовании таких сведений исполняется организацией связи не позднее 3 суток с момента получения постановления о контроле.

5. Проверка сведений о пользователях связи и об оказанных им услугах связи может осуществляться следователем в соответствующей организации с участием специалиста, понятых из числа работников организации, о чем составляется протокол, в котором указывается, кем и в какой срок осуществлялась проверка, какие сведения были при этом проверены и (или) скопированы.

---

[39] Иванов А.Н. Проблемы получения при расследовании преступлений информации у операторов связи // Криминалистика в системе правоприменения: материалы конференции. – Москва. – С. 135.

6. Документы, полученные у организации связи, приобщаются к материалам уголовного дела в порядке, установленном в статье 84 настоящего кодекса на основании постановления следователя»[40].

Именно по этим работам можно отследить важную тенденцию в процессе формирования понятия и оснований получения информации о соединениях между абонентами и (или) абонентскими устройствами. Хотя, с имеющейся в действующем законодательстве процессуальной нормой, можно раскритиковать вышеуказанные предложения. Не останавливаясь на критике, заметим, что все авторы, предпринявшие попытки создания новой нормы уголовно-процессуального закона, указывают на одну вещь – «в процессе истребования сведений об абонентах и абонентских устройствах необходимо обеспечить «тайну связи»». Ограничение конституционного права на тайну телефонных переговоров в данном случае следует рассматривать, в другом плане, нежели чем, например, при производстве контроля и записи переговоров. При получении информации о соединениях между абонентами и (или) абонентскими устройствами содержание самого разговора между абонентами не становится известным, а устанавливается лишь факт телефонных контактов, абонентские номера, с которых велись переговоры. Однако, несмотря на приведенное обстоятельство, и в данном случае речь идет об ограничении конституционного права. Это означает что, для получения информации о соединениях между абонентами и (или) абонентскими устройствами следственным органам необходимо получение судебного решения. Иное означало бы несоблюдение требования ч. 2 ст. 23 Конституции РФ о возможности ограничения права на тайну телефонных переговоров только на основании судебного решения. В подтверждение вышесказанному, приведем пример из обзора судебной практики, утвержденного Президиумом Верховного суда РФ, в котором говорится, что «информацией, составляющей охраняемую Конституцией Российской Федерации

---

[40] Васюков В.Ф. Особенности раскрытия и расследования грабежей и разбоев, совершенных на открытой местности: автореф. дис. … канд. юрид. наук. Орел: Орловский юридический институт МВД России, 2009. С. 11-12.

и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи»[41]. Однако для получения такого решения, как свидетельствует практика, требуется достаточно продолжительное время, что снижает возможность раскрытия преступления по «горячим следам»[42]. В связи с этим, данное определение подверглось критике со стороны ряда ученых и практиков, к мнению которых, безусловно, стоит присмотреться. Так, Батоев и Бычков критикуют данное определение, ссылаясь на потребности практических сотрудников в раскрытии и расследовании преступлений в кратчайшее время[43]. А.Е. Чечетин, например, пишет: «Конституционный Суд исходит из расширительного толкования понятия тайны телефонных переговоров. Такой подход нарушает баланс интересов государства и личности в сторону последнего, что в современной криминальной ситуации в России вряд ли оправданно». Получение информации о входящих и исходящих соединениях не может находиться в поле зрения конституционной защиты права на тайну телефонных и иных переговоров, потому что в этой информации не содержится сама суть переговоров, соответственно тайна телефонных переговоров не нарушается[44]. Это подтверждает судья Чернушинского районного суда Пермской области А. Богдановский, который отметил, что «Конституционный Суд РФ забывает, что электронные соединения не могут быть такой же тайной, как содержание телефонных переговоров. Ведь содержание телефонных переговоров невозможно узнать, пока не прослушаешь или не запишешь их, а электронные соединения

---

[41] Обзор судебной практики, утвержденный Президиумом Верховного Суда Российской Федерации 27 июня 2012 г. // Бюллетень Верховного Суда РФ. – 2012. – № 10. – С. 47.

[42] По данным анкетирования, 78,3% опрошенных отметили проблему, связанную с потерей времени при получении судебного решения на производство следственного действия, предусмотренного статьей 186.1 УПК РФ, что повлияло на раскрытие преступления «по горячим следам».

[43] Батоев В.Б., Бычков В.В. Раскрытие и расследование хищений средств мобильной связи: монография / В.Б. Батоев, В.В. Бычков. – Москва: Юрлитинформ, 2013. С. 49.

[44] Чечетин А.Е. Ограничение тайны связи // Законность. 2005. № 7. С. 40.

автоматически фиксируются на магнитных носителях и могут быть в любой момент распечатаны и выданы тому, кому это положено»[45]. Такой же позиции придерживаются Т.В. Винокурова и Ю.А. Астафьев[46], В.М. Быков и Т.П. Сазонова[47], считающие, что сведения о соединениях к тайне телефонных переговоров не относятся.

Выйти из сложившейся ситуации возможно при детальном регламентировании на законодательном уровне порядка взаимодействия операторов сотовой связи с органами, осуществляющими предварительное расследование и судами. Под «детальностью» мы предполагаем разработку самой процедуры предоставления информации о пользователях услуг связи и об оказанных им услугах связи, правах и обязанностях всех сторон взаимодействия. В связи с этим, следует разделить позицию А.В. Шебалина, предлагающего инициировать подготовку Пленума Верховного Суда РФ, посвященного вопросам преступлений в сфере компьютерной информации, где, в том числе разрешить вопрос порядка получения необходимой информации от операторов сотовой связи, в рамках осуществления ОРД, предварительного и судебного следствия[48].

Проанализировав научные исследования и основываясь на действующем законодательстве, сделаем вывод о том, что под тайной связи понимаются «юридически охраняемые сведения, передаваемые по сетям электросвязи и сетям почтовой связи от одного пользователя к другому опосредованно через исполнителя любым способом передачи информации, входящие в сферу деятельности оператора связи». На наш взгляд, к тайне связи относятся данные биллинга: время и продолжительность разговора, номера вызывающего и вызываемого абонентов и местоположение абонента. Судебная и следственная

---

[45] Богдановский А. Может ли ошибаться Конституционный Суд? // Законность. 2006. № 8. С. 34.

[46] Астафьев Ю.В., Винокурова Т.В. Проблема получения сведений о телефонных соединениях при производстве ОРД. – [Электронный ресурс]. URL: http://www.consultant.ru.

[47] Быков В.М., Сазонова Т.П. Истребование сведений о телефонных контактах как процессуальное действие по собиранию доказательств // Уголовный процесс. 2008. №9. С. 54 –56.

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

практика традиционно включает в содержание тайны связи любые сведения о соединениях средств связи:

а) о содержании переговоров;

б) только о фактах взаимодействий абонентских устройств (двух или нескольких при использовании услуги конференцсвязи);

в) данные о сигналах вызова, если при этом становится известным номер вызываемого устройства.

Следует, что тайна связи включает в себя тайну телефонных переговоров и по объему тайна связи больше, чем тайна телефонных переговоров, а биллинг, в свою очередь дает больше информации чем, просто запись переговоров, а значит, определенно требует судебной защиты.

Итак, получение информации о соединениях между абонентами и (или) абонентскими устройствами, по своей правовой сущности и направленности должно решать вопрос о получении новых доказательств путем ограничения конституционного права российских граждан на тайну связи. Подчеркнем, что речь идет о гражданах, которые в силу различных обстоятельств вовлечены в уголовное судопроизводство и имеют различный уголовно-процессуальный статус. По этой причине решение о проведении рассматриваемого уголовно-процессуального средства должно носить взвешенный, обоснованный и законный характер, с тем, чтобы были исключены случаи необоснованного ограничения конституционного права граждан. Судебное решение для получения информации о соединениях между абонентами и (или) абонентскими устройствами является гарантией защиты конституционного права гражданина на тайну телефонных переговоров и иных сообщений.

С момента вхождения сотовой связи в повседневную жизнь граждан, у представителей правоохранительных органов появилось осознание того, что используя информацию об абонентах, их соединениях и абонентских устройствах, можно повысить результативность расследования по уголовным делам любой категории. Еще до введения указанной нормы в УПК РФ, В.А. Козинкин пишет, что «средства сотовой связи становятся все более доступными, а их технические

возможности постоянно совершенствуются. Во многом благодаря указанным качествам средства мобильной связи сейчас – самый распространенный инструмент человеческого общения, используемый и преступными формированиями при подготовке и совершении преступлений, а также для сокрытия следов противоправной деятельности и противодействия расследованию. Как показывает практика, средства связи задействуются при подготовке и совершении заказных убийств, похищения людей, вымогательств, взяточничества, преступлений, связанных с незаконным оборотом наркотических средств, хищений и других общественно опасных деяний. В этой связи 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 криминалистически значимой информации»[49].

Автор акцентировал внимание на том, что сотовые системы подвижной связи, безусловно, отличаются от стационарной телефонной связи. В связи с этим для получения информации, передаваемой по их сетям, необходима разработка не только специальных приёмов её фиксации и изъятия, но и соответствующей правовой базы. Речь идет, прежде всего, об отсутствии на тот момент законодательной регламентации деятельности органов расследования по получению сведений о соединениях абонента сотовой связи в тех случаях, когда это необходимо в целях раскрытия преступления.

В 2006 году была опубликована статья А. Иванова и О. Корниенко, где авторы рассматривали вопросы использования в доказывании информации, полученной от оператора связи. Указанные исследователи отмечают, что освоены новые полосы радиочастот и уже прошел переход на создание сотовых систем подвижной радиосвязи общего пользования, что способствовало увеличению емкости мобильных сетей и количества абонентов, получивших услуги автоматизированной местной и междугородной связи. Кроме того, новые

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

технологии позволили расширить возможности пользователей сотовой связи до международного уровня, т.е. использовать связь и при пересечении границ других государств. Однако, как отмечают авторы «данное средство связи используется не только в рамках закона, но при совершении самых различных преступлений»[50]. Кроме того, они говорят о появлении новой на тот момент категории преступлений – преступлений в сфере мобильных телекоммуникаций и приходят к выводу о том, что если сотовый телефон активно используется в процессе совершения преступления, то сведения по данному факту могут послужить ценной в криминалистическом плане информацией для правоохранительных органов.

Е.П. Ищенко в 2008 г. отметил: «Наиболее криминалистически значимой представляется … биллинговая информация … которая содержит сведения о количестве и длительности звонков, осуществленных в местной сети и с использованием роуминга (междугородних) … данные о входящих и исходящих звонках с данного аппарата… Регистрация и долговременное (обычно не менее 3 лет) хранение основных параметров всех телефонных соединений, наличие жесткой взаимосвязи абонента и базовой станции, а также технические возможности современных компьютерных средств и систем управления базами данных позволяют весьма оперативно обрабатывать колоссальные объемы биллинговой информации и получать сведения, облегчающие расследование преступлений»[51].

Действительно необходимость появления новой статьи, которая позволила бы в установленном порядке получать информацию о входящих и исходящих вызовах, SMS и MMS сообщения, о регистрационных данных абонента и абонентского устройства, обусловлена не только повсеместным распространением средств сотовой связи, но и отсутствием единого процессуального порядка

---

[50] Иванов А. Использование в доказывании информации, полученной у операторов связи / А. Иванов, О. Корниенко // Уголовное право. – 2006. – № 1. – С. 111.

[51] Ищенко Е.П. Получение и использование новых видов доказательств – актуальная задача российской криминалистики // Криминалистика в системе правоприменения. Материалы конференции, 27–28 октября 2008 г., Москва, МГУ им. М.В. Ломоносова. М., 2008. С. 143.

истребования и закрепления вышеуказанных сведений. Напомним, что до введения рассматриваемой нормы Уголовно-процессуального кодекса РФ на практике и в научной теории не существовало единого порядка получения информации об абонентах и абонентских устройствах.

11 июня 2010 года Государственной Думой Федерального Собрания РФ[52], был рассмотрен законопроект Федерального закона № 143-ФЗ «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации», которым вводилось в уголовное судопроизводство новое следственное действие под названием «Получение информации о соединениях между абонентами и (или) абонентскими устройствами».

23 июня 2010 года вышеуказанный Федеральный закон был одобрен Советом Федерации Федерального Собрания РФ[53] и 1 июля этого же года подписан Президентом РФ[54]. Законопроект был внесен в Государственную Думу Федерального Собрания РФ 22 января 2008 года членом Совета Федерации Федерального Собрания РФ Е.Н. Трофимовым[55].

Возможность получения информации о входящих и об исходящих сигналах соединения телефонов при расследовании любых категорий уголовных дел при непременном наличии судебного решения, вынесенного по ходатайству следователя (дознавателя) не была предусмотрена ст. 186 УПК РФ, регламентирующей контроль телефонных и иных переговоров. В связи с этим, Е.Н. Трофимов предложил урегулировать вопрос получения данной информации путем внесения в УПК РФ изменений. Нововведения в УПК РФ определенно

---

[52] О Федеральном законе «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» (проект № 7176-5): Постановление Государственной Думы Федерального Собрания РФ пятого созыва от 11 июня 2010 г. № 3766-5 ГД // Собрание законодательства РФ. 2010. № 25. Ст. 3081.

[53] О Федеральном законе «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации»: Постановление Совета Федерации Федерального Собрания РФ от 23 июня 2010 г. № 258-СФ // Собрание законодательства РФ. 2010. № 26. Ст. 3282.

[54] Собрание законодательства РФ. 2010. № 27. Ст. 3427.

[55] О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации о получении информации о входящих и исходящих сигналах соединений телефонов при расследовании уголовных дел на основании судебного решения: паспорт проекта Федерального закона № 7176-5. – [Электронный ресурс]. – режим доступа: http://www.lawmix.ru/lawprojects/234443.

упорядочили процесс получения и использования информации о соединениях между абонентами и (или) абонентскими устройствами при расследовании по уголовным делам. Однако среди исследователей возникли разногласия относительно понятия нового следственно действия и оснований его проведения.

Рассмотрим несколько понятий данного следственного действия, предложенных исследователями. В.Ю. Стельмах называет получение информации о соединениях между абонентами и (или) абонентскими устройствами «самостоятельным следственным действием, которое производится по судебному решению и заключается в получении от оператора связи на материальном носителе сведений о фактах соединений между абонентами и (или) абонентскими устройствами, осмотре следователем данного носителя и сведений, и решении вопроса о признании носителя с представленными сведениями вещественным доказательством и приобщении его к уголовному делу». Достаточно емкое определение, так как позволяет индивидуализировать и в полной мере охарактеризовать рассматриваемое следственное действие. Однако следует заметить, что автор в своем определении упускает цель названного следственного действия, хотя она присутствует в ст.186.1 УПК РФ.

Е.В. Ионова в одной из своих работ отмечает: «Получение информации о соединениях между абонентами и (или) абонентскими устройствами – это длящееся следственное действие, представляющее собой поэтапный сбор и изучение (исследование) сведений о контактах абонентов и (или) абонентских устройств»[56]. С данным определением также нельзя согласиться в полном объеме, так как рассматриваемое следственное действие не всегда длящееся, к примеру в случаях, когда интересующая информация носит ретроспективный характер и относится к прошедшим событиям. Оно будет таковым, если получаемая информация носит перспективный характер и имеет значения для будущих событий. Следует согласиться с замечанием Е.С. Лапина по данному

[56] Ионова Е.В. Понятие, значение и тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ) // Вестник криминалистики. 2011. Вып. 1 (37). С. 35.

определению, который отмечает, что необходимо говорить не о поэтапном сборе информации, а об этапах его производства, где должны четко выделяться подготовка, рабочий этап с технической составляющей и заключительный этап, тем самым делая уклон на организационно-тактические аспекты следственного действия[57]. Следует заметить, что Е.С. Лапин один из первых ученых, кто стал изучать данное следственное действие и тактику его проведения, и кроме конструктивной критики он также предлагает свое определение: «… следственное действие, состоящее из ряда взаимосвязанных процессуальных действий, заключающихся в получении на основании судебного решения от операторов связи определенных результатов (данных) АСР (биллинга) и приобщения данной информации в полном объеме к материалам уголовного дела в качестве вещественного доказательства на основании осмотра и соответствующего постановления следователя, а также сохранения ее в опечатанном виде при деле»[58]. В данном определении упомянута аббревиатура «АСР» - Автоматизированные системы расчетов. Дело в том, что именно этот термин используется в России вместо более привычного нам иностранного «Billing» (Биллинг), что означает «тарификация, составление и выписывание счетов за предоставление телекоммуникационных услуг»[59]. Несмотря на определение, фактически под биллингом понимается целый технический процесс подготовки и выпуска счетов для абонента.

О.И. Пигорев предлагает свое определение рассматриваемого следственного действия: «Получение информации о номерах телефонов, времени, дате и продолжительности соединения абонентов, а также о географическом положении и учетных записях абонентов»[60]. Очевидно, что предложенная формулировка, в

---

[57] Лапин Е.С. Тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами: монография. – Юрлитинформ, 2014. С. 40.

[58] Лапин Е.С. Тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами: монография. – Юрлитинформ, 2014. С. 46.

[59] Невдяев Л.М. Телекоммуникационные технологии. Англо-русский толковый словарь-справочник / под ред. Ю.М. Горностаева. Серия изданий «Связь и бизнес». М., 2002.С. 42.

[60] Пигорев О. И. Развитие института следственных действий в российском уголовно-процессуальном праве: автореф. дис. … канд. юрид. наук. М., 2010. С. 8.

которой в качестве средства связи указаны только телефоны, сузит область применения следственного действия даже по сравнению с теми, что установлены в настоящий момент. Кроме того, считаем, что не рационально умышленно умалять потенциал статьи 186.1 УПК РФ.

Интересное определение мы находим в работе Н.А. Архиповой. Под данным следственным действием автор понимает «комплекс взаимосвязанных действий следователя по получению судебного решения для истребования от осуществляющей услуги связи организации информации на любом материальном носителе о соединениях абонентов и поручения ей отслеживания поступающей искомой информации в базу данных мобильной связи, а также осмотру и анализу документов, содержащих указанную информацию, приобщению их к материалам дела в целях установления всех обстоятельств, имеющих значение для раскрытия и расследования преступлений»[61]. В общем, данное определение достойно особого внимания, однако, автор также предлагает новую редакцию п. 24.1 ст. 5 УПК РФ, где конкретизирует сведения, которые можно получить с помощью следственного действия, предусмотренного ст. 186.1 УПК РФ. Новая редакция выглядит следующим образом: «Получение информации о соединениях между абонентами и (или) абонентскими устройствами – это получение сведений о дате, времени, продолжительности соединений между абонентами и (или) абонентскими устройствами (пользовательским оборудованием), номерах абонентов, других данных, позволяющих идентифицировать абонентов, сведений о номерах и месте расположения приемопередающих базовых станций, а также содержание переданной текстовой, графической или иной электронной информации, связанной с абонентскими соединениями»[62]. На наш взгляд, расширять возможности рассматриваемого следственного действия, добавляя к ним передачу графической и текстовой информации не совсем верно. Действительно, в сформулированном законом понятии есть упоминание «другие

---

[61] Архипова Н.А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи: автореф. дис. … канд. юрид. наук. СПб.: Санкт-Петербургский университет МВД России, 2011. С. 11.

[62] Там же. С. 9-10.

данные». И среди исследователей на этот счет и вправду не сложилось единого подхода. Основным предметом разногласий как раз является вопрос, можно ли относить к другим данным информацию, составляющую содержание SMS, EMS и MMS? Н.А. Архипова в подтверждение целесообразности предложенной ей редакции п. 24.1 ст. 5 УПК РФ поясняет, что текстовые сообщения представляют собой текстовой фрагмент, состоящий из букв, цифр и символов, набранных в определенной последовательности абонентом при помощи клавиатуры мобильного телефона. При отправке сообщения к его содержанию добавляются сведения о соединении. Данные сведения сохраняются в базе данных операторов связи в виде компьютерной информации, которая может быть скопирована на любой материальный носитель. В связи с этим, форма передачи, отражения и хранения текстовых сообщений и их содержания в базах данных операторов связи позволяет автору отнести их к категории информации о соединениях между абонентами и (или) абонентскими устройствами[63]. Следовательно, сведения о текстовых сообщениях и их содержание могут быть получены от операторов связи при проведении следственного действия, предусмотренного ст. 186.1 УПК РФ[64].

Действительно, письменный текст и изображения хранятся в базах сотового оператора в виде компьютерной информации, и есть техническая возможность получить данные сведения. Кроме того, данная информация в соответствии с п. 35 ст. 2 Федерального закона «О связи», относится к электросвязи, а под электросвязью понимаются любые излучения, передача или прием знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам[65].

Как может показаться, природа такой информации, позволяет отнести ее к категории информации о соединениях между абонентами и (или) абонентскими

---

[63] Архипова Н.А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи: автореф. дис. … канд. юрид. наук. СПб.: Санкт-Петербургский университет МВД России, 2011. С. 13.

[64] Там же. С. 21.

[65] О связи: федеральный закон от 07.07.2003 № 126-ФЗ. (действующая редакция). – [Электронный ресурс]. − URL: http:// www.consultant.ru.

устройствами. Но получение содержания SMS сообщений, не может быть осуществлено посредством проведения следственного действия, предусмотренного ст. 186.1 УПК РФ, так как смысл данного следственного действия подразумевает собой получение только сведений о дате, времени, абонентах, осуществляющих переписку, а также об абонентских базовых станциях связи и их местоположении и не может отражать содержание текстового сообщения. Получить содержание сообщения можно путем проведения такого оперативно-розыскного мероприятия, как получение компьютерной информации, в соответствии с Федеральным законом «Об оперативно-розыскной деятельности» либо путем производства выемки, регламентированной ст. 183 УПК РФ.

С.А. Вазюлин, В.Ф. Васюков, считая, что получение сведений об информационном (графическом, знаковом) содержании электронных сообщений в рамках следственного действия, регламентированного ст. 186.1 УПК РФ, является неправомерным, подтверждают нашу точку зрения[66]. Хотя, идея законодательно закрепить «получение текстовой, графической иной электронной информации, связанной с абонентскими соединениями», нами поддерживается. Тем более, что такой инструмент будет достаточно актуальным в современных условиях роста киберпреступности, телефонных мошенничеств и нарастающей террористической угрозе со стороны радикальных объединений (ИГИЛ и т.п.).

Анализируя точки зрения ученых и исследователей по поводу понятия и сущностной природы данного следственного действия, мы приходим к выводу, что, несмотря на специфичный, сложный и комплексный характер, рассматриваемое следственное действие является мощным процессуальным инструментом в руках следователя по получению доказательственной и криминалистических значимой информации. Справедливо заметить, что сложный и комплексный характер носят и другие следственные действия, например, наложение ареста на почтово-телеграфные отправления, их осмотр и выемка (ст. 185 УПК РФ), контроль и запись переговоров (ст. 186 УПК РФ).

---

[66] Вазюлин С. А., Васюков В. Ф. Получение информации о соединениях между абонентами: специфика процедуры // Уголовный процесс. 2014. № 1. С. 10 – 20.

Специфика получения информации о соединениях между абонентами и (или) абонентскими устройствами заключается в цели и задачах следственного действия. Кроме характерных для всех следственных действий целей, таких как получение сведений о неустановленных обстоятельствах, а также данных подтверждающих либо опровергающих уже известные факты совершенного преступного деяния, в рамках рассматриваемого следственного действия реализуется специальная цель, которая заключается в получение криминалистически значимой информации, отражающей совокупность данных об использовании конкретного абонентского устройства и (или) абонентского номера проверяемым лицом в определенный период времени.

Достижение указанных целей определяет необходимость постановки и решения следующих **задач**:

1. Установление оператора сотовой связи, принадлежность к которому имеет проверяемый абонентский номер;

2. Установление принадлежности абонентского номера и (или) абонентского устройства конкретному лицу;

3. Определение периода времени, за который необходимо получить сведения о соединениях между абонентами и (или) абонентскими устройствами;

4. Подготовка необходимых процессуальных документов, выступающих юридическим основанием для получения информации о соединениях между абонентами и (или) абонентскими устройствами;

5. Обращение к оператору сотовой связи в целях технического исполнения рабочего этапа следственного действия;

6. Анализ полученных результатов, определение объема данных, представляющих доказательственное значение и сведений, носящих информационный характер.

Исходя из вышеизложенного, определим, что **получение информации о соединениях между абонентами и (или) абонентскими устройствами – это комплексное следственное действие, состоящее в получении от оператора сотовой связи по судебному решению интересующих следствие сведений об**

абонентах, абонентских устройствах и их соединениях. Применение нами термина «комплексное следственное действие», в авторском определении обусловлено структурными составляющими тактики производства получения информации соединениях между абонентами и (или) абонентскими устройствами. Речь об этом пойдет во второй главе диссертационного исследования.

Представляется целесообразным привести классификацию информации, получаемой в ходе производства данного следственного действия, по ее содержанию:

а) информация об абоненте (данные о лице, на чье имя зарегистрирована SIM-карта);

б) информация об абонентском устройстве (данные о конкретном устройстве, IMEI-код);

в) сведения о состоявшихся соединениях между абонентами (дата, время, продолжительность соединения;

г) информация о местонахождении абонентских устройств или конкретных лиц.

В зависимости от использования указанных сведений в процессе расследования по уголовному делу информация может приобрести статус доказательственной или использоваться в качестве ориентирующей (криминалистически значимой). Такую информацию, следователь может относить к категории сведений, касающихся:

а) отдельных элементов предмета доказывания преступления (дата, время, продолжительность переговоров, абонентский номер подозреваемого, предмет преступления).

б) иных данных (количество соучастников, характер группы лиц, ее состав, связь подозреваемых, субъекты противодействия расследованию).

Для получения информации о соединениях между абонентами необходимы фактические и юридические основания. Из анализа ч. 1 ст. 186.1 УПК РФ следует, что под фактическими основаниями рассматриваемого следственного действия понимается некая совокупность сведений, позволяющая определить, имеет ли

информация о соединениях между абонентами (и или) абонентскими устройствами значение для уголовного дела. Другими словами, будет достаточно результатов оперативно-розыскной деятельности или других доказательств, исходя из содержания которых, будет ясно, что интересующая информация, полученная от оператора связи, будет иметь определенное значение.

Основным представляется наличие того, что следственные органы имеют в своем распоряжении достоверную информацию, свидетельствующую о значимости для уголовного сведений об абонентах и абонентских соединениях. При этом назначать получение информации о соединениях между абонентами и (или) абонентскими устройствами недопустимо без зафиксированных в материалах уголовного дела сведений. Содержание информации, которые выступают в качестве оснований для производства следственного действия, предусмотренного статьей 186.1 УПК РФ, может быть различным.

Во-первых, такая информация может отражать прямые указания на то, что лицо пользовалось каким-либо средством связи в целях совершения действий, входящих в объективную сторону состава преступления или направленных на его совершение (к примеру, исходя из показания потерпевшего, свидетеля или соучастника следует, что подозреваемый созванивался с ними посредством сотовой связи).

Во-вторых, в их качестве могут выступать данные только о наличии у того или иного лица абонентского устройства (причем, оно само может и не быть изъято), а вывод об его использовании в процессе совершения преступления вправе сделать сам следователь на основании изучения и анализа материалов конкретного уголовного дела и общих положений методики расследования преступлений. Необходимо учитывать, что «определенная часть познавательной деятельности проходит скрытно, в сознании следователя… путем мыслительных операций. Эта сторона познания регулируется не нормами права, а закономерностями разумного человеческого мышления»[67].

---

[67] Давлетов А.А. Основы уголовно-процессуального познания. 2-е изд., испр. и доп. Екатеринбург, 1997. С. 14.

В-третьих, ситуации, когда следователь может лишь предположить, что лицо совершившее преступление использовало сотовый телефон (например, в целях формирования круга лиц, причастных к совершению преступления). Допустимо принятие решение о производстве рассматриваемого следственного действия, когда характер преступного посягательства предполагает коммуникацию лиц, так или иначе прикосновенных к нему (обвиняемых, потерпевших, свидетелей), с помощью средств электросвязи.

В-четвертых, когда не известна личность преступника, в целях обеспечения поискового характера.

Итак, фактические основания сводятся к тому, что производство указанного следственного действия даст определенный результат или в материалах уголовного дела имеются данные о том, что в интересах следствия необходимо ограничить конституционные права человека.

Кроме фактических оснований, для производства рассматриваемого следственного действия необходимы формальные основания (юридические). К ним можно отнести:

1) Получение информации о соединениях между абонентами и (или) абонентскими устройствами может быть проведено только после возбуждения уголовного дела.

2) Рассматриваемое следственное действие может производиться только в течение срока предварительного следствия по конкретному уголовному делу. Это значит:

а) до объявления первому из обвиняемых об окончании производства следственных действий в порядке ст. 215 УПК РФ;

б) до вынесения постановления о прекращении уголовного дела;

в) до вынесения постановления о приостановлении предварительного следствия.

К указанному времени электронный носитель информации с данными биллинга должен быть получен от оператора связи, осмотрен и в случае необходимости приобщен к уголовному делу в качестве вещественного

доказательства. Запрещается проведение данного следственного действия после уведомления обвиняемых и потерпевших об окончании следственных действий. В частности, недопустима ситуация, когда технический этап следственного действия не завершен к моменту принятия названных решений, он продолжается во время ознакомления потерпевших и обвиняемых с материалами уголовного дела, а сама информация приобщается к делу уже в ходе такого ознакомления.

3) Проводить данное следственное действие могут лица, в производстве которых находится уголовное дело. В случае расследования дела следственной группой возбудить перед судом ходатайство о разрешении следственного действия может только ее руководитель (п. 7 ч. 4 ст. 163 УПК РФ). Возникает вопрос о возможности поручения производства названного следственного действия другому следственному органу в порядке ч. 1 ст. 152 УПК РФ, то есть не по месту производства предварительного расследования, когда офис оператора связи, в котором сосредоточена искомая информация, находится в другом населенном пункте. Такую возможность следователю указанная норма предоставляет. Но вполне очевидно, что поручать другому следователю нужно не весь круг процессуальных действий, детализации соединений абонента (сигналов) у оператора электросвязи. Иными словами, действия следователя–исполнителя поручения ограничиваются направлением постановления судьи о разрешении проведения следственного действия оператору связи и получения от него информации о соединениях абонента и (или) абонентского устройства. Отсюда, к указанному поручению должно прилагаться решение судьи на производство следственного действия, полученное следователем, дающим это поручение. Такой порядок является важной гарантией обеспечения прав и законных интересов человека.

В заключении, отметим, насколько ценным является получение информации о соединениях между абонентами и (или) абонентскими устройствами для правоохранительных органов. О его значении можно судить по практики применения, и том насколько часто к его производству прибегают при расследовании уголовных дел. Согласно статистическим данным, в первом

полугодии 2015 года в суды Свердловской области поступило 2 502 ходатайства в порядке ст. 186.1 УПК РФ о получении информации о соединениях между абонентами и (или) абонентскими устройствами, из которых 2 495 рассмотрены по существу, по 7 обращениям приняты иные решения (3 возвращены для устранения недостатков, по 4 производство прекращено). Из рассмотренных по существу 2 288 ходатайств удовлетворено (91,7 %), в удовлетворении 207 отказано[68]. К числу основных причин отказа к производству получении информации о соединениях между абонентами и (или) абонентскими устройствами относятся непредставление органами предварительного расследования достаточных данных, подтверждающих наличие оснований для производства указанного следственного действия, неоправданные требования о производстве указанного следственного действия в отношении неопределенного круга лиц.

§ 3. Процессуальные особенности и отличие получения информации о соединениях между абонентами и (или) абонентскими устройствами от иных следственных действий и оперативно-розыскных мероприятий

Получение информации о соединениях между абонентами и (или) абонентскими устройствами закреплено в действующем УПК РФ с 1 июля 2010 года, а необходимость использования сведений об абонентской активности появилась задолго до этой даты. При расследовании преступлений правоохранительные органы использовали информацию об абонентах и их устройствах, получая ее вполне законными способами. Практика в этом отношении развивалась в разных направлениях и не отличалась единообразием.

В одних случаях детализацию вызовов предоставлял сам участник производства по уголовному делу, но это было возможно только в бесконфликтной

---

[68] Справка по результатам обобщения практики судебных обращений по применению положений ст.ст. 186, 186.1 Уголовно-процессуального кодекса Российской Федерации. – [Электронный ресурс]. – www.ekboblsud.ru/doc/sudpr/pr_obzor_ug.doc.

ситуации. В других случаях информация о соединениях между абонентами и (или) абонентскими устройствами предоставлялась в рамках производства других следственных действий или оперативно-розыскных мероприятий. Часто данная информация получалась в форме выемки. Некоторые процессуалисты полагают, что такая выемка должна производиться на основании судебного решения, поскольку получаемая информация составляет охраняемую законом тайну[69]. Другие считают, что указанные сведения тайны не образуют и их выемка судебного разрешения не требует[70]. Иногда указанное действие проводилось в рамках контроля и записи телефонных и иных переговоров[71]. За получение этих сведений в рамках данного следственного действия высказывались и другие ученые[72]. В ряде случаев интересующая информация получалась путем отправления письменных запросов в организацию оператора связи.

Имея в настоящий момент закрепленное на законодательном уровне процессуальное средство получения биллинговой информации, становится очевидным, что выемка, контроль и запись переговоров или отправление письменных запросов следователя в полной мере не отражали существа истребования сведений о соединениях абонентов и использовались для этого лишь за неимением полностью адекватной процессуальной формы.

Оператор сотовой связи располагал интересующей следствие информацией и, имея технические возможности оборудования, мог ее предоставить. В свою очередь, правоохранители не располагали необходимым правовым инструментарием для получения и использования доказательственной информации. Получение информации о соединениях между абонентами в рамках

---

[69] Варпаховская Е., Вяткин А. Расследование хищений мобильных телефонов // Законность. 2005. № 3. С. 23.

[70] Винокурова Т. В., Астафьев Ю. В. Проблема получения сведений о телефонных соединениях при производстве ОРД // Российская юстиция. 2008. № 1. С. 55.

[71] Ширев Д. А. Контроль и запись телефонных и иных переговоров и их доказательственное значение в уголовном судопроизводстве России: дис. … канд. юрид. наук. М., 2009. С. 3.

[72] Васюков В. Ф. Сведения об абонентах связи как криминалистически значимая информация при раскрытии и расследовании грабежей и разбоев, совершаемых на открытой местности // Правовые вопросы связи. 2008. № 2. С. 15; Научное обеспечение деятельности органов внутренних дел Российской Федерации / под. ред. В.М. Юрина. Саратов, 2007. С. 185.

других следственных действий приводило иногда к достаточно сложным ситуациям, когда следователь возбуждал ходатайство о производстве одного следственного действия (например, контроля и записи телефонных и иных переговоров), а судьей по этому же ходатайству давалось разрешение на проведение другого (выемки). Так, президиум Белгородского областного суда, отменяя решение суда районного звена, указал, что судьей было отказано в даче разрешения на производство контроля и записи телефонных и иных переговоров, в то время как следователем возбуждалось ходатайство о выемке сведений о соединениях между абонентами. Таким образом, ходатайство следователя, по сути, осталось нерассмотренным[73]. Сходные ситуации имели место и по другим уголовным делам[74].

Получение сведений о соединениях между абонентами по запросу следователя было еще менее правильным, поскольку такая информация представляет собой сведения о телефонных переговорах, которые в соответствии с Конституцией Российской Федерации могут быть получены только по судебному решению. На явный отход от этого правила правоприменительная практика длительное время просто закрывала глаза. Вместе с тем в отдельных случаях информация о соединениях между абонентами, полученная от оператора связи, без судебного решения, впоследствии расценивалась судом как недопустимое доказательство[75].

С появлением в УПК РФ статьи 186.1 возникли проблемы, касающиеся нарушения конституционных прав, возникающие при предоставлении информации о соединениях между абонентами и (или) абонентскими устройствами без уведомления на то субъекта, данные о чьих соединениях запрашивались. Так, Новосельцев А.В. обратился с жалобой в Конституционный

---

[73] Дело № 22-3246. Надзорное постановление президиума Белгородского областного суда от 15 сентября 2011 г. // Архив Белгородского областного суда. 2011 г.

[74] Дело № 22-11939. Кассационное определение судебной коллегии по уголовным делам Московского городского суда от 13 сентября 2010 г. // Архив Московского городского суда. 2010 г.

[75] Дело 22к-1817/11. Кассационное определение судебной коллегии по уголовным делам Кемеровского областного суда от 28 апреля 2011 г. // Архив Кемеровского областного суда. 2011 г.

суд РФ, так как посчитал нарушением тот факт, что по возбужденному в отношении него уголовному делу суд, неоднократно удовлетворял ходатайства о получении сведений об абонентах и их соединениях, при этом заявитель не уведомлялся о проведении таких судебных заседаний, а судебные решения до него не доводились[76]. Разрешить данную проблему позволило Определение Конституционного суда РФ, в котором даются разъяснения о том, что предусмотренная статьями 165, 186 и 186.1 УПК РФ процедура судебного рассмотрения ходатайства следователя с согласия руководителя следственного органа, связана с решением промежуточных для уголовного процесса задач, а рассмотрение судом вопросов о проведении в стадии предварительного расследования следственных действий, ограничивающих конституционные права и свободы граждан, еще не является судебным разбирательством по существу уголовного дела, в связи с чем, требования открытости, гласности и состязательности сторон в этом производстве могут быть реализованы не в полной мере[77]. На наш взгляд, позиция суда справедлива и обоснована, так как эффективность производства следственных и процессуальных действий напрямую зависит от их конфиденциального характера, а при уведомлении о предстоящем их проведении заинтересованных лиц они могут утратить всякий смысл.

Примечательно, что изучив справку по результатам обобщения практики судебных обращений по применению положений ст.ст. 186, 186.1 УПК РФ судов Свердловской области, мы приходим к выводу, что даже после закрепления получения информации о соединениях между абонентами и (или) абонентскими устройствами как следственного действия судами допускались ошибки, когда в

---

[76] Об отказе в принятии к рассмотрению жалобы гражданина Новосельцева Александра Викторовича на нарушение его конституционных прав статьями 4, 74, 88, 165, 186 и 406 уголовно-процессуального кодекса российской федерации: Определение Конституционного суда РФ от 16 декабря 2010 г. № 1712-О-О [Электронный ресурс]. – URL: https://rospravosudie.com. (дата обращения 05.03.2018 г.).

[77] Об отказе в принятии к рассмотрению жалобы гражданина Власова Валерия Александровича на нарушение его конституционных прав положениями статей 115 и 165 Уголовно-процессуального кодекса Российской Федерации: Определение Конституционного Суда Российской Федерации от 25 марта 2004 года № 124-О [Электронный ресурс]. – URL: https://rospravosudie.com. (дата обращения 05.03.2018 г.).

постановлениях судов объединены разные следственные действия, такие, как выемка, контроль и запись переговоров, получение информации о соединениях между абонентами и абонентскими устройствами[78].

Выделение в системе в качестве самостоятельного следственного действия получения информации о соединениях между абонентами и (или) абонентскими устройствами было необходимостью, которая сформировалась под давлением не только ученых и исследователей, но и практиков. Автономизация рассматриваемого следственного действия позволила закрепиться процедуре получения информации о соединениях между абонентами в качестве законодательно урегулированного правового инструмента, соответствующему характеру проводимых действий. Кроме того, решилась проблема законности вторжения в область гарантированных конституционных прав граждан, поскольку указанное действие допускается только по судебному решению. Однако, несмотря на самостоятельность и обособленность в системе следственных действий, получение информации о соединениях между абонентами и (или) абонентскими устройствами, не перестает сочетать в себе некоторые признаки других следственных действий, а также оперативно-розыскных мероприятий. Прежде всего, прослеживается схожесть с контролем и записью переговоров, выемкой, прослушиванием телефонных переговоров, снятием информации с технических каналов связи и получением компьютерной информации. Вместе с тем, рассматриваемое следственное действие обладает индивидуальными признаками, отличающими его от схожих по форме и содержанию перечисленных следственных действий и оперативно-розыскных мероприятий.

Итак, получение информации о соединениях между абонентами и (или) абонентскими устройствами имеет следующие принципиальные отличия от контроля и записи переговоров.

---

[78] Справка по результатам обобщения практики судебных обращений по применению положений ст.ст. 186, 186.1 Уголовно-процессуального кодекса Российской Федерации. – [Электронный ресурс]. – www.ekboblsud.ru/doc/sudpr/pr_obzor_ug.doc.

1. Предмет контроля и записи переговоров представляется намного шире и включает в себя непосредственно содержание самих переговоров. Что касается предмета получения информации о соединениях между абонентами и (или) абонентскими устройствами, то в него входят только сведения об абонентах и их соединениях, в том числе и о передаче телематических электронных сообщений, которые были зафиксированы оборудованием оператора сотовой компании и хранятся у последнего в базах данных. По сути, это электронная информация, т.е. электрические импульсы, сохраненные оборудованием оператора связи с возможностью их хранения и, в случае необходимости, последующей записи на материальные носители.

2. Процессуальный порядок назначения рассматриваемых следственных действий различен.

Контроль и запись переговоров осуществляется в общем и особом порядке. В общем порядке, когда необходимо получить сведения, имеющие значение для доказывания обстоятельств уголовного дела, данное следственное действие производиться только по делам о преступлениях средней тяжести, тяжких и особо тяжких и предполагает во всех случаях получение судебного разрешения. Особый порядок применяется при наличии угрозы совершения насилия, вымогательства и других преступных действий в отношении потерпевшего, свидетеля или их близких. Такой порядок может быть избран независимо от категории преступлений, поскольку цель следственного действия в этом случае, обусловлена не интересами расследования, а необходимостью обеспечения безопасности лиц, участвующих в производстве по делу, которая не может быть поставлена в зависимость от характера преступления[79]. В данном случае законодатель предусматривает две альтернативные процедуры назначения следственного действия: а) в случае письменного согласия в форме добровольного заявления лиц, в отношении которых поступили угрозы, – без судебного разрешения; б) при отсутствии такого заявления – по судебному решению. Процессуалистами

[79] В.Ю. Стельмах Следственные действия, ограничивающие тайну связи. – М.: Юрлитинформ, 2016. С. 268-269.

подчеркивается, что «когда индивид сам инициирует доступ третьих лиц к своим переговорам… судебного решения не требуется»[80].

Порядок осуществления следственного действия, предусмотренного статьей 186.1 УПК РФ не зависит от процессуального статуса участников уголовного судопроизводства, являющихся абонентами, и непосредственной цели получения данной информации, так как по своему содержанию получение информации о соединениях между абонентами и (или) абонентскими устройствами не позволяет отразить сведения о конкретных угрозах в адрес указанных лиц. Данное следственное действие всегда требует судебного разрешения, без каких-либо исключений.

3. Получение информации о соединениях между абонентами и (или) абонентскими устройствами носит длящийся характер в силу наличия технического этапа, во время которого возможно производство других следственных действий. Кроме того, следственное действие, предусмотренное статьей 186.1 УПК РФ, фактически, состоит из трех взаимосвязанных действий (истребование информации, ее осмотр и приобщение к уголовному делу электронного носителя информации в качестве вещественного доказательства или распечатки в качестве иного документа), что подчеркивает его комплексный характер. По структуре контроль и запись переговоров в целом довольное схожее следственное действие с получением информации о соединениях между абонентами и (или) абонентскими устройствами. Но технический этап того и другого имеет существенное различие. Так, при контроле и записи переговоров происходит подключение с помощью технических средств (аппаратного комплекса СОРМ) к интересующему абонентскому терминалу, конспиративный слуховой контроль и запись переговоров[81]. При получении информации о

---

[80] Брусницын Л. УПК РФ: соответствует ли он рекомендациям ООН и Совета Европы по обеспечению безопасности свидетелей // Уголовное право. 2010. № 6. С. 65–66; См. также: Коротков А.П., Токарева М.Е. Контроль и запись переговоров при осуществлении оперативно-розыскных мероприятий и следственных действий: методические рекомендации / А.П. Коротков, М.Е. Токарева. – Москва, 2005. – С. 13.

[81] Балашов Н.М., Маликов С. В. Криминалистика: учебник М., 2005. С. 312.

соединениях между абонентами в автоматическом режиме накапливается информация, принятая аппаратурой оператора связи.

4. Результатом производства контроля и записи переговоров является фонограмма переговоров, а получения информации о соединениях между абонентами – список соединений абонентского номера (детализация). Хотя по факту и в том и другом случае – это электронный носитель информации.

5. Важным отличием контроля и записи переговоров от получения информации о соединениях между абонентами и (или) абонентскими устройствами является время, за которое следователь хотел бы истребовать интересующую информацию. Контроль и запись переговоров проводится ориентирован «на будущее», то есть для получения информации, содержащейся в телефонных переговорах в период, установленный после получения судебного разрешения, поскольку содержание всех ведущихся разговоров аппаратурой операторов связи не фиксируется[82]. Получение информации о соединениях между абонентами может быть направлено как на будущий период, так и на прошлый промежуток времени, который ограничен 3 годами. Именно такой срок установлен законодателем для хранения накопленной информации[83].

6. Для контроля и записи переговоров установлен определенный срок проведения, который ограничивается сроком предварительного расследования. При получении информации о соединениях между абонентами, исходя из смысла п. 3 ч. 2 ст. 186.1 УПК РФ, 6-месячный срок проведения установлен только применительно к перспективному порядку производства данного следственного действия. Для ретроспективного порядка каких-либо временных ограничений получения информации законом не предусмотрено.

7. При осуществлении контроля и записи переговоров законодательно не определена периодичность представления полученной информации следователю,

---

[82] Стельмах В.Ю. Следственные действия, ограничивающие тайну связи. – М.: Юрлитинформ, 2016. С. 271.

[83] О порядке оказания услуг телефонной связи: постановление правительства Российской Федерации от 9 декабря 2014 г. № 1342 г. Москва. – [Электронный ресурс]. − URL: http:// www.consultant.ru.

а предоставляется по запросу следователя. В ч. 4 ст. 186.1 УПК РФ установлено, что полученная информация о соединениях между абонентами представляется следователю не реже одного раза в неделю. Очевидно, что такой более детализированный порядок является следствием только более позднего принятия ст. 186.1 УПК РФ, в которой была учтена необходимость конкретизации сроков представления следователю полученной информации.

Касаемо сравнения получения информации о соединениях между абонентами и (или) абонентскими устройствами и выемки, нами выделены следующие отличительные признаки:

1. Как отмечалось выше, предметом получения информации о соединениях между абонентами и (или) абонентскими устройствами выступают сведения об абонентах, абонентских устройствах и их соединениях, без отражения содержания разговора или переписки. Предметом выемки выступают овеществленные объекты, существующие на материальных носителях к моменту принятия решения о производстве следственного действия. Это в полной мере относится и к выемке электронных носителей информации (например, сотового телефона). Кроме того, в ходе выемки могут изыматься любые объекты и документы, находящиеся у любых лиц или организаций, т.е. по содержанию предмета выемка ограничений не имеет.

2. Очевидно различие и по процессуальному порядку производства следственных действий. По общему правилу, выемка производится на основании постановления следователя, а в предусмотренных УПК РФ ситуациях – по судебному решению. В прямо установленных законом случаях выемка может быть проведена без судебного решения, с уведомлением прокурора и суда о ее производстве (ч. 5 ст. 165 УПК РФ). Получение информации о соединениях между абонентами и (или) абонентскими устройствами проводиться только по судебному решению.

3. Следственные действия, предусмотренные статьями 186.1 и 186 УПК РФ, являются длящимися, что обусловлено наличием соответствующих технических

этапов. Выемка отличается своей простой структурой, представляя собой одно действие, и одномоментностью, что не предполагает перерывов.

4. Еще одним важным отличием выемки от рассматриваемого следственного действия является процедура получения интересующей следствие информации. Действия по изъятию предметов и документов при выемке производятся самим следователем, в то время как информация о соединениях между абонентами копируется работниками операторов связи и направляется следователю.

Сравним получение информации о соединениях между абонентами и (или) абонентскими устройствами с указанными оперативно-розыскными мероприятиями.

1. Получение информации о соединениях между абонентами регулируется УПК РФ, оперативно-розыскные мероприятия – Федеральным законом «Об оперативно-розыскной деятельности».

2. Получение информации о соединениях между абонентами возможно только после возбуждения уголовного дела, оперативно-розыскные мероприятия могут быть проведены до возбуждения уголовного дела и в процессе расследования.

3. Инициатива производства следственного действия принадлежит следователю, и именно он (с согласия руководителя следственного органа) возбуждает ходатайство перед судом о получении информации о соединениях между абонентами. Оперативно-розыскные мероприятия инициируются оперативным сотрудником, который возбуждает соответствующее ходатайство по согласованию с руководителем органа дознания, осуществляющего оперативно-розыскную деятельность.

4. Субъектом принятия информации о соединениях между абонентами является следователь, а результатов оперативно-розыскных мероприятий – субъекты ОРД.

5. Результаты получения информации о соединениях между абонентами оформляются в порядке, предусмотренном УПК РФ (составляется протокол

осмотра полученной детализации), итоги оперативно-розыскных мероприятий фиксируются в справках и сводках об их проведении[84].

6. Результаты следственного действия имеют непосредственное доказательственное значение, в то время как результаты оперативно-розыскных мероприятий прежде чем приобрести статус доказательства, соответствующего всем критериям, требуют особой процедуры их введения в уголовно-процессуальную деятельность[85]. В абз. 3 п. 14 Постановления пленума Верховного Суда Российской Федерации от 31 октября 1995 г. № 8 «О некоторых вопросах применения судами Конституции Российской Федерации при осуществлении правосудия» установлено, что результаты оперативно-розыскных мероприятий, связанных с ограничением конституционных прав граждан, могут быть использованы в качестве доказательств, когда они получены по разрешению суда и проверены в соответствии с уголовно-процессуальным законодательством.

Итак, сравнительный анализ процессуальных особенностей получения информации о соединениях между абонентами и (или) абонентскими устройства со схожими по форме и содержанию другими следственными действиями, а также с оперативно-розыскными мероприятиями позволяет нам говорить об уникальности рассматриваемого следственного действия и присущих исключительно ему характеристик. Следовательно, получение информации о соединениях между абонентами и (или) абонентскими устройствами является

---

[84] Криминалистика: учебник / Л. Я. Драпкин, В. Н. Карагодин. 2-е изд., перераб. и доп. М., 2011. С. 263.

[85] Веденин А.В. Понятие результатов оперативно-розыскной деятельности // Вестник Владимирского юрид. ин-та. 2008. № 2 (7). С. 114; См. также: Доля Е.А. Использование в доказывании результатов оперативно-розыскной деятельности. М., 1996. С. 35; Макаров А.В., Фирсов О. В. Особенности использования результатов оперативно-розыскной деятельности в процессе доказывания по уголовным делам // Российский следователь. 2012. № 8. С. 43; Миролюбов С. Л. Генезис правовой основы использования результатов ОРД в доказывании по уголовным делам: актуальные проблемы // Вестник Владимирского юридического института. 2009. № 1 (10). С. 115; Фомин М.А. Допустимость материалов ОРМ в качестве доказательств по делам о получении взятки // Уголовный процесс. 2011. № 2 (62). С. 20; Фролова Т.А. Закрепление результатов ОРД и передача их следственным органам и суду // Уголовный процесс. 2008. № 3 (39). С. 30; Фролова Т.А. Использование в доказывании результатов оперативно-розыскной деятельности // Уголовный процесс. 2008. № 9 (45). С. 10; Шергин Г.Н. Использование результатов ОРД в уголовно-процессуальном судопроизводстве // Российский следователь. 2011. № 11. С. 24–26.

обособленным, самостоятельным следственным действием и, безусловно, занимает важное место в их системе. Благодаря техническому оборудованию оператора связи, и потенциалу данного следственного действия, у правоохранителей есть возможность получения и использования доказательственной информации, касающейся абонентов и их соединений в рамках сотовой связи. Следует констатировать тот факт, что технический прогресс не стоит на месте, а законодательство при этом не успевает усовершенствовать и приспособить правовые документы к новым реалиям, актуальным на тот момент. Это подтверждает то, что получение информации о соединениях между абонентами и (или) абонентскими устройствами было введено в УПК РФ в 2010 году, а средства связи начали свое развитие уже с конца 1990-х – начала 2000-х годов. Видится, что развитие следственных действий, предметом которых является получение сведений, передаваемых с помощью средств электросвязи, будет обусловлено техническими возможностями этих средств. Поэтому можно предположить, что дальнейшее развитие системы следственных действий будет происходить в двух направлениях: либо по мере появления новых средств коммуникации будет вводиться соответствующее следственное действие, обеспечивающее возможность получения сведений, передаваемых с помощью этих средств, что сложно представить, либо будет установлено единое следственное действие, которое позволит получить сведения о любых взаимодействиях всех однотипных устройств связи, имеющих одинаковые принципы передачи этих сведений. К вопросу о расширение возможностей получения информации о соединениях между абонентами и (или) абонентскими устройствами, отметим, что это обусловлено научно-техническим прогрессом и должно стать задачей законодателя. Исходя из данных анкетирования, следует, что 97,7% опрошенных считают необходимым расширять возможности указанного следственного действия[86]. Однако, к данному вопросу следует подходить осторожно, необходимо тщательно взвесить все «за» и «против», так как выделение новых следственных действий и дробление уже имеющихся, усложнит

[86] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

и без того перегруженный уголовно-процессуальный закон, порождая самые разные ошибки его применения среди практических сотрудников.

ГЛАВА 2. ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИЕ АСПЕКТЫ ПРОИЗВОДСТВА ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ

§ 1. Типичные следственные ситуации, требующие производства следственного действия «Получение информации о соединениях между абонентами и (или) абонентскими устройствами» и программа действий следователя

В процессе расследования преступления следователь всегда находится в условиях выбора тактически оптимального, исходя из сложившейся следственной ситуации, процессуального действия. Этап принятия решения присутствует при производстве любого следственного действия, в большей или меньшей степени, однако, особое значение такое решение приобретает при производстве следственных действий, требующих судебного санкционирования, к которым относится получение информации о соединениях между абонентами и (или) абонентскими устройствами. Сложность и в тоже время важность такого подхода обусловлена тем, что в случае ошибочного принятия решения о производстве рассматриваемого следственного действия, во-первых, будет проделана трудоемкая, затратная по времени и в итоге ненужная работа, во-вторых – безосновательно ограничены конституционные права граждан.

На решение о производстве получения информации о соединениях между абонентами и (или) абонентскими устройствами влияет информационный компонент, включающий в себя определенный объем и качество сведений об обстоятельствах, подлежащих установлению по расследуемому уголовному делу. В связи с этим, анализ имеющейся следственной ситуации, является определяющим фактором, влияющим на принятие решения. Действительно, чем больше доказательственной и ориентирующей информации получено следствием, тем более оптимальные решения принимаются следователем, тем легче и эффективнее они реализуются[87].

---

[87] Драпкин Л.Я., Долинин В.Н. Тактика следственных действий: учебно-практическое пособие. – Екатеринбург: издательский дом Уральского государственного университета, 2015. – С. 17.

Понятие следственной ситуации сформировалось в науке не сразу, а в результате продолжительной дискуссии известных ученых-правоведов. Научная дискуссия сводилась к разрешению спора о содержании и месте следственной ситуации в процессе расследования. Исходя из точки зрения Л.Я. Драпкина[88], И.Ф. Герасимова[89], следует, что ситуации занимают место внутри процесса расследования преступления. Мы солидарны с мнением указанных авторов, так как следственная ситуация, во-первых, неразрывно связана с расследованием и изначально отражает обстановку события, во-вторых, является предпосылкой для производства необходимых действий, т.е. выступает как совокупность факторов, обусловивших дальнейшие действия лиц, осуществляющих расследование по уголовному делу и, в-третьих, следственная ситуация предполагает качественную оценку всех уже известных обстоятельств.

Большая группа ученых понимают следственную ситуацию как объективную обстановку, в которой ведется расследование (Р.С. Белкин, В.А. Образцов, В.Г. Танасевич, В.И. Шиканов)[90]. По мнению Р.С. Белкина, «следственная ситуация – это совокупность условий, в которых в данный момент осуществляется расследование, т.е. та обстановка, в которой протекает процесс доказывания»[91].

Т.С. Волчецкая определяет следственную ситуацию как степень информационной осведомленности следователя о преступлении, а также состояние процесса расследования, сложившееся на любой определенный момент времени, анализ и оценка которого позволяют следователю принять наиболее целесообразное по делу решение[92].

---

[88] Драпкин Л.Я. Понятие и иллюстрация следственных ситуаций. Следственные ситуации и раскрытие преступлений. - Свердловск, 1975. - С. 28.

[89] Герасимов И.Ф. Принципы построения методики раскрытия преступлений. Вопросы криминалистической методологии, тактики и методики расследования. - М.,1973. С. 82

[90] Образцов В. А., Танасевич В. Г. Понятие и криминалистическое значение следственной ситуации // Сов. государство и право. 1979. № 8. С. 113; Шиканов В. И. Разработка теории тактических операций – важнейшее условие совершенствования методики расследования преступлений // Методика расследования преступлений. М., 1976. С. 157.

[91] Белкин Р. С. Курс советской криминалистики. М., 1979. Т. 3 С. 70.

[92] Волчецкая Т. С. Криминалистическая ситуалогия: монография / под ред. проф. Н.П. Яблокова. М.; Калининград, 1997. С. 93.

Распространение получило определение следственной ситуации, предложенное И.Ф. Герасимовым: «следственная ситуация – это сложившаяся на определенный момент расследования, внутренне склонная к изменению совокупность характеризующих расследование материальных, информационных и иных факторов и их оценка, которая обусловливает основные направления расследования, принятие решений и выбор способов действий»[93].

В нашем понимании, вышеуказанные авторы определили следственную ситуацию как совокупность определенных данных об определенном этапе расследования.

Для целей настоящего исследования, предлагается в качестве основополагающего термина «следственная ситуация» использовать ее определение, сформулированное Л. Я. Драпкиным и разделяемое рядом ученых. В этом определении, следственная ситуация понимается как «динамическая информационная система, отражающая с различной степенью адекватности многообразные логико-познавательные связи между установленными и еще неизвестными обстоятельствами, имеющими значение для дела, тактико-психологические отношения участников (сторон) уголовного судопроизводства, а также организационно-управленческую структуру и уровень внутренней упорядоченности процесса расследования»[94]. Исходя из смысла данного определения, следует, что процесс принятия и реализации адекватных сложившейся ситуации следственных и оперативно-розыскных решений периодически осложняется разнообразными трудностями. В зависимости от соотношения трудностей, противостоящих следователю, и совокупности всех его ресурсов возникают простые или сложные следственные ситуации.

Для простых ситуаций характерно наличие несущественных тактических, информационных трудностей, проблем психологического плана, и, напротив, наличие в распоряжении следователя доказательственной информации и

---

[93] Там же. С. 90.

[94] Драпкин Л. Я. Общая характеристика следственных ситуаций // Следственная ситуация: сб. научных трудов. – Москва, 1984. С. 18.

возможностей по успешному преодолению возникающих сложностей, что способствует становлению благоприятных условий и обстановки процесса расследования преступления. При простых следственных ситуациях отсутствует тактических риск, управленческая и организационная неупорядоченность, проблемность, конфликт и противоборство сторон. Поэтому в рамках таких следственных ситуациях, как правило, все процессуальные и оперативно-розыскные решения успешно реализуются, а производство следственных действий максимально эффективно и влечет положительный результат.

Иное положение возникает по делам, в случаях затруднения процесса расследования образованием противодействия со стороны подозреваемого (обвиняемого) и других конфликтующих с ним лиц, отсутствием надежных источников информации, способов и средств достижения целей, времени, средств и ресурсов. Именно при таких обстоятельствах возникает неблагоприятная обстановка, которая влечет за собой образование сложной следственной ситуации. В зависимости от количества, характера и содержания формирующих негативных факторов все сложные следственные ситуации можно дифференцировать на несколько групп: проблемные, конфликтные, тактического риска, организационно неупорядоченные и комбинированные[95].

Перед тем как перейти к рассмотрению типичных следственных ситуаций, в которых необходимо производство получения информации о соединениях между абонентами и (или) абонентскими устройствами, полагаем правильным выделить общие ситуации расследования, складывающиеся на момент принятия решения о производстве указанного следственного действия.

Заметим, что на сегодняшний день в научной и методической литературе отсутствует подробный анализ ситуаций, которые могли бы сложиться к моменту принятия решения о производстве получения информации о соединениях между

---

[95] Криминалистика: учебник для бакалавров / под ред. Л. Я. Драпкина. М., 2013. Сер. Бакалавр: Углубленный курс. С. 54-55.

абонентами и (или) абонентскими устройствами. Классификацию таких ситуаций, мы находим в работе Е.С. Лапина, который выделяет следующие ситуации:

- сделано заявление подозреваемым (обвиняемым) о наличии алиби, связанного с абонентскими соединениями;

- имеется информации о том, что подозреваемый может звонить потерпевшему или его близким после совершения преступления, или о том, что он звонил им до совершения преступления;

- имеют место данные о том, что предполагаемый преступник выходит или возможно будет выходить на связь со своими родственниками, близкими, знакомыми или соучастниками преступления;

- есть информация, что перед преступлением имелись телефонные переговоры (сговор) между соучастниками – членами организованной группы или группы лиц по предварительному сговору[96].

Также интересной является классификация ситуаций использования средств мобильной связи при совершении преступлений, в зависимости от совокупности действий, произведенных с мобильным телефоном, представленной Н.А. Архиповой. Автор выделил:

- ситуации, когда мобильные телефоны используются в качестве средства организации подготовки, совершения, сокрытия преступных действий между участниками преступной группы и иными лицами;

- ситуации, когда мобильные телефоны используются как непосредственное средство совершения преступления;

- ситуации, когда преступные действия направлены на хищение мобильных телефонов;

- ситуации, когда использование мобильного телефона напрямую не связано с совершением преступления, а носит случайный, ситуационный характер[97].

---

[96] Лапин Е.С. Тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами: монография. – Юрлитинформ, 2014. С. 91.

[97] Архипова Н.А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи: автореф. дис. … канд.юрид. наук. СПб.: Санкт-Петербургский университет МВД России, 2011. С. 14-15.

Проанализировав вышеуказанные ситуации, мы пришли к выводу, что перечень ситуаций расследования, при котором необходимо производство, следственного действия, предусмотренного статьей 186.1 УПК РФ, может быть расширен и конкретизирован. Видится что, данный перечень должен содержать ситуации, когда сотовый телефон похищен, но имеется информация о его последнем местонахождении, дате и времени последнего вызова; случаи, когда существует возможность установить предполагаемого преступника или преступную группу, путем производства получения информации о соединениях между абонентами и (или) абонентскими устройствами в отношении неопределенного круга лиц.

Таким образом, мы выделили следующие группы ситуаций расследования, в рамках которых предлагаем типичные следственные ситуации, требующие включения в алгоритм действий следователя получения информации о соединениях между абонентами и (или) абонентскими устройствами:

Ситуации, когда имеются данные, что до, во время и после совершения преступления имели место телефонные переговоры между соучастниками преступных действий, членами организованной группы или группы лиц по предварительному сговору. 90,7% опрошенных практических сотрудников отметили, что в таких случаях субъект расследования принимает решение о получении биллинговой информации[98].

Действительно, до совершения преступления преступниками разрабатываются все возможные варианты дальнейших мероприятий, направленных на достижения преступных целей, используя при этом сотовую связь для корректировки и согласования действий. Осуществляя подготовку, преступники продумывают план по сокрытию следов, приобретая новые абонентские устройства, SIM-карты или похищая сотовые телефоны для временного использования при совершении противоправных действий. Использование средств сотовой связи во время совершения преступления позволяет участниками преступной группы действовать скоординировано и

[98] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

согласовано. После совершения преступления, преступник может выходить на связь с потерпевшим (свидетелем) в целях оказания давления, с родственниками (знакомыми), соучастниками преступления. В другом случае, сразу после совершения преступления, уничтожается SIM-карта, сотовый телефон, предпринимаются попытки изменения код IMEI-устройства и т.п.

В качестве примера, указанной ситуации может послужить уголовное дело по факту незаконной предпринимательской деятельности, которое расследовалось следственной частью ГСУ ГУ МВД России по Свердловской области. Дело было возбуждено по факту задержания на автомобильной трассе Серов-Екатеринбург грузовых автомашин, незаконно перевозивших спитросодержащую продукцию. На момент задержания водителя одного из грузовиков, не было известно ни место приобретения, хранения, ни отправители, ни получатели. Анализ информации о соединениях между абонентами и (или) абонентскими устройствами позволил установить других водителей, осуществляющих незаконную перевозку груза, их маршрут передвижения и отправную точку маршрута – поселок Лобва Свердловской области, где расположен биохимический завод производящий данную продукцию. Также было установлено, что каждый абонент (водитель) с момента прибытия для погрузки, и далее с определенной периодичностью отзванивался ограниченному кругу лиц[99]. Каждый из вызовов был зафиксирован базовой станицей оператора сотовой связи, поэтому, получив детализацию вызовов с привязкой к координатам местоположения базовых станций, следствию удалось установить не только лиц, причастных к совершению преступления, но и проследить точку отправления, примерный маршрут незаконной перевозки указанной продукции, точное время вывоза.

Приведенный пример показывает что, посредством сотовой связи, осуществлялась подготовка (с водителями связывались и договаривались о месте и времени погрузки), а затем координация действий в процессе совершения преступления.

---

[99] Официальный сайт ГУ МВД России по Свердловской области. – [Электронный ресурс]. − URL: https://66.мвд.рф.

Данной группе ситуаций расследования соответствуют типичные следственные ситуации, в зависимости от наличия информации о преступлении, об использовании средств сотовой связи преступником.

1) преступник установлен, имеется информация о преступлении и собраны данные, свидетельствующие об использовании средств сотовой связи;

2) преступник не установлен, имеются сведения о преступлении, собраны данные, свидетельствующие об использовании виновным средств сотовой связи;

3) преступник не установлен, но имеются сведения о совершении преступления, сотовый телефон не обнаружен, информации об использовании средств сотовой связи нет.

Первая следственная ситуация является простой, так как в распоряжении следователя, достаточно исходных данных, имеются возможности успешного преодоления психологических и тактических трудностей, пополнения дефицита доказательственной информации, нет условий тактического риска или конфликта, что свидетельствует о благоприятной обстановке расследования. В такой ситуации необходимо выполнение следующего алгоритма действий следователя:

1. Допросить подозреваемого. Помимо обстоятельств преступления и его роль в преступной группе, необходимо уточнить каким образом осуществлялась связь между соучастниками, обстоятельства использования средств сотовой связи при подготовке и непосредственно совершении преступления, имеются ли документы на используемый сотовый телефон, при каких обстоятельствах он приобретен, где в настоящее время находится (если не изъят, то выброшен, потерян, продан, передан кому-либо), на кого оформлена SIM-карта, какой абонентский номер, есть ли документы на SIM-карту.

2. Если сотовый телефон, используемый подозреваемым изъят, то провести осмотр, при необходимости с участием специалиста. Приобщить сотовый телефон в качестве вещественного доказательства.

3. Получить информацию о соединениях между абонентами и (или) абонентскими устройствами, в целях подтверждения показаний подозреваемого,

установления его местоположения в период совершения преступления, выявления иных лиц, причастных к совершению преступления.

4. Использовать полученную информацию об абонентах и (или) абонентских устройствах в ходе повторного допроса, целях установления новых обстоятельств преступления, соучастников или иных лиц, причастных к совершению преступления.

Вторая следственная ситуация видится нам проблемной, так как на первоначальном этапе расследования в распоряжении следователя имеется совокупность неполных, недостаточных или противоречивых сведений (исходные данные) и неизвестное искомое (обстоятельство, подлежащее установлению и доказыванию). Однако, очевидно, что установить виновность лица и определить дальнейшее направление расследования представляется возможным.

В данной следственной ситуации выполняются следующие действия:

1. Осмотр места происшествия. В случае обнаружения сотового телефона, SIM-карты проводится их осмотр с участием специалиста и приобщение в качестве вещественного доказательства.

2. Получение информации о соединениях между абонентами и (или) абонентскими устройствами с целью установить абонентов, которые были активные в известный промежуток времени в районе места преступления. Если есть информация об устройстве или абонентском номере, установить их принадлежность, получить детализацию соединений с привязкой к местоположению, затем тщательно проанализировать полученные сведения.

3. Проверка выявленных абонентов на причастность к совершению преступных действий.

Третья следственная ситуация также проблемная, характеризуется повышенной остротой проблем и трудностей, и требует еще больших усилий для ее разрешения и использования широкого спектра следственных и оперативно-розыскных мероприятий. Для данной ситуации характерен минимум исходной информации, сведений о преступнике нет.

Основными методами разрешения такой проблемной ситуации являются, выдвижение всех возможных версий, проведение гласных и негласных оперативно-розыскных мероприятий, сплошной перебор всех возможных вариантов[100]. Таким образом, алгоритм действий следователя будет варьироваться в зависимости от конкретной следственной ситуации, каждое последующее решение о проведение того или иного мероприятия будет зависеть от результатов предыдущего. Наиболее эффективным способом успешного разрешения данной следственной ситуации является производство тактической операции, основными задачами которой будут: установление места и времени преступления, установление пользователей сотовой связи в определенный интервал времени, в районе места происшествия, свидетелей и лиц, причастных к совершению преступления.

Выполнение этих задач достигается путем производства следующих следственных действий и оперативно-розыскных мероприятий:

1. Проведение осмотра места происшествия.

2. Допросы свидетелей и очевидцев.

3. Производство экспертиз (судебно-медицинской экспертизы, трасологической и др.).

4. Получение информации о соединениях между абонентами и (или) абонентскими устройствами для установления перечня абонентских соединений, состоявшихся в конкретный период в вблизи места происшествия.

5. Проанализировать полученную информацию на предмет установления тех соединений, которые были совершены вблизи с местом происшествия, и проверить, не совпадают ли места вызовов с местом происшествия на дату преступления и сравнить с данными из других источников (камеры видеонаблюдения, показания свидетелей и т.п.).

---

[100] Драпкин Л.Я., Долинин В.Н. Тактика следственных действий: учебно-практическое пособие. – Екатеринбург: издательский дом Уральского государственного университета, 2015. – С. 18.

6. Поручения органу дознания о выявлении лиц, возможно причастных к совершению преступления, наведении справок и разработке лиц, осуществляющим содействие правоохранительным органам.

7. Провести допросы выявленных лиц на причастность к совершению преступления.

Еще раз подчеркнем, что данный алгоритм действий может быть расширен и варьироваться в зависимости от конкретной следственной ситуации, мы лишь предлагаем примерный алгоритм действий следователя или его часть, когда принимается решение об использовании при расследовании следственное действия, предусмотренного статьей 186.1 УПК РФ.

Ситуации, когда сотовый телефон используется в качестве средства совершения преступления. Данная группа ситуаций характерна для так называемого «телефонного мошенничества», являющегося очень распространенным в настоящее время. Жертвой преступления выступает пользователь абонентского устройства связи. Такие преступления, как правило, совершаются группой лиц, причем распространены случаи, когда руководители групп отбывают наказания в местах лишения свободы[101].

Мошенники при подготовке преступления находят абонентские номера жертв по наводке, путем случайного набора номеров, используя SMS рассылку, объявления в интернете о продаже движимого и недвижимого имущества, поиска работы, сайтов знакомств и т.п. Лица, занимающиеся мошенничествами, являются «хорошими психологами», они сообщают ложную информацию, проверяют реакцию, затем входят в доверие и завуалировано сообщают свои предложения, направленные на хищение денежных средств. Как правило, преступник на первоначальном этапе расследования еще не установлен, однако всегда имеются сведения о способе передачи денежных средств потерпевшего.

---

[101] Опыт учреждений и органов ФСИН России по предупреждению поступления средств мобильной связи в исправительные учреждения и следственные изоляторы: сб. передового опыта / сост. С.Ю. Смирнов. М., 2010. С. 6.

Наличие таких ситуаций отмечено 81,4% анкетируемых практических сотрудников[102] и, очевидно, что алгоритм действий следователя не обходится без получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Выделим типичные следственные ситуации, характерные для данного варианта процесса расследования, в зависимости от способа передачи денежных средств мошеннику.

1) преступник не установлен, имеется информации о телефонном мошенничестве, потерпевший передал обговоренную сумму денег курьеру либо оставил в условленном месте.

2) преступник не установлен, имеется информации о телефонном мошенничестве, деньги переведены через банк либо через приложение «Мобильный банк»[103].

3) преступник не установлен, имеется информации о телефонном мошенничестве, деньги переведены через различные интернет сервисы (Qiwi кошелек, Яндекс деньги и т.п.).

4) преступник не установлен, имеется информации о телефонном мошенничестве, деньги переведены на абонентский номер мошенника.

Видится, что все отмеченные ситуации характеризуются как сложные проблемные, так как перед следователем возникают препятствия, связанные исследованием и получением фактических данных, содержащихся в достоверно или предположительно определенных источниках (носителях) информации. Имея в распоряжении электронные следы, следователю необходимо перейти от полного или частичного незнания к полному или достоверному знанию[104]. Однако, некоторые из этих ситуаций, могут оказаться простыми, например, если

---

[102] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

[103] Мобильный банк - это услуга, с помощью которой возможно совершать различные платежи с карты и запрашивать информацию по собственным банковским картам через мобильный телефон, посредством специального мобильного приложения.

[104] Драпкин Л. Я. Следственные ситуации: роль и значение в раскрытии и расследовании преступлений: учебное пособие / Л. Я. Драпкин, Д. Л. Кокорин, И. Г. Пяткова. – Екатеринбург: Уральский юридический институт МВД России, 2017. – С. 8.

преступник оказался недостаточно неопытным, действовал один, пользовался абонентским устройством или SIM-картой, зарегистрированными на свое имя, а потерпевший перечислил денежные средства на его абонентский номер. В таком случае, не составит труда, получить интересующие следствие сведения от оператора связи, установить преступника и осуществить его задержание. Аналогично, эта же ситуация может быть мнимо простой. Так, при тех же действиях следователя по установлению личности преступника, выявляется, что сотовый телефон или SIM-карта действительно оформлены на соответствующее лицо, но были утеряны либо украдены до совершения преступления. Таким образом, процедура определения принадлежности абонентского номера конкретному лицу значительно усложняется.

Рассмотрим алгоритм действий следователя в каждой из перечисленных следственных ситуаций.

В рамках первой следственной ситуации необходимо провести следующий алгоритм действий:

1. Допросить потерпевшего, выяснив все обстоятельства и подробности состоявшегося разговора с мошенником. Целесообразно узнать с какого номера поступил звонок, как представился преступник, суть его предложений, количество состоявшихся бесед, какая сумма была передана и за какие услуги, место и способ передачи денежных средств. Кроме того, необходимо выяснить особенности голоса и речи преступника. Если деньги передавались через курьера, то при допросе выясняются все признаки внешности, которые запомнил потерпевший и другие данные о курьере.

2. Получить информации о соединениях между абонентами и (или) абонентскими устройствами.

3. Установив по детализации вызовов, лицо, на которое зарегистрирован абонентский номер, проверить его на причастность к совершению преступных действий. Можно использовать оперативные возможности органа дознания.

4. Если лицо, на которое оформлен абонентский номер, заявляет, что не оформлял данную SIM-карту у оператора, то необходимо истребовать договор об

оказании услуг сотовой связи у оператора сотовой связи по данному номеру. Установить и допросить сотрудника компании сотовой связи, оформившего договор об оказаний услуг сотовой связи.

5. Запросив сведения о местоположении абонентского устройства в момент соединения с потерпевшим, следует проверить наличие в районе базовой станции мест лишения свободы. В случае подтверждения, направить в подразделение ФСИН поручение по установлению личности преступника и обнаружению абонентского устройства связи.

6. Если устройство связи обнаружено, необходимо установить какие еще SIM-карты использовались в данном устройстве, и проверить соответствующие абонентские соединения. Это позволить найти соучастников преступления или других потерпевших.

Вторая следственная ситуация, может содержать мероприятия, перечисленные в рамках алгоритма действий первой следственной ситуации, но при этом отличается наличием действий по поиску и систематизации информации от банковских учреждений, через которые осуществлялся перевод.

В связи с этой особенностью, к алгоритму действий первой следственной ситуация добавляются следующие мероприятия:

1. В рамках допроса уточнить, каким именно банковским сервисом и какого банка пользовался потерпевший («блиц-перевод», переводом через банкомат по номеру карты, перевод в отделении банка или перевод через приложение «Мобильный банк»).

2. Получить все, имеющиеся у потерпевшего сведения о получателе (реквизиты счета, чеки, выписки по счету, абонентский номер, предоставленный для перевода «по номеру телефона», другие известные данные о получателе).

3. С целью уточнения данных о личности получателя, запросить в банке информацию обо всех совершенных действиях, с указанием дат, адресов банков и банкоматов, сумм переводов и т.п.

4.Установление личности получателя, розыск и допрос на предмет причастности его к совершению преступления.

Алгоритм действий третей следственной ситуации будет отличаться от предыдущей только тем, что запросы о получателе денежных средств будут направляться в иные организации, через сервисы которых осуществлялся перевод денежных средств преступникам.

Как уже отмечалось, четвертая следственная ситуация может быть простой, или мнимо простой. В связи с этим, алгоритм действий следователя имеет следующую структуру и содержание:

1. Допрос потерпевшего, с установлением тех же обстоятельств, что и при допросе в рамках первой следственной ситуации.

2. Получение информации о соединениях между абонентами и (или) абонентскими устройствами для установления сведений о лице, его соединениях.

3. Допрос, установленного лица, на предмет причастности его к совершению преступления. Если подтверждается факт совершения указанным лицом преступления, то ситуация благоприятна и лишена проблемных аспектов, а соответственно считается простой. Но лицо может приводить различные доводы о якобы своей непричастности к преступлению, пытаясь ввести следователя в заблуждение. В таком случае возникает мнимо простая ситуация, а алгоритм действий следователя дополняется другими мероприятиями.

4. Анализируются сведения о местоположении абонентского устройства, номера других SIM-карт, работающих в искомом устройстве.

5. Осуществляется проверка наличия в районе базовой станции мест лишения свободы. В случае подтверждения, соответствующее поручение направляется в подразделение ФСИН для установлению личности преступника и обнаружения абонентского устройства связи.

6. Если преступник еще не установлен, то проводятся мероприятия, связанные с его выявлением, путем изучения мест, где наиболее часто проявляется абонентская активность лица и близ, находящихся мест, где могут быть камеры видеонаблюдения, пропускные пункты и т.п.

7. Проверяются все абонентские соединения, которые зафиксированы в детализации, на предмет причастности абонентов к преступным действиями.

Проводятся допросы для выяснения обстоятельств приобретения абонентского устройства и SIM-карты, фактов передачи их другим лицам, и установления все данных об этих лицах и т.п.

8. Сотрудникам оперативных подразделений могут быть даны поручения по работе с лицами, занимающимися скупкой и перепродажей мобильных устройств.

В данном случае ситуация оказывается мнимо простой и требует больше времени на разрешения, а также сил и средств правоохранительных органов.

Примеров следственных ситуаций, когда сотовый телефон используется в качестве средства совершения мошеннических действий, в частности «телефонных мошенничеств» множество. Приведем пример наиболее новой схемы мошенничества, которая набирает обороты с конца 2017 года.

Мошенники покупают у оператора сотовой связи виртуальные телефонные станции, якобы для работы вымышленной компании, а затем, с помощью веб-интерфейса меняют номер, принадлежащей им станции, на номер банка. Под видом сотрудников банка мошенники обзванивают случайных клиентов, узнают у них данные карт и перечисляют деньги доверчивых клиентов на свои счета, маскируя движение денежных средств.

Ситуации, когда мобильный телефон является предметом преступного посягательства.

Ярким примером таких ситуаций, выступают хищения средств сотовой связи, которые совершаются сравнительно часто.

В сентябре 2014 года Петрова, находясь совместно со своими подругами, увидела у одной из них в открытой сумке сотовый телефон «HTC Desire 300». Воспользовавшись тем, что потерпевшая отошла и оставила сумку без присмотра, Петрова похитила сотовый телефон. Допрос потерпевшей позволил установить информацию о похищенном абонентском устройстве, необходимую для его идентификации (IMEI-код, марку, модель, данные SIM-карты) и возможных свидетелей. Одновременно с вызовом свидетелей, следователем было проведено изучение информации о соединениях между абонентами и (или) абонентскими устройствами. Результатом последнего стали сведения об абоненте на 1 листе

бумаги формата А4, согласно которым в интересующий период времени украденный сотовый телефон использовался с другим абонентским номером, принадлежащим Куркалову Александру Сергеевичу. В ходе дальнейших следственных действий и оперативно-разыскных мероприятий было установлено, что Куркалов подрабатывает скупкой и продаже поддержанных сотовых телефонов. Он пояснил, что приобрел вышеуказанный мобильный телефон (не подозревая, что он краденный) у молодой девушки по описанию похожей на Петрову. В ходе дополнительного допроса с учетом имеющихся доказательств Петрова созналась в содеянном[105]. Волна преступлений, когда массово похищались мобильные телефоны в России уже прошла, однако, данные анкетирования[106] и результаты изучения уголовных дел[107] все же свидетельствуют совершении таких преступлений.

Рассмотрим классификацию типичных следственных ситуаций, характерных для данной группы преступлений, в зависимости от объема информации о похищенном абонентском устройстве, находящейся в распоряжении следователя.

1) преступник установлен и задержан, имеется информация о преступлении, похищенный сотовый телефон обнаружен и изъят.

2) преступник не установлен, имеется информация о преступлении, имеются все интересующие следствие сведения о похищенном абонентском устройстве.

3) преступник не установлен, известны обстоятельства преступления, информация о похищенном абонентском устройстве имеется не в полном объеме или отсутствует.

Для первой следственной ситуации характерны обстоятельства, при которых у задержанного преступника, обнаружен сотовый телефон, а данные о настоящем

---

[105] Уголовное дело № 140583135.Невьянский городской суд – [Электронный ресурс]. – URL:http://neviansky.svd.sudrf.ru/

[106] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

[107] См.: Результаты изучения уголовных дел, связанных с использованием средств сотовой связи, в процессе раскрытия и расследования преступлений (Приложение 2).

владельце отсутствуют. Эти ситуации чаще всего возникают, когда преступник задержан «по горячим следам» или же в ходе производства следственных действий и оперативно-розыскных мероприятий по другому уголовному делу. В данной следственной ситуации необходимо:

1. Провести осмотр изъятого мобильного телефона, описать внешние признаки, марку, модель, установить IMEI-код данного устройства.

2. Выяснить является ли данное абонентское устройство похищенным имуществом.

3. Получить информацию о соединениях между абонентами и (или) абонентскими устройствами, тем самым выяснить, кому принадлежит устройство.

4. При допросе потерпевшего установить обстоятельства пропажи сотового телефона и наличие документов, подтверждающих принадлежность устройства.

5. Проверить причастность задержанного к хищению сотового телефона.

По нашему мнению, рассматриваемая следственная ситуация характеризуется как простая, если при реализации данного алгоритма действий не возникает никаких барьеров. В ином случае, следственная ситуация может перерасти в проблемную, например, если задержанный утверждает, что купил находящийся при нем сотовый телефон, не подозревая, что он является похищенным, при этом указывает обстоятельства приобретения, но утверждает, что данные о продавце ему неизвестны. Также он может заявить, что нашел данное устройство или приобрел у неизвестного лица, например, на улице за символическую цену. В таком случае, ситуация осложняется, так как проверить достоверность таких показаний довольно сложно.

Вторая типичная следственная ситуация имеет место, когда на первоначальном этапе расследования следователь получает от потерпевшего всю необходимую информацию о похищенном сотовом телефоне и событии преступления. Данная ситуация является простой, так как предполагает переход от благоприятной исходной к благоприятной завершающей ситуации[108]. Имея в

[108] Драпкин Л.Я., Долинин В.Н. Тактика следственных действий: учебно-практическое пособие. – Екатеринбург: издательский дом Уральского государственного университета, 2015. – С. 15.

распоряжении достаточно исходных сведений, следователь может выстроить наиболее эффективную тактику действий по поиску похищенного имущества. Алгоритм действий в описываемой следственной ситуации можно представить следующим образом:

1. Осмотр места происшествия. Следует уделить особое внимание на то, как преступник прибыл и как покинул место происшествия. При отходе, он мог избавиться от SIM-карты, чехла, брелка.

2. При допросе потерпевшего, кроме обстоятельств совершения преступления, выясняется следующее: модель, цвет, размеры устройства, состояние, IMEI-код, данные SIM-карты, находившейся в устройстве на момент хищения, частные признаки (сколы, царапины, наклейки на корпусе, наличие брелков, цепочек и т.п.)

3. Выемка у потерпевшего документов на похищенное устройство (гарантийный талон, чек, руководство по эксплуатации, договор об оказании услуг сотовой связи) или коробки от устройства.

4. Поручить органам дознания проверить ломбарды, лиц, занимающихся скупкой и продажей бывших в употреблении устройств связи и т.п.

5. Поставить сотовый телефон на учет похищенного имущества.

6. Провести получение информации о соединениях между абонентами и (или) абонентскими устройствами, выяснить работает ли данной устройства с другой SIM-картой и установить возможное местоположение.

7. При установлении абонентских соединений, получить данные о личности и проверить этих лиц на причастность к событию преступления.

8. При установлении местоположения абонентского устройства или лица, причастного к совершению преступления, незамедлительно организовать задержание последнего, провести личный обыск, обыск по месту жительства, работы.

9. При обнаружении устройства изъять и провести его осмотр, приобщив в качестве вещественного доказательства.

Третья следственная ситуация имеет сходные признаки со второй, но осложнена отсутствием в распоряжения следователя некоторой важной информации об устройстве. Так, потерпевший может не помнить технические характеристики устройства, частные признаки и т.п. Не всегда сохраняются документы на сотовый телефон, а соответственно, нельзя оперативно установить IMEI-код. Ситуация является проблемной, однако верно выстроенный алгоритм действий, позволяет ее разрешить.

Таким образом, не имея в распоряжении полной информации об устройстве, необходимо:

1. Установить IMEI-код, путем производства следственного действия, предусмотренного статьей 186.1 УПК РФ. Оператор связи, имеет техническую возможность установить IMEI-код, зная абонентский номер, с которым работал сотовый телефон.

2. Получив IMEI-код, выполняется алгоритм действий, в соответствие со второй следственной ситуацией.

3. Если по каким-то причинам установить IMEI-код не представляется возможным, например преступник, сразу после хищения «перепрошил»[109] телефон и изменил его, то необходимо уточнить у потерпевшего признаки похищенного и обстоятельства преступления. Возможно, выясняются новые сведения.

4. Провести тактическую операцию по розыску похищенного имущества, поручив органам дознания, проверить ломбарды, комиссионные магазины, лиц, занимающихся скупкой и продажей бывших в употреблении устройств связи.

5. При обнаружении абонентского устройства, представить его на опознание потерпевшему.

Ситуации, когда есть информации о возможном выходе на связь скрывающегося от следствия преступника с его близкими, родственниками,

---

[109] Прошивкой (англ. Firmware, fw) называют содержимое энергонезависимой памяти компьютера или любого цифрового вычислительного устройства – микрокалькулятора, сотового телефона, GPS-навигатора и т.д., в которой содержится его программа. Перепрошивка – действия по внесению изменений в технические характеристики устройства.

знакомыми или предполагаемыми соучастниками преступления. Большая часть анкетируемых сотрудников отмечает наличие такого вида следственных ситуаций (82%)[110].

На наш взгляд, такие ситуации всегда проблемные, так как исходных сведений достаточно мало. Возникают они при расследовании похищений, когда достоверно известно о том, что преступники выдвинут требования или в рамках производства по любым другим уголовным делам, когда от соучастников преступления или из других источников известно о том, что преступник поддерживает с кем-либо связь.

Предполагаем, что для данного варианта расследования могут быть характерны следующие типичные следственные ситуации, в зависимости от наличия информации о преступнике:

1) имеется информация о преступнике, имеется информация о лицах, причастных к совершению преступления, есть сведения возможной связи преступниками с иными лицами.

2) сведений о преступнике нет, имеется информация о преступлении, есть сведения о выходе преступника на связь.

Для первой следственной ситуации, характерны обстоятельства, когда задержаны лица, причастные к совершению преступления (соучастники, члены банды) и они дают показания, исходя из которых, известны данные о личности преступника. Алгоритм действий следующий:

1. При допросе задержанного лица, выяснить каким образом поддерживалась связь, каким устройством и абонентским номером пользовался задержанный. Узнать максимально больше информации об образе жизни скрывающегося преступника, данные о личности, место проживания, круг общения, родственников, знакомых, с кем чаще всего общается, места, где может скрываться.

2. Если допрашиваемый готов сотрудничать со следствием, то необходимо попытаться сделать так, чтобы он связался с разыскиваемым преступником и

[110] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

назначил встречу. Затем осуществить его задержание. В ином случае алгоритм действий продолжается следующим образом.

3. Запросить детализацию вызовов задержанного, установить IMEI-код устройства, которым пользовался скрывающийся от следствия преступник.

4. Назначить контроль и запись переговоров по абонентским номерам лиц, с которыми может связаться преступник.

5. Поручить органу дознания осуществлять наблюдения за лицами, с которыми может встретиться разыскиваемый.

6. Провести проверку мест, где может скрываться преступник.

7. Организовать операцию по розыску и задержанию подозреваемого.

Вторая следственная ситуация может сложиться при обстоятельствах, когда преступники требуют выкуп при захвате заложника или похищении лица.

Алгоритм действий при этом следующий:

1. При допросе потерпевшего выяснить все обстоятельства преступления, когда было похищено лицо, где, в какое время и с кем находилось, на какой машине увезли, в каком направлении уехали преступники, сколько преступников было, выходили ли на связь, с какого номера при этом звонили, какие требования выдвигали, какие сроки установили для выполнения требований.

2. Организовать тактическую операцию по освобождению заложников.

3. Если при допросе установлен номер, с которого преступники связывались, то получить информацию о лицу, которому принадлежит и другие сведения.

4. Назначить контроль и запись переговоров по данному номеру или поручить органам дознания провести соответствующие оперативно-розыскные мероприятия.

5. Установить местонахождение данного абонента и действовать по плану тактической операции или специальной операции по освобождению заложников.

Приведем пример описываемой следственной ситуации. В апреле 2010 года неизвестные похитили ребенка семьи состоятельного предпринимателя А. и заявили требования о передачи крупной суммы денег. В противном случае,

угрожали убить девочку. Преступники звонили в течение нескольких дней, торопили со сбором денег, не давали послушать голос ребенка. После выяснения всех обстоятельств, незамедлительно была организована тактическая операция. Путем производства получения информации о соединениях между абонентами и (или) абонентскими устройствами были выявлены средства связи преступников, был определен участок местности, откуда чаще совершались звонки. В результате проведения контроля и записи телефонных переговоров были установлены лица, возможно, причастные к похищению. Органы расследования смогли предположить примерное местонахождение похищенного ребенка, так как технические возможности оператора связи позволили определить и уточнить расстояние от переговорщиков до ближайшей базовой станции оператора. В результате спецоперации преступники были задержаны, ребенок освобожден[111].

Ситуации, когда существует возможность установить предполагаемого преступника или преступную группу, путем производства получения информации о соединениях между абонентами и (или) абонентскими устройствами в отношении неопределенного круга лиц. Примером, может послужить уголовное дело по факту убийства гражданина США с признаками насильственной смерти. Труп был обнаружен в яме недостроенного гаражного бокса на окраине Орджоникидзовского района города Екатеринбурга. В ходе следствия было установлено, что данный гражданин прилетел в аэропорт Кольцово города Екатеринбурга, далее его местонахождение неизвестно. Отметим, что аэропорт Кольцово и район обнаружения трупа находятся на значительном расстоянии друг от друга. Следователем была получена информация о соединениях между абонентскими устройствами, которые работали в том и другом районе. Из огромного числа абонентов, было выделено всего четыре, которые были активны. В ходе дальнейшей проверки установлен один из участников банды, в общей сложности совершившей более 10 убийств[112].

---

[111] Уголовное дело № 55782-2011 г. // Архив ГСУ ГУ МВД России по Свердловской области.

[112] Архив отдела криминалистики Следственного управления СК РФ по Свердловской области. Уголовное дело № 30011233.

Такие ситуации характеризуются минимумом исходной информации о событии преступления и являются проблемными. Выделим типичные следственные ситуации:

1) обнаружен труп, информация о событии преступления отсутствует, преступники не установлены.

2) имеется заявление о пропаже лица, информации о преступлении отсутствует, труп не обнаружен.

3) имеется информация о преступлении, сведения о преступниках отсутствуют

Алгоритм действий в первой следственной ситуации можно представить следующим образом:

1. Провести осмотр места происшествия, установить личность трупа, обнаружить все возможные вещественные доказательства.

2. Допросить родственников, знакомых или иных лиц, с целью выяснить сведения о личности убитого, о его связях, роде деятельности, места проживания, мест пребывания, возможные конфликты, каким средством связи пользовался, абонентский номер.

3. Получить информацию о соединениях между абонентами и (или) абонентскими устройствами с целью установления последних соединений потерпевшего, последнего маршрута передвижения.

4. Проверить установленных абонентов на причастность к совершению преступления.

5. Установить абонентские устройства, которые были активны в районе места обнаружения трупа и районе последней абонентской активности потерпевшего. Выявить соответствия и проверить на причастность к совершению преступления установленных лиц.

Вторая следственная ситуация начинается с организации розыска пропавшего. В случае его обнаружения, необходимо установить были ли в отношении него совершены противоправные действия. Если да, то необходимо выяснить все обстоятельства случившегося и провести алгоритм действий по

поиску лиц, причастных к совершению преступления. В случае обнаружения трупа лица, по факту пропажи которого поступило заявление, выполнить алгоритм действий первой следственной ситуации.

Для разрешения третей следственной ситуации выполняется следующий алгоритм действий:

1. Осмотр места происшествия

2. Установить и допросить свидетелей и потерпевших с целью выяснения обстоятельств случившегося.

3. Получить информацию о соединениях между абонентами и (или) абонентскими устройствами в отношении неопределенного круга лиц.

4. Проверить всех установленных абонентов на причастность к совершению преступления.

Полагаем, что алгоритм действий в указанной следственной ситуации можно конкретизировать и наполнить иными следственными действиями и оперативно-розыскными мероприятиями, исходя из обстоятельств и вида преступления. Мы представили лишь примерный алгоритм действий, при котором целесообразно проведение получения информации о соединениях между абонентами и (или) абонентскими устройствами в отношении неопределенного круга лиц.

Перечень вышеперечисленных ситуаций расследования можно дополнить **ситуациями, когда осуществляется противодействие следствию, путем предоставления ложной информации, причем как со стороны подозреваемого (обвиняемого), так и со стороны потерпевшего**. Согласно данным анкетирования, такие ситуации нашли отражение в 61,2 % ответах следователей (дознавателей)[113]. Приведем пример такой следственной ситуации. П. привлекался к уголовной ответственности за покушение на сбыт наркотических веществ. Преступник прятал наркотические средства в тайниках, делал так называемые «закладки», после чего созванивался с покупателями и сообщал, где забирать «товар». Доказать вину П. было достаточно сложно, так как ни его самого, ни

[113] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

действий, им совершаемых, никто не видел. Поэтому важными изобличающими его вину доказательствами послужила детализация абонентский соединений с лицами, которым он сбывал наркотики[114]. А также **ситуации, когда на месте происшествия обнаружены абонентское устройство связи или модули SIM-карт.** Само по себе обнаружение сотового телефона на месте происшествия, представляет огромный интерес для следствия. Это возможность обнаружения материальных следов (отпечатки пальцев рук, биологические следы) и хранящаяся на устройстве информация. С помощью идентификационного кода IMEI, можно узнать о том, какие абонентские номера использовались в устройстве, кому принадлежал телефон и т.п.

На наш взгляд, в рамках данных ситуаций, невозможно определить конкретный перечень типичных следственных ситуации. Однако данные ситуации нередко возникают в процессе расследования по уголовным делам и не отметить их мы не могли. К тому же, совершенно очевидно, что в алгоритм действий следователя в данных ситуациях необходимо включение следственного действия, предусмотренного статей 186.1 УПК РФ, так как оно обладает высоким тактико-криминалистическим потенциалом и используется в целом ряде сфер, связанных с доказыванием: факта присутствия подозреваемых, обвиняемых в определенном месте, а равно маршрута их перемещения, имеющего значение для дела; наличия соучастников, характера их взаимоотношений, свидетелей и очевидцев; попыток сокрытия преступления, осуществления противодействия расследованию; многоэпизодного, серийного характера совершения преступлений.

Кроме вышеперечисленных ситуаций расследования и соответствующих каждой из них типичных следственных ситуации, мы можем выделить следственные ситуации, которые возникают именно в рамках конкретного

---

[114] Стельмах В. Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: монография / В.Ю. Стельмах. – Екатеринбург: Уральский юридический институт МВД России, 2014. С.40.

следственного действия, а именно, при производстве получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Так, при простой следственной ситуации, видится, что производство рассматриваемого нами следственного действия обусловлено определенными условиями и обстановкой, сложившейся на момент принятия решения о его производстве. При этом, не возникает проблем с получением судебного решения, сам процесс проведения следственного действия проходит согласно плана следователя, в рамках технического этапа получения интересующей информации от оператора сотовой связи не возникает трудностей и отсутствует конфликтность, т.е. конкретный сотрудник добросовестно выполняет работу по обработке и записи на электронный носитель необходимых данных, а организация связи своевременно предоставляет должным образом оформленную детализацию вызовов. Кроме того, результаты следственного действия проанализированы, обработаны и не вызывают у следователя сомнений в их достоверности. Предполагаем, что такая следственная ситуация может возникнуть в рамках расследования абсолютно любого уголовного дела, когда перед следователем нет никаких препятствий и не возникает трудностей в процессе получения информации о соединениях между абонентами и (или) абонентскими устройствами.

Однако, не следует исключать и случаи, когда в связи с комплексностью, сложностью и трудоемкостью проведения рассматриваемого следственного действия, возникает организационно-неупорядоченная ситуация. К примеру, когда оператором сотовой связи не предоставляется или несвоевременно предоставляется запрошенная следователем информация. Это может быть обусловлено техническими неполадками оборудования, халатностью или некомпетентностью сотрудников организации связи. Так, например, в ходе первого судебного процесса по делу Политковской сын потерпевшей заявил, что количество его звонков матери в день убийства различается с тем количеством,

которые отражены в данных оператора связи[115]. Выход из указанной конфликтной ситуации видится в налаживании психологического контакта с работниками организации связи или повторном получение интересующих сведений, что и последовало в ситуации при расследовании убийства Анны Политковской. Суд был вынужден сделать повторный запрос оператору, и звонки обнаружили, что было объяснено «техническими неполадками»[116].

Следует обратить внимание, что такие ситуации возникают не часто, и основаны, как правило, на несвоевременном предоставлении детализации. Исходя из данных анкетирования по вопросу, касающегося срока предоставления сведений от оператора связи, только 13,2% от числа опрошенных отметили, что операторы связи предоставляют запрашиваемую информацию с большими запозданиями лишь и 5,4%, что запрашиваемая информация предоставляется не по каждому уголовному делу[117].

Резюмируя вышесказанное, констатируем, что следственная ситуация представляет собой совокупность криминалистически значимых сведений, которыми владеет сам следователь на определенном этапе расследования преступления. При этом такие сведения носят внутренний, субъективный характер. Каждый следователь по разному подходит к исследованию следственной ситуации, одна и та же следственная ситуация для одного следователя видится простой, для другого – сложной. Это обусловлено личными и профессиональными качествами конкретного следователя, его компетенциями и опытом работы.

§ 2. Тактика производства получения информации о соединениях между абонентами и (или) абонентскими устройствами

Под криминалистической тактикой следует понимать систему теоретических положений и практических рекомендаций по организации и

---

[115] Маркин В. И.Самые громкие преступления XXI века в России / Владимир Маркин. – Москва: Издательство «Э», 2016. С. 93.
[116] Там же. С. 98.
[117] См.: Результаты изучения уголовных дел, связанных с использованием средств сотовой связи, в процессе раскрытия и расследования преступлений (Приложение 2).

планированию расследования оптимальной линии поведения лиц, осуществляющих расследовании, с учетом их отношений и взаимодействия с другими участниками расследования[118]. Основной задачей криминалистической тактики является эффективная организация криминалистической деятельности с учетом целей следственных действий, оперативно-розыскных и других мероприятий и всего процесса расследования, а также построение системы взаимодействия участников процесса.

Организация получения информации о соединениях между абонентами и (или) абонентскими устройствами представляет собой целый комплекс мер, подчиненных единому замыслу и общей цели. При его реализации могут быть задействованы не только органы предварительного расследования, но и другие участники уголовного судопроизводства: должностное лицо оператора связи, специалист экспертно-криминалистического подразделения, должностное лицо субъекта оперативно-розыскной деятельности, иные специалисты, компетентные в области связи.

Рассуждая о тактике получения биллинговой информации, следует обратить внимание на тот факт, что применение самого термина «тактика» в данном случае вызывает критику со стороны некоторых ученых и исследователей.

Так, Е.С. Лапин предлагает использовать термин «технология» применительно к данному следственному действию[119]. Аналогичной точки зрения придерживаются и другие ученые. Р.С. Белкин пишет, что «в условиях расследования о тактике в полном смысле следует говорить именно тогда, когда она служит средством преодоления оказываемого следователю противодействия», а «технология – наиболее целесообразный и эффективный способ осуществления неких трудовых операций в должной последовательности, когда исполнителю не оказывается противодействие»[120]. О.Я. Баев, утверждает, что «тактика как способ действий существует там и только там, где есть необходимость предупреждать и

---

[118] Яблоков Н. П. Криминалистика: учебник / Н. П. Яблоков. – Москва, 2005. – С. 395.
[119] Лапин Е.С. Указ соч. С. 110.
[120] Белкин Р.С. Курс криминалистики: Учебное пособие для вузов. – 3 изд., дополненное, М. 2001. С. 599.

(или) преодолевать непосредственное или опосредованное противодействие оптимальному достижению интересов в этих условиях субъекта»[121]. Е.Е. Центров делает акцент на то, что термин тактика применим в случае, когда имеет место «…соперничество или несовпадение интересов...»[122] и употребление этого термина возможно при осуществлении противодействия или противоборстве сторон.

На первый взгляд, использование вместо «тактики» термина «технология» относительно получения информации о соединениях между абонентами и (или) абонентскими устройствами достаточно справедливо и обоснованно. Однако, если обратиться к этимологическому значению слов то следует, что одно из значений термина «тактика» - это «совокупность методов и приемов, применяемых для достижения намеченной цели»[123], а это применимо для любого следственного действия. Технология – это «совокупность производственных методов и процессов в определенной отрасли производства, а также научное описание способов производства»[124]. Очевидно, что технология не вполне подходит в принципе к следственным действиям. К тому же, не умаляя авторитет исследователей, отметим что, если рассматривать тактику как совокупность приемов и способов достижения намеченной цели, то данный термин применим практически к любой деятельности, в том числе, где нет необходимости преодоления противодействия. На наш взгляд, термин «тактика», уже укоренился в криминалистической науке, и было бы нецелесообразно заменять его при изучении следственного действия, предусмотренного статьей 186.1 УПК РФ. К тому же, следует обратить внимание на тот факт, что Р.С. Белкин и О.Я. Баев,

---

[121] Баев О.Я. Основы криминалистики: курс лекций. 2-е изд.,перераб. и доп. М.: Экзамен, 2003. С. 200.

[122] Центров Е.Е. Особенности использования положений следственной тактики в правоприменительной деятельности // Криминалистика в системе правоприменения. Материалы конференции, 27–28 октября 2008 г., Москва, МГУ им. М.В. Ломоносова. М.,2008. С. 25 – 26.

[123] Ожегов С.И. Толковый словарь русского языка / С.И. Ожегов, Н.Ю. Шведова. – URL: http://slovarozhegova.ru/word.php?wordid=31378.

[124] Ожегов С.И. Толковый словарь русского языка / С.И. Ожегов, Н.Ю. Шведова. – URL: http://slovarozhegova.ru/word.php?wordid=31378.

говоря о «технологии» некоторых следственных действий, в своих трудах предпочитают употреблять термин «тактика».

Для уяснения криминалистической сущности получения информации о соединениях между абонентами и (или) абонентскими устройствами и тактического потенциала данного следственного действия важно рассмотреть его в структуре этапов, каждый из которых представляет собой относительно самостоятельный вид следственной деятельности.

По общему правилу тактика любого следственного действия представлена в виде трех этапов:

1) подготовительный;

2) основной (рабочий);

3) заключительный (оформление результатов следственного действия).

На каждом из них решаются конкретные задачи, выполнение которых необходимо для достижения соответствующего результата следственного действия.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами включает в себя следующие элементы:

- подготовку и изучение материалов уголовного дела;

- определение цели и задач проводимого следственного действия;

- уточнение организации связи, где зарегистрирован интересующий абонент или абонентское устройство;

- получение судебного решения на производство следственного действия и его дальнейшее направление оператору связи;

- получение и обособление необходимой информации должностным лицом оператора связи при исполнении запроса следователя;

- осмотр представленной информации о соединениях между абонентами и (или) абонентскими устройствами;

- оценка результатов следственного действия;

- приобщение полученной процессуальной информации в форме допустимой уголовно-процессуальным законом (протокол осмотра

представленной информации, вещественного доказательства или иного документа).

Перед тем, как рассмотреть вышеназванные элементы относительно наполненности этапов в структуре тактики получения информации о соединениях между абонентами и (или) абонентскими устройствами, следует указать, что немаловажным является момент принятия решения о его производстве. Данное следственное действие, технически сложное мероприятие, состоящее из целого ряда действий, к тому же проводится по судебному решению, так как затрагивает конституционные права граждан. В связи с этим, принимая решение, следователь должен определиться обоснованно ли ограничение прав и свобод человека, являются ли это соразмерным, пропорциональным и необходимым для реализации целей уголовного судопроизводства.

В процессе расследования следователь всегда стоит перед выбором наиболее эффективного следственного действия. Все решения принимаются с учетом тактических соображений, напрямую зависящих от конкретной следственной ситуации. Таким образом, принятие решения о производстве рассматриваемого следственного действия, обусловлено выводом следователя о том, что именно оно необходимо и оптимально в данной следственной ситуации и позволит получить, а затем использовать интересующие сведения.

Следует учесть, что база данных оператора сотовой связи постоянно обновляется, что свидетельствует о том, что срок хранения информации ограничен. Согласно действующему законодательству срок предоставления сведений об абонентах и (или) абонентских устройствах ограничен 3 годами[125], что обусловлено техническими возможностями оборудования организации связи. Кроме того, технические возможности также имеют значение, если решение о проведении названного следственного действия принимается с целью получения информации о местоположении абонентского устройства.

---

[125] О порядке оказания услуг телефонной связи: постановление правительства Российской Федерации от 9 декабря 2014 г. № 1342 г. Москва. – [Электронный ресурс]. − URL: http:// www.consultant.ru.

При анализе специальной технической литературы, мы находим, что на точность определения местоположения абонентского устройства, влияют не только уровень сигнала или особенности аппаратуры, но и погодные условия на момент осуществления абонентского соединения, особенности окружающего природного и индустриального ландшафта, «загруженность» близлежащих базовых станций связи и т.д.[126]. В связи с этим, анализируя биллинговые данные, следует иметь ввиду возможные погрешности. Хотя, очевидный, технический прогресс, развитие аппаратно-программных комплексов, позволяющих определить местоположение абонента, а также практика применения методов определения местоположения абонентских устройств, все же свидетельствуют о том, что информация, предоставляемая операторами сотовой связи, точная и позволяет решать следователю поставленные задачи.

Одним из важных факторов, влияющих на принятие решения о производстве следственного действия, предусмотренного статьей 186.1 УПК РФ, является неотложность его проведения в конкретной следственной ситуации. Так, например, по делам о хищении сотовых телефонов, если следователю известны IMEI-код, абонентский номер SIM-карты, данные о пользователе, и сомневаться в достоверности этих сведений нет оснований, то оперативное получение информации от оператора сотовой связи позволит быстро найти виновных и похищенное имущество. Аналогичная ситуация может возникнуть при противодействие расследованию, например, при даче ложных показаний, тогда принимая решение о производстве рассматриваемого следственного действия, следователь рассчитывает не только пополнить доказательственную базу, но и выбрать контраргументы для подавления противодействия, путем демонстрации сведений о соединениях или местоположении абонента.

Перечисляя факторы, обуславливающие принятие решения о производстве следственного действия, предусмотренного статьей 186.1 УПК РФ, отметим

---

[126] Сухов В.А. Повышение точности определения местоположения мобильных абонентских устройств в сетях IEEE 802.11G путем применения оптимальных алгоритмов обработки сигналов: дис. … канд. технич. наук. СПб.: Санкт-Петербургский государственный политехнический университет, 2012. С. 4.

основной – устранение недостатка информации на первоначальном этапе расследования. Наличие данного обстоятельства, при ситуациях, связанных с использованием средств сотовой связи, не оставляет поводов сомневаться при принятии решения о выборе следственного действия.

Тем не менее, приняв решение о производстве получения информации о соединениях между абонентами и (или) абонентскими устройствами, следователь в целях недопущения тактических и процессуальных ошибок должен приступить к тщательной подготовке к нему.

Подготовительный этап получения информации о соединениях между абонентами и (или) абонентскими устройствами условно можно разделить на две стадии (первая – изучение и систематизация необходимых материалов уголовного дела, вторая – подготовка постановления о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами).

Первая стадия действий проводится до вынесения постановления о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами. На этом этапе изучаются материалы уголовного дела, устанавливаются известные данные об абоненте или абонентском номере, при этом особенно важно как можно больше узнать о лице, чьи соединения будут проверяться. Уникальными идентификационными номерами, в зависимости от его вида, считаются: а) IMEI, то есть идентификационный номер самого устройства; б) номер SIM-карты. Названные идентификационные номера должны быть отражены в материалах уголовного дела до назначения следственного действия. Они могут фигурировать как в протоколе следственного действия, так и в иных процессуальных документах, например, объяснениях. Для принятия решения о возбуждении ходатайства о разрешении следственного действия не требуется обязательного «процессуального перезакрепления» указанной информации посредством следственных действий.

Следователь определяет цели и задачи, а также решает, целесообразно ли проведение следственного действия, прогнозируя возможные результаты. Научная

литература содержит тезис о том, что подготовка любого следственного действия начинается с постановки задач, подлежащих достижению [127]. Постановка конкретных задач рассматриваемого следственного действия напрямую зависит его цели – получение информации об абонентах, их соединениях или местоположении в определенный промежуток времени и месте. Перед следователем могут стоять следующие задачи:

- конкретизация информации о лице, совершившем преступление;

- установление личности других участников преступления и свидетелей;

- выявление организованной преступной группы;

- розыск лиц, причастных к совершению преступлений;

- установление местоположения и задержания подозреваемого;

- выявление мест хранения похищенного имущества, орудий и средств преступления;

- выявление средств и способов сокрытия следов преступления;

- выявление неблагоприятных обстоятельств для расследования (характера противодействия расследованию и др.);

- проверки алиби;

- выявление признаков инсценировки;

- выдвижение и проверка имеющихся версий, планирование расследования;

- использование процессуальной информации в рамках доказывания события преступления и использования ее ходе иных следственных действий[128].

Постановка задач и анализ ситуации является первым элементом подготовки к проведению любого следственного действия, в том числе и получения информации о соединениях между абонентами и (или) абонентскими устройствами. В этой связи дополним, что подбор и изучение материалов

[127] Белкин Р.С. Тактика следственного действия // Криминалистика. Учебник для вузов/ под ред. Б.А. Викторова и Р.С. Белкина. М., 1976. С. 226-229.

[128] Результаты анкетирования подтверждают, что все перечисленные тактические задачи в большей или меньшей степени решаются субъектами расследования. Самые распространенные задачи, которые ставят перед собой следователи (дознаватели): установление личности других участников преступления и свидетелей; установление местопребывания и задержание подозреваемого; розыск лиц, причастных к совершению преступления; выявление организованной преступной группы.

уголовного дела, сведений о лице, информацию о соединениях которого предполагается получить, представляют собой лишь часть аналитической деятельности следователя и носят в большей степени вспомогательный характер. Более того, рассмотрение этих операций, в отрыве от мыслительных, лишает их практического смысла. В реальных ситуациях эти операции неразделимые. Изучая материалы уголовного дела, следователь формирует, уточняет мысленную модель ситуации, выделяет в ней благоприятные и неблагоприятные условия. С учетом этого, прежде всего, ставятся задачи использования благоприятных и изменения неблагоприятных условий. На это обстоятельство указывал Р.С. Белкин, отмечая, что изучая материалы уголовного дела, следователь неминуемо сталкивается с проблемой моделирования и прогнозирования дальнейшего развития следственной ситуации[129].

К этому необходимо добавить, что оценка следственной ситуации не ограничивается только изучением материалов уголовного дела, следователь оценивает всю известную ему информацию, в том числе и не отраженную в документах, находящихся в деле. В частности, определенные сведения он может получить в процессе устного обмена информацией с работниками органов дознания, проводившими оперативно-розыскные мероприятия по делу или оказывавшими другие виды содействия расследованию. Возможно и мысленное обращение следователя к сохранившимся в памяти сведениям, полученным им в результате личного восприятия определенных фактов, материальных отражений, поведения и реакции отдельных лиц, в том числе субъектов, сведения о переговорах которых потребуется получить. Следует сказать, что оценка сложившейся ситуации не исчерпывается применением только анализа. Несомненно, это один из основных методов познания используемых на данном этапе, но далеко не единственный. Оценка условий реальной ситуации представляет собой информационно-познавательный процесс, осуществляемый

---

[129] Белкин Р.С. Курс криминалистики: Учебное пособие для вузов. – 3 изд., дополненное, М. 2001. С. 630.

при помощи совокупности методов познания: анализа, синтеза, моделирования, сравнения, наблюдения и т.д.

Действия второй стадии подготовительного этапа выполняются, когда становится известно о факте регистрации абонента у того или иного оператора связи. Данный факт устанавливается путем получения данных о персональной принадлежности, интересующих предварительное следствие, абонентских номеров (номеров абонентских устройств). Для их получения направляется письменный запрос на имя руководителя оператора связи (Приложение 3)[130][131]. Изложение фабулы уголовного дела в запросе не требуется. Следует отметить, что возможности интернета позволяют следователю установить принадлежность абонентского номера той или иной сотовой компании путем специальных сервисов в сети интернет, например, spravportal.ru или gsm-inform.ru. Таким образом, необходимость в составлении и направлении запроса всем операторам связи, действующим в регионе, отпадает, что полностью удовлетворяет принцип процессуальной экономии. Кроме того, следователь значительно облегчает себе задачу, так как на указанных выше сервисах просто задается интересующий абонентский номер, а программа выдает регион и оператора связи, которому он принадлежит.

На основании полученных от оператора связи данных следователь выносит постановление о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами и согласовывает данное постановление с руководителем следственного органа (Приложение 4)[132].

В постановлении указываются те моменты, которые необходимы для расследования уголовного дела, например, можно запросить:

- перечень входящих/исходящих вызовов;

---

[130] Образец письменного запроса оператору сотовой связи (Приложение 3).

[131] О персональных данных: федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.).

[132] Образец постановления о возбуждении перед судом ходатайства о получении информации о соединениях между абонентами и (или) абонентскими устройствами (Приложение 4).

- данные SIM-карты (сведения об абоненте);

- геолокацию абонентского устройства;

- идентификационный код IMEI;

- биллинговые данные.

С согласия руководителя следственного органа постановление направляется в суд и в случае принятия судом решения о получения информации о соединениях между абонентами и (или) абонентскими устройствами его копия направляется в соответствующую организацию связи. Руководитель организации связи, куда было направлено решение суда, обязан предоставить интересующую следователя информацию[133]. Кроме того, на этом же этапе следователь определяет, за какой период (прошлый или будущий, и за какой конкретно срок) необходима детализация соединений. Решение указанного вопроса в каждом случае индивидуально и должно обусловливаться обстоятельствами конкретного уголовного дела.

На этом же этапе следователь определяет, за какой период (прошлый или будущий, и за какой срок) необходима детализация соединений. Решение указанного вопроса в каждом случае индивидуально и должно обусловливаться обстоятельствами конкретного уголовного дела. Следует помнить, что операторы связи хранят анализируемую информацию в течение 3 лет[134].

На этапе подготовки рассматриваемого следственного действия, которое обращено в будущее, перспективного получения искомой информации, следователю необходимо помнить, что пассивного ожидания появления интересующей его информации быть не должно. Иными словами, нужно создавать благоприятные условия для получения информации о соединениях между абонентами и (или) абонентскими устройствами, когда лица будут стремиться установить связь между собой по телефону и информация о таких

---

[133] Уголовно-процессуальный кодекс Российской Федерации. ч. 3 ст. 186.1 (действующая редакция). – [Электронный ресурс]. − URL: http:/www.consultant.ru

[134] Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность: постановление правительства Российской Федерации от 27 августа 2005 г. № 538 (ред. от 10.04.2013) // Собрание законодательства Российской Федерации. 2005. – № 36 ст. 3704.

соединениях окажется имеющей значение для раскрытия и расследования преступления. Например, создание ситуации, при которой подозреваемый вынужден соединиться по телефону с лицом, связь с которым он отрицает, или в случае, когда он скрывает местонахождение предполагаемого соучастника. Способом создания данных тактических условий может быть допрос лица, в определенной форме и на такой предмет, после которого допрошенный нуждается в обмене информации с иными лицами, интересующими следствие.

Тактическими условиями получения перспективной биллинговой информации, имеющей значение для уголовного дела, являются наличие возможности и потребности у интересующих следствие (дознание) лиц контактировать посредством обращения к услугам, предоставляемым операторами связи. При этом у таких лиц - абонентов не должно возникать подозрения и тем более иметься сведений о том, что в отношении их телефонных и иных соединений в ходе расследования будет запрашиваться информация. Если лицу станет известно о начатом в отношении него следственном действии, то его проведение потеряет всякий смысл и начнется противодействие расследованию. Способами создания указанных тактических условий могут стать: допросы лиц, интересующих субъект деятельности по расследованию преступлений, на такой предмет, после которого допрошенные испытывают необходимость обменяться информацией; создание ситуации, при которой интересующие следствие (дознание) абоненты будут располагаться в отдаленных друг от друга местах, и когда электросвязь для них будет насущной потребностью; создание у этих абонентов ощущения, что расследование не будет вторгаться в сферу их частной жизни, не станет ограничивать их право на тайну телефонных и иных переговоров. Еще раз подчеркнем, что тактические условия, обеспечивающие результативность рассматриваемого следственного действия, имеющего перспективный характер, должны создаваться до вынесения постановления о разрешении получения информации о соединениях между абонентами и (или) абонентскими устройствами, на этапе подготовки к его осуществлению.

За тактическое правило, следует принять положение о сохранении в тайне факта проведения данного следственного действия от соответствующих участников предварительного расследования и иных лиц, чьи соединения попадают в поле зрения получаемой следствием детализации соединений абонентов. Однако, если лицо осведомлено о факте расследования преступления, например является подозреваемым (обвиняемым), то это не означает не проводить в отношении него рассматриваемое следственное действие перспективного характера. Как показывает практика, данное следственное действие оказывается эффективным даже после предъявления лицу в ходе допроса детализации его состоявшихся телефонных соединений. Это происходит по причине неосведомленности о возможности получения следствием не только информации о состоявшихся соединениях, но и о тех звонках, которые могут произойти в будущем.

Основной (рабочий) этап заключается как в деятельности следователя, так и должностного лица учреждения связи. Данный этап также можно представить в виде двух последовательных стадий: технической и исследовательской.

Первая стадия связана с проведением технических мероприятий. Среди них имеются подготовительные действия и операции, направленные на получение и фиксацию информации с помощью технических средств, однако следователь при этом не участвует. После получения организацией связи постановления и копии судебного решения от следователя на производство следственного действия, предусмотренного ст. 186.1 УПК РФ, сотрудник компании сотовой связи производит действия технического характера. На наш взгляд, следователь, не обладая специальными познаниями в соответствующей отрасли техники не должен вмешиваться в проведение этих мероприятий, однако, уголовно-процессуальный закон не запрещает ему присутствовать на данном этапе. По данным анкетирования лишь 12% (16 из 129) сотрудников ответили, что следователь присутствует при осуществлении оператором связи технических действий по получению интересующей информации[135]. Затем информация

[135] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

систематизируется и отправляется следователю в установленном порядке. В УПК РФ указано, что информация, поступающая от мобильного оператора может быть зафиксирована на любом материальном носителе, и предоставляется в опечатанном виде с сопроводительным письмо, в котором указывается период времени и номера абонентов или абонентских устройств[136]. Следует отметить, что интересующую следствие информацию предоставляет конкретный сотрудник организации связи, который осуществляет ее извлечение и копирование на внешний носитель, поэтому, не следует исключать человеческий фактор (халатность или ошибки при обработке данных), а также технические неполадки оборудования. В таком случае, если следователь располагает данными о недостоверности, представленных сведений, он может лично посетить офис оператора связи, объяснить противоречия данных и запросить новую информацию о соединениях абонента.

В рамках исследовательской стадии, следователь, получив сведения от оператора, проводит анализ и выборку интересующей информации, выполняет круг процессуальных действий, а также принимает некоторые тактические решения, касающиеся хода дальнейшего расследования. Согласно УПК РФ, полученные данные следователь осматривает в присутствии понятых, а при необходимости с участием специалиста. Случаи, когда необходимо участие специалиста определяет следователь. Целесообразно привлекать специалиста, если возникают сложности в систематизации сведений о соединениях между абонентами и (или) абонентскими устройствами, необходима дополнительная фиксация хода следственного действия или для консультации в рамках терминологии и разъяснении некоторых технических моментов для участников следственного действия. В качестве специалиста могут выступать работник компании оператора совой связи из числа инженерного персонала, владеющего методами позиционирования мобильных телефонов, специалист в области связи (представитель организации связи), специалист в области эксплуатации

---

[136] Уголовно-процессуальный кодекс Российской Федерации. ч. 3 ст. 186.1 (действующая редакция). [Электронный ресурс]. − URL: http:/www.consultant.ru.

конкретного вида абонентских устройств). При необходимости можно осуществить допрос специалиста на предмет того, какими услугами пользовался абонент, какие вызовы являются местными, междугородними, международными и т.п. Специалист в области связи может объяснить и показать места расположения базовых станций, по которым получена информация о местоположении абонентского устройства.

Как отмечает в своих исследования В.Ф. Васюков, «если осуществляющая услуги связи организация представила информацию в электронном виде (на диске), то следователь в присутствии понятых обрабатывает ее с помощью компьютера, что поэтапно фиксируется в протоколе осмотра. Для обработки кодированной информации или представляющей большой объем к осмотру следует привлекать специалистов в области программного обеспечения сетей сотовой связи»[137]. Л.Б. Краснова в одной из своих статьей указывает, что «при осмотре электронного носителя информации, содержащаяся в нем информация является основной целью данного действия, и он обязательно должен проводиться с участием специалиста»[138], под которым подразумевает специалиста по информационным технологиям. По данному мнению справедлива критика Е.С. Лапина, который указывает, что «такое правило приемлемо в отношении случаев обыска, выемки, осмотра, включая осмотр места происшествия, но не в случае, связанном с производством процессуального действия, предусмотренного ст. 186.1 УПК РФ»[139]. Действительно, следователь, руководствуясь личными навыками владения техникой, сам определяет в каком формате и на каком носителе ему будет представлена информация, следовательно, самостоятельно способен обработать полученные сведения. Решение об участии специалиста следователь принимает лично, если считает, что этого требует ситуация. Анализ

---

[137] Васюков В.Ф. Процессуальные особенности истребования информации об абонентских соединениях и абонентских устройствах при расследовании преступлений против личности. /В.Ф. Васюков // Наука и практика. – 2012. – № 3. – С.15-17.

[138] Краснова Л.Б. Электронные носители информации как вещественные доказательства // Известия Тульского государственного университета. Вып. 4. Ч. II. Юридические науки. Тула, 2013. С. 258.

[139] Лапин Е.С. Указ. соч. С. 124.

материалов следственной практики показывает, что прибегать к помощи специалиста рекомендуется, если возникают сложности в систематизации сведений о соединениях между абонентами и (или) абонентскими устройствами, если необходима дополнительная фиксация хода следственного действия или в целях консультации по разъяснению терминов и технических тонкостей.

Вышесказанное подтверждают результаты опроса. При анкетировании практических сотрудников, по поводу участия специалиста разделились следующим образом: 33,3% указали, что участие специалиста не требуется, 30,2% - необходим специалист для фиксации хода следственного действия, 27,9% - требуется помощь специалиста (сотрудника компании сотовой связи) для консультации по представленной информации[140]. Также, в одной из работ Ю.Н. Соколова мы находим пример, участия специалиста в области связи при осмотре полученной детализации. Следователю оказывал содействие сотрудник Екатеринбургского филиала ОАО «МТС» «Макро-регион Урал», который пояснил некоторые условные обозначения, используемые для идентификации имеющейся информации о соединениях между абонентами и (или) абонентскими устройствами применительно к секторам местности станций сотовой компании[141].

На заключительном этапе следственного действия составляется протокол осмотра документов, в котором, по мнению следователя, указывается наиболее значимая информация для уголовного дела (Приложение 5)[142], а также выносится постановление о признании и приобщении к уголовному делу электронного носителя информации. Протокол осмотра документа может быть составлен непосредственного после обработки всего массива предоставленной информации либо по ходу исследования.

Отметим, что в УПК РФ одним из видов самостоятельного следственного действия (следственного осмотра) предусмотрен осмотр предметов и документов. В связи с этим, добавим, что, если информация об указанных соединениях была

---

[140] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).
[141] Соколов Ю.Н. Использование биллинговой информации в уголовном процессе: учебное пособие. Екатеринбург, 2012. С. 132 – 133.
[142] Образец протокола осмотра предмета (документа). Приложение 5.

получена путем производства выемки, то следователь осуществляет ее дальнейшее визуальное обследование в рамках самостоятельного следственного действия – осмотра документов, руководствуясь положениями не ч. 5 ст. 186.1 УПК РФ, а ст. 176, 177, ч. 2 ст. 180 УПК РФ, а также нормами, регулирующими общие условия производства следственных действий: ст. 164, 166, 170 УПК РФ.

Независимо от процессуальной формы осуществления осмотра электронного носителя, его визуальное обследование осуществляется по правилам осмотра документов, разработанным в недрах криминалистической техники. Осматривая документ либо иной материальный носитель информации, следователь должен указать дословно ту часть информации, которая, по его мнению, имеет отношение к уголовному делу. К таковой информации законодатель в ч. 5 ст. 186.1 УПК РФ вполне относит следующие данные: дата, время, продолжительность соединений между абонентами и (или) абонентскими устройствами, номера абонентов и т.д.

Но при внешнем сходстве тактико-криминалистических приемов, в случае реализации положений ст.ст. 176, 177, ч. 2 ст. 180 УПК РФ применяется иная процессуальная форма. Следовательно, в целом при едином порядке производства осмотра документа, содержащего информацию о соединениях между абонентами и (или) абонентскими устройствами как части следственного действия, предусмотренного ст. 186.1 УПК РФ, и осмотра документов как самостоятельного следственного действия, предусмотренного ст.ст. 176, 177, 180 УПК РФ, есть некоторые нюансы различия.

Например, это различие касается участия понятых. Действующая редакция ст. 170 УПК РФ, устанавливающая случаи участия понятых при производстве следственных действий, по общему правилу, не предусматривает необходимость их участия при осмотре материального носителя информации о соединениях в рамках ч. 5 ст. 186.1 УПК РФ. Но законодатель допускает возможность участия понятых при производстве любого, в т.ч. и данного следственного действия, при наличии ходатайства участников уголовного судопроизводства либо собственной инициативы следователя (ч. 2 ст. 170 УПК РФ). Полагаем, что по смыслу ч. 2 ст.

170 УПК РФ имеются в виду ситуации, когда следователь, руководствуясь общими положениями о производстве следственных действий, производит следственное действие с участием приглашенных им по своей инициативе иных участников (специалиста, владельца абонентского устройства), и именно эти лица заявляют ходатайство об участии понятых. Думается, что вряд ли законодатель имел в виду возможность учета ходатайства любых участников процесса, не участвующих в данном следственном действии, но проходящих по уголовному делу, поскольку это неоправданно усложнило бы процесс расследования.

В случае производства осмотра в рамках ч. 5 ст. 186.1 УПК РФ без понятых законодатель не возлагает на следователя обязанности использовать технические средства фиксации хода и результатов следственного действия. Вместе с тем, полагаем, что в целях обеспечения высокой достоверности данного доказательства применение технических средств фиксации его хода и результатов является желательным.

Несколько иная ситуация с участием понятых при осмотре материального носителя информации в порядке ст.ст. 176, 177, 180 УПК РФ. Согласно ч. 1.1 ст. 170 УПК РФ при производстве следственного действия, предусмотренного ст. 177 (порядок производства осмотра), понятые принимают участие по усмотрению следователя. Но если по решению следователя понятые не участвуют в указанном следственном действии, то следователь обязан применять технические средства фиксации хода и результатов следственного действия.

Существуют и иные отличительные признаки. Так, если в рамках ч. 6 ст. 186.1 УПК РФ осмотренный носитель информации должен быть приобщен к уголовному делу и опечатан, после чего храниться при уголовном деле как вещественное доказательство, то в случае производства осмотра в порядке ст.ст. 176, 177, 180 УПК РФ законодатель допускает, но не требует обязательного опечатывания этого документа.

Подобные нюансы различия в двух возможных режимах осмотра носителя информации о соединениях между абонентами и (или) абонентскими устройствами, к сожалению, не всегда точно учитываются на практике. Субъекты

уголовного судопроизводства порой смешивают указанные режимы производства двух сходных следственных действий, что, на наш взгляд, недопустимо, а потому должно быть постепенно нейтрализовано, в том числе и посредством дальнейших исследований данной проблемы и выработки действенных методических рекомендаций.

После составления протокола осмотра документа, следователь выносит постановление о признании и приобщении к уголовному делу электронного носителя информации. Данный процессуальный документ и будет являться итоговым, завершающим рассматриваемое следственное действие. Изученные материалы приобщаются в полном объеме на основании постановления следователя и хранятся в опечатанном виде в условиях, исключающих возможность ознакомления с ними посторонних лиц и обеспечивающих их сохранность.

Выделив три основных этапа и соответствующие им стадии в тактике получения информации о соединениях между абонентами и (или) абонентскими устройствами мы подчеркнули комплексность рассматриваемого следственного действия. Казалось бы, что следователь при производстве получения информации о соединениях между абонентами и (или) абонентскими устройствами присутствует «на входе и на выходе» следственного действия, своего рода отсутствует рабочий этап, однако это не так. При производстве следственного действия, осуществляется целый комплекс мероприятий. Исходя из структуры тактики рассматриваемого следственного действия, следует, что оно содержит в себе признаки нескольких следственных действий, а при его производстве последовательно выполняются несколько относительно самостоятельных процессуальных действий: получение сведений, осмотр, анализ информации и закрепление в качестве вещественного доказательства.

Понятие комплексности впервые было затронуто С.Б. Россинским. Автор говорит, что законодатель предусматривает наличие уголовно-процессуальных

мероприятий комплексного характера – процессуальных комбинаций[143], а затем поясняет, что «комплексное следственное действие (процессуальная комбинация) – это предусмотренный уголовно-процессуальным законодательством комплекс определенных взаимообусловленных следственных и иных процессуальных действий, направленных на решение частных (локальных) задач уголовного судопроизводства и производимых на основании общего процессуального решения»[144]. Исходя из логики автора, следует, что процессуальные комбинации позволяют сочетать не только отдельные процессуальные действия в рамках одного следственного действия, но и целый комплекс взаимообусловленных следственных действий с иными процессуальными действиями. Соответственно, в данном контексте комплексность не находит отражения в следственном действии, предусмотренном ст. 186.1 УПК РФ. Некоторые авторы называют комплексными такие следственные действия, которые характеризуются сочетанием признаков нескольких следственных действий[145]. Например, наложение ареста на почтово-телеграфные отправления сочетает в себе наложение ареста на них, выемку данных отправлений и их осмотр. Также существует точка зрения о том, что комплексные – это такие следственные действия, состоящие из действий нескольких участников[146], что по нашему мнению не совсем точно, так как при производстве всех следственных действий могут присутствовать несколько участников и данный признак не будет отличительной чертой комплексного следственного действия.

Мы считаем, что комплексность представляет собой выполнение всех этапов и стадий, представленных в виде самостоятельных, но неразрывно связанных действий, в рамках одного следственного действия в едином комплексе. В связи с этим, следует согласиться с утверждением о том, что «…следственные действия,

---

[143] Россинский С.Б. Уголовный процесс России: курс лекций / С.Б. Россинский. – 2-е изд., исправл. и доп. – М.: Эксмо, 2008. – С. 297.
[144] Там же. С. 300.
[145] Криминалистика: учебник / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. – 3-е изд., перераб. и доп. – Москва: Норма, 2008. С. 599-600.
[146] Железняк А.С. Криминалистика: тактико-методические основы уголовного судопроизводства (досудебная стадия): учеб. пособие / А. С. Железняк. – Москва: МГИУ, 2007. – С. 38.

состоящие из серии самостоятельных процессуальных действий, которые в силу прямого указания закона должны выполняться обязательно и в строго определенной последовательности, составляя в итоге единый процессуальный комплекс, будут являться комплексными»[147]. Также отметим, что в УПК РФ нет никаких указаний ни на комплексные следственные действия, ни на процессуальные комбинации. Хотя, по аналогии с выделенными нами этапами в структуре тактики получения информации о соединениях между абонентами и (или) абонентскими устройствами комплексными следует признать, например: наложение ареста, осмотр и выемку почтово-телеграфных отправлений, контроль и запись переговоров, что требует отдельного исследования.

В силу требований ст. 186.1 УПК РФ, получение информации о соединениях между абонентами и (или) абонентскими устройствами включает следующий комплекс действий следователя:

1) получение следователем судебного разрешения;

2) направление его оператору связи;

3) систематизация работниками оператора связи соответствующих соединений и предоставление списка соединений (детализации) следователю;

4) осмотр детализации;

3) оценка и приобщение ее к материалам уголовного дела в качестве вещественного доказательства.

Мы полностью разделяем мнение В.Ю. Стельмаха, который указывает, что «следственное действие, предусмотренное ст. 186.1 УПК РФ является комплексным, представляя собой единый процессуальный комплекс, включающий в себя три самостоятельных действия (само получение информации, осмотр носителя с информацией и принятие решения о приобщении в качестве

---

[147] Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: монография / В.Ю. Стельмах. – Екатеринбург: Уральский юридический институт МВД России, 2014. – С. 42-43.

вещественного доказательства), которые должны производиться в обязательном порядке в последовательности, указанной в законе»[148].

На наш взгляд, именно из-за сложности (комплексности) структуры данного следственного действия и возникли непонимание и споры среди исследователей о тактике получения информации о соединениях между абонентами и (или) абонентскими устройствами. Рассматриваемое следственное действие представляет собой единый процессуальный комплекс, включающий в себя несколько самостоятельных действий, которые должны производиться в обязательном порядке в той последовательности, какая указана в законе. Мы считаем, что выделение группы сложных (комплексных) следственных действий имеет практическое значение и состоит в обеспечении лучшего понимания их правовой природы, когда они рассматриваются как единый процессуальный комплекс, а не как механический набор самостоятельных и независимых друг от друга действий, производимых по усмотрению следователя в зависимости от конкретной ситуации, складывающейся при расследовании уголовного дела. Кроме того, соблюдение определенной тактики производства получения информации о соединениях между абонентами и (или) абонентскими устройствами позволяет правоприменителю решить поставленные задачи.

Криминалистическая тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами ныне лишь постепенно нарабатывается. И в этой связи весьма важно обеспечить следователей криминалистическими рекомендациями по эффективному производству данного следственного действия, минимизации потенциально конфликтных ситуаций расследования. Полагаем, что постепенная систематизация эмпирической практики и выработанных тактико-криминалистических рекомендаций со временем может послужить добротным источником для дальнейшей оптимизации положений ст. 186.1 УПК РФ.

---

[148] Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: монография / В. Ю. Стельмах. – Екатеринбург: Уральский юридический институт МВД России, 2014. – С. 44.

§ 3. Получение информации о соединениях между абонентами и (или) абонентскими устройствами в структуре тактических операций

Практика правоохранительных органов и проведенные на ее основе исследования свидетельствуют о малоэффективности производства отдельно взятых следственных действий в конфликтных ситуациях, для которых характерны недостаток информации, а также противоборство сторон. Повышению результативности следственных действий способствует их производство в системе тактических операций.

В научной литературе нет единой точки зрения по поводу понятия тактической операции, хотя проблемы связанные с ним исследуются достаточно давно.

Термин «тактическая операция» впервые был использован в публикации А.В. Дулова «О разработке тактических операций при расследовании преступлений»[149]. Автор рассматривал ее как средство решения общих задач предварительного расследования путем производства групп следственных действий в сочетании с оперативно-розыскными и ревизионными мероприятиями[150]. Данного мнения придерживаются А.В. Шиканов, М.В. Савельева, А.Б. Смушкин и др.[151]. Например, А.В. Шиканов определяет тактическую операцию как «систему согласованных между собой следственных, оперативно-розыскных мероприятий и иных действий, предпринятых в полном соответствии с требованиями норм уголовно-процессуального закона правомочными должностными лицами для выяснения вопросов, входящих в

---

[149] Дулов А.В. О разработке тактических операций при расследовании преступлений // 50 лет советской прокуратуры и проблемы совершенствования предварительного следствия. М., 1973. С. 23 - 24.

[150] Там же. С. 26.

[151] Савельева М.В. Теория и практика использование фактора внезапности в уголовном судопроизводстве: дис. .. канд. юрид. наук. Саратов, 2003. С. 227. Смушкин А.Б. Задержание в структуре тактической операции при расследовании преступлений: дис. .. канд. юрид. наук. Саратов, 2005. С. 243. Шиканов В.И. Разработка теории тактических операций – важнейшее условие совершенствование методики расследования преступлений // Методика расследования преступлений (общие положения): материалы науч.-практ. Конф. М., 1976. С. 156-157.

предмет доказывания по расследуемому уголовного делу[152]. При этом Л.Я. Драпкин, Р.С. Белкин высказывают мнение о том, что вышеуказанное понятие больше относиться к категории тактической комбинации[153].

По мнению А.С. Фоминой тактическая операция – это обусловленная следственной ситуацией и поставленной тактической задачей динамическая система следственных действий, оперативно-розыскных и иных мероприятий, без которых достижение определенной локальной цели расследования невозможно или нерационально[154].

Интерес вызывает точка зрения И.М. Комарова, который понимает под тактической операцией «обусловленный ситуациями расследования метод познания практической деятельности субъекта доказывания, используемый при решении системных задач досудебного производства»[155]. Кроме того, автор именует тактическую операцию криминалистической, а также говорит, что ее суть заключается в полифункциональном способе информационно-познавательной деятельности субъекта доказывания. Хотя очевидно, что тактические операции уполномочены проводить только следователи и дознаватели. Весьма сомнительно использование тактической операции как метода познания, так как тактическая операция представляет собой самостоятельное структурированное средство достижения определенной цели, а метод – это, прежде всего совокупность приемов и правил, сопровождающих переход от незнания к знанию.

В рамках настоящего исследования, мы предлагаем использовать, определение, данное Л.Я. Драпкиным, понимает тактическую операцию как «комплекс взаимосвязанных следственных, оперативно-розыскных,

---

[152] Шиканов В.И. Теоретические основы тактической операции в расследовании преступлений: дис. … канд. юрид. наук / В.И. Шиканов. – Иркутск, 1983. С. 114.

[153] Драпкин Л.Я. Особенности информационного поиска в процессе расследования и тактика следствия // Проблемы повышения эффективности предварительного следствия: тез. науч. конф. Л., 1976. С. 54. Криминалистика: учебник / под ред. Р.С. Белкина. М.: НОРМА – ИНФРА – М, 1999. С. 990.

[154] Фомина А.С. Основные тактические операции при расследовании серийных убийств: автореф. дис. ... канд. юрид. наук. Воронеж, 2003. – С. 15.

[155] Комаров И.М. Основы частной теории криминалистических операций досудебного производства: монография / И.М. Комаров. – Москва: Юрлитинформ, 2010. – С. 78.

организационно-подготовительных, ревизионно-проверочных, иных действий и приемов, проводимых в сравнительно сжатые сроки, по единому плану, с учетом следственной ситуации и направленных на решение важных промежуточных задач»[156]. На наш взгляд, данное понятие, являясь наиболее полным, отражает сущность и значение тактических операций не только для криминалистической науки, но и правоприменительной деятельности следователя по расследованию и раскрытию преступлений.

Самыми распространенными видами тактических операций считаются: розыск и задержание подозреваемого; изобличение лиц, причастных к совершению преступления; преследование преступника «по горячим следам»; задержание с поличным; поиск и фиксация доказательств на месте происшествия и т.д. Вышеперечисленные операции можно классифицировать по нескольким основаниям: по содержанию, по временной и организационной структуре, по ведомственной принадлежности[157]. Исходя из позиции Л.Я. Драпкина, следует, что все тактические операции имеют цель, путем достижения которой решаются промежуточные задачи расследования. При этом определенные следователем цели и соответствующие им задачи напрямую зависят от конкретных обстоятельств и условий сложившейся следственной ситуации.

Тактическая операция как криминалистическая категория изучается достаточно продолжительное время, но единого мнения по ее структуре так и не сложилось. Интересной представляется структура, которую предложил А.В. Дулов. Автор указал, что структура тактической операции состоит из цели (задачи), условий, средств, субъекта и объекта. В связи с чем, говоря о тактической операции, где в качестве центрального звена выступает получение информации о соединениях между абонентами и (или) абонентскими устройствами, необходимо рассмотреть каждый элемент ее структуры отдельно.

---

[156] Драпкин Л.Я., Долинин В.Н. Тактика следственных действий: учебно-практическое пособие. – Екатеринбург: издательский дом Уральского государственного университета, 2015. – С. 11.

[157] Криминалистика: учебник для бакалавров / под ред. Л.Я. Драпкин. – М.: Издательство Юрайт, 2013. – С. 401.

Цель тактической операции, в основе которой лежит получение информации о соединениях между абонентами и (или) абонентскими устройствами может быть разной в зависимости от того, какое значение представляют для уголовного дела сведения об абонентах. Биллинговая информация может иметь основополагающее значение, т.е. выступать в качестве доказательства или носить ориентирующий характер, т.е. создавать условия для выбора дальнейших действий следователем. Тактическая операция с использованием данного следственного действия проводится для получения новых сведений об уже известном факте соединения абонентских устройств и личности, фактического пользователя устройства связи либо обнаружения еще неустановленных устройств, с которыми зафиксировано соединение.

Условиями таких тактических операций являются конкретные следственные ситуации, сложившиеся на данный момент расследования. Опять же здесь идет речь о таких аспектах как необходимость подтверждения каких-либо сведений, ставших уже известными или напротив необходимо установить абонента, местонахождение устройства и т.п.

Субъектами тактической операции по получению информации о соединениях между абонентами и (или) абонентскими устройствами являются следователь, представитель организации связи и иные должностные лица, взаимодействующие с ним. Взаимодействие с оператором сотовой связи предполагается исходя из правовой сущности следственного действия, предусмотренного ст. 186.1 УПК РФ, а взаимодействие с другими должностными лицами зависит от необходимости содействия следователю.

Объектом анализируемых тактических операций может выступать как подозреваемый, потерпевший, так и неустановленное лицо (предполагаемый преступник, лицо, причастное к совершению преступления или иное лицо).

Средства тактической операции в научной криминалистической литературе понимаются по-разному. Одни ученые считают, что круг средств тактической операции ограничен следственными действиями и организационно-техническими

мероприятиями с целью решения конкретной задачи[158]. Другие добавляют к ним оперативно-розыскные мероприятия и ревизионные действия[159]. Третьи полагают, что средства тактической операции - это система следственных и иных процессуальных и не процессуальных действий, а так же тактических приемов и средств[160]. Кроме того, в уголовно-процессуальном законодательстве предусмотрены следственные, иные процессуальные и оперативно-розыскные действия. Остальные средства применяемые следователем и субъектами тактической операции можно назвать иными[161]. Отметим, что тактические приемы являются самостоятельными средствами тактической операции, поскольку следственные действия являются формой реализации тактико-криминалистических средств, к которым и относиться тактический прием.

Резюмируя, можно говорить о том, что к средствам тактической операции относятся следственные, иные процессуальные, оперативно-розыскные и иные действия, а так же тактические приемы. В структуре тактических операций, получение информации о соединениях между абонентами и (или) абонентскими устройствами выступает в качестве средства, путем использования которого достигается решение задач.

Одним из наиболее значимых признаков тактической операции является системность. Данный признак обеспечивается проведением тактических операций

---

[158] Гармаев Ю.П. Раскрытие и расследование должностных преступлений, совершенных работниками таможенных органов (методическое пособие). Иркутск, 1998. С. 93; Криминалистика: учебник / под ред. А.Г. Филиппова. М., 2000. С. 184.

[159] Драпкин Л.Я. Особенности информационного поиска в процессе расследования и тактика следствия // Проблемы повышения эффективности предварительного следствия. Л., 1976. С. 54; Дулов А.В. Тактические операции при расследовании преступлений / А.В. Дулов. – Минск: Издательство БГУ, 1979. – С. 44; Михальчук А.Е. Тактические комбинации при производстве следственных действий: монография / А.Е. Михальчук. – Саратов: Издательство Саратовского университета, 1991 С. 19.

[160] Шиканов В.И. Теоретические основы тактической операции в расследовании преступлений: дис. … канд. юрид. наук. – Иркутск, 1983.. С. 20; Комаров И.М. Проблемы теории и практики криминалистических операций в досудебном производстве: дис. ... д-ра юрид. наук. – Барнаул, 2003. С. 163.

[161] Прыткова Е.В. Обеспечение безопасности подозреваемого (обвиняемого), заключившего досудебное соглашение о сотрудничестве, на стадии предварительного расследования: Тактические аспекты.: дис. канд. юрид. наук. Барнаул, 2015. С. 197.

по единому плану. Хотя необходимо также учитывать, что уровень планирования обуславливается исходя из условий конкретной следственной ситуации, где в качестве немаловажных факторов выступают качество информации об искомых объектах, об известных обстоятельствах, данные о личности и т.д. Системность и последовательность действий отмечается В.И. Шикановым, который сформулировал основы тактических операций и среди основных их признаков отметил алгоритмичность образующих их действий[162]. Однако некоторые ученые выступили с критикой в отношении такой точки зрения. Так, И.Ф. Герасимов полагал, что такое понимание лишает тактические операции индивидуальности и занижает значение уникальных факторов конкретных следственных ситуаций[163]. На наш взгляд, критика не совсем обоснованна, так как вся следственная деятельность алгоритмична. Это обусловлено предписаниями закона об основаниях и порядке проведения следственных действий и иных процессуальных мероприятий, а также повторяющимися условиями типичных следственных ситуации и вытекающих из них задач расследования, решаемых путем применения сходных методов, приемов и средств.

Тактические операции действительно носят характер алгоритмов, а соответственно содержат в себе такой признак, как взаимосвязанность и согласованность всех элементов. Согласованность как признак тактической операции означает, что выполнение определенных составляющих и достижение того или иного результата, влечет за собой возможность или невозможность последующих действий, а также определяет целесообразность дальнейших мероприятий, влияющих на конечный результат.

Как и любая другая деятельность, тактические операции могут быть направлены на изменения неблагоприятных условий расследования или сохранение благоприятных и проводятся в условиях сложных, проблемных,

---

[162] Шиканов В.И. Разработка теории тактических операций – важнейшее условие совершенствование методики расследования преступлений / В.И. Шиканов // Методика расследования преступлений (общие положения): материалы научно-практической конференции. – Москва, 1976. –. С. 17 - 21.

[163] Герасимов И.Ф. Тактическая операция как форма взаимодействия органов предварительного расследования // Тактические операции и эффективность расследования. Свердловск, 1986.

конфликтных или смешанных ситуаций, и поэтому, прежде всего, направлены на преодоление имеющихся трудностей.

В проблемных и проблемно-конфликтных ситуациях целью тактических операций является преодоление неполноты и неопределенности имеющейся релевантной информации. В связи с этим цели тактических операций можно в наиболее общем виде представить, как восполнение информационной неполноты и ликвидация или уменьшение до допустимых пределов ее неопределенности. Сокращение имеющегося дефицита данных в ходе расследования может быть достигнуто посредством получения новых сведений из уже известных или еще неустановленных источников.

Известно, что любые переговоры или переписка предполагают наличие минимум двух участников, хотя следует учитывать, что современные технические средства связи допускают одновременное общение 10 и более устройств, например, конференц-связь. Таким образом, на момент планирования получения информации о соединениях между абонентами и (или) абонентскими устройствами может быть известен либо только один, либо двое и более участников. Чаще всего на стадии планирования известен только один субъект телефонных соединений, и он не всегда обладает необходимой информацией или намеренно ее скрывает. В связи с этим, отметим ситуации, формирующиеся на момент принятия решения о производстве тактической операции с использованием получения информации о соединениях между абонентами и (или) абонентскими устройствами. Прежде всего, это ситуации, характеризующиеся неполнотой сведений об участниках, их местонахождении, времени и обстоятельствах расследуемого события. Это также ситуации, когда показания известных участников события требуют подтверждения, путем получения информации абонентах или абонентских устройствах от оператора сотовой связи. Таким образом, следственное действие, предусмотренное ст. 186.1 УПК РФ в совокупности с другими процессуальными, оперативно-розыскными и организационно-подготовительными мероприятиями является единственным и наиболее рациональным средством восполнения дефицита информации. В

подобных ситуациях также могут быть достоверно известны носители искомой информации, однако они тщательно скрывают свою осведомленность и отрицают факт связи с другими лицами, причастными к совершению преступления. Подобные ситуации возникают при расследовании преступлений, совершенных группами, члены которых препятствуют установлению других участников, их роли и возможного нахождения. Получение информации о соединениях между абонентами и (или) абонентскими устройствами позволят установить факт соединений с предполагаемыми соучастниками, время, продолжительность и частоту, вызовов. Кроме того, можно получить достоверную информацию о постоянном местонахождении или определить места, откуда чаще всего совершались звонки, и во взаимодействии с сотрудниками оперативных подразделений выявить лиц, скрывающих от следствия.

Практике известны ситуации, когда преступниками, посредством абонентских устройств поддерживается связь с потерпевшим или свидетелем. Такие ситуации возникают, когда неизвестные угрожают, высказывают требования, присылают сообщения, побуждающие к определенным действиям и т.п. Угрозы чаще всего высказываются в адрес свидетелей, потерпевших, подозреваемых, содействующих следствию и дающих правдивые показания об обстоятельствах. Такие следственные ситуации требуют проведения тактической операции по установлению участников преступления и их изобличению. Казалось бы, что в рассматриваемых ситуациях, наиболее полную, интересующую следствие информацию можно получить путем включения в тактическую операцию контроля и записи переговоров. Действительно, контроль и запись переговоров достаточно эффективное следственное действия и, несомненно, с его помощью пополняется доказательственная база по уголовному, но оно достаточно трудоемкое и требует основательной подготовки. Кроме того, контроль и запись переговоров позволяет узнать информацию, содержащуюся в телефонных переговорах, которые только будут совершены, что значительно его ограничивает. Во многих ситуациях время не позволяет ждать, когда случится очередной разговор между интересующими субъектами, поэтому необходимо искать

альтернативу, которая позволит установить и изобличить виновных, а также дополнить «копилку» доказательственной и иной значимой информации. Поэтому в ряде случаев справедливо изначально включать в тактическую операцию получение информации о соединениях между абонентами и (или) абонентскими устройствами, а затем, учитывая результаты возможно и производство контроля и записи переговоров.

Для установления практического значения производства получения информации о соединениях между абонентами и (или) абонентскими устройствами необходимо рассмотреть его роль в структуре наиболее распространенных тактических операций, к которым отнесем **операции по установлению лиц, причастных к совершению преступления, по изобличению подозреваемых, обвиняемых, проверку алиби лица, проверку признательных показаний подозреваемого, обвиняемого и других лиц.**

Тактическая операция по установлению лиц, причастных к совершению преступления, является одной из самых распространенных в правоохранительной практике. Содержание такой операции включает в себя следующий набор действий: рассмотрение известных данных о личности предполагаемого преступника и потерпевшего, изучение и анализ оперативной обстановки и материалов уголовного дела, выдвижение версий, розыск и задержание подозреваемого, производство неотложных следственных действий, обращение к данным оперативных и криминалистических учетов.

Отметим, что тактическая операция представляет собой комплекс взаимосвязанных мероприятий, а не просто набор определенных действий. Соответственно, каждое последующее действие, зависит от тактики, порядка и результативности предыдущего.

Получение информации о соединениях между абонентами и (или) абонентскими устройствами включается в структуру тактической операции по выявлению лиц, причастных к совершению преступлений не только в тех случаях, когда преступное деяние продолжается, но и когда имеет место оконченное преступление. В обоих случаях важно знать, что преступник будет поддерживать

связь с сообщниками. Путем производства указанного следственного действия станет известен круг абонентских номеров, с которыми связывался подозреваемый. По установлению необходимых сведений об интересующих абонентских номерах, можно определить круг предполагаемых лиц, причастных к расследуемому преступлению. Дальнейшим действием будет установление их местонахождения и задержание. Подобные тактические операции применимы при расследовании уголовных дел о похищении человека, захвате заложников, заведомо ложном сообщении о террористическом акте, вымогательстве и других преступлениях, когда неизвестные ведут переговоры с помощью средств сотовой связи. Преступник осуществляет звонок с мобильного телефона, сообщает информацию о готовящихся взрыве, поджоге или иных действиях, создающих угрозу безопасности общества, а в базе оператора сотовой связи остаются не только сведения об используемом устройстве (идентификационный код IMEI и данные SIM-карты), но и биллинговые значения, которые позволяют определить его местонахождение.

Рассматриваемые ситуации можно конкретизировать и разделить на две группы: когда местонахождение предполагаемых преступников неизвестно или когда известно место их пребывания, но отсутствуют сведения о личности. Добавим, что при подготовке преступники подбирают средства связи, не принадлежащие им (украденные, купленные с рук, без документов и т.п.), а также SIM-карты, оформленные на других лиц. Очевидно, что не во всех случаях следователь располагает верными и актуальными данными о личности преступника. Поэтому в таких ситуациях в первую очередь необходимо руководствоваться географическими координатами базовых станции, которые зафиксировали соединения абонентских устройств. Соответственно, представляется возможным установить примерный маршрут передвижения или точку, откуда наиболее часто совершались звонки. Таким образом, в тактическую операцию по установлению лиц, причастных к совершению преступления включаются оперативно-розыскные мероприятия (опросы, наблюдение, наведение справок, получение компьютерной информации обследование помещений, зданий

сооружений, участков местности и транспортных средств, в ряде случаев, прослушивание телефонных переговоров) и следственные действия (осмотры, допросы, получение информации о соединениях между абонентами и (или) абонентскими устройствами, обыск). В рамках рассматриваемой тактической операции именно, результаты следственного действия, предусмотренного статьей 186.1 УПК РФ, выступают в качестве отправной точки и ориентира для последующих действий и решений следователя.

В качестве примера рассмотрим ситуацию, где речь идет о захвате заложников. Как правило, на первоначальном этапе расследования известен абонентский номер, с которого поступил звонок, намного реже место, откуда совершен звонок. Основной задачей в таких ситуациях является установление местонахождения предполагаемого преступника и сведений о его личности. Возможно дополнение тактической операции контролем и записью переговоров или прослушиванием телефонных переговоров. Так, в рассматриваемом нами выше примере о похищении ребенка предпринимателя А, где в случае невыполнения их требований угрожали убийством девочки, в течение нескольких дней, преступники звонили родителям и торопили их со сбором денег, при этом давая слушать голос ребенка. В результате проведения контроля и записи телефонных переговоров были установлены лица, возможно, причастные к похищению. Путем производства получения информации о соединениях между абонентами и (или) абонентскими устройствами были выявлены средства связи преступников, был определен участок местности, откуда чаще совершались звонки. Соответственно, органам расследования стало известно примерное местонахождение похищенного ребенка. Технические возможности оператора связи также позволили определить и уточнить расстояние от переговорщиков до ближайшей базовой станции оператора. В ходе оперативно-розыскных мероприятий и последовавшей затем спецоперации преступники были задержаны, ребенок освобожден[164].

[164] Уголовное дело № 55782-2011 г. // Архив ГСУ ГУ МВД России по Свердловской области.

Из представленной ситуации видно, что своевременная и грамотно спланированная тактическая операция, в структуру которой включены следственные действия, предусмотренные статьями 186 и 186.1 УПК РФ, позволили выявить круг подозреваемых, их местонахождение, а также найти и освободить заложника без риска для его жизни. При этом, нельзя определить какое из указанных следственных действий было центральным звеном тактической операции. Приведем пример, когда получение информации о соединениях между абонентами и (или) абонентскими устройствами в структуре тактической операции может выступать в качестве главного звена и сыграть основополагающую роль. Так, у гр. А. были похищены денежные средства путем мошенничества с использованием мобильного телефона. При производстве такого следственного действия, как получение информации о соединениях между абонентами и (или) абонентскими устройствами был установлен абонентский номер преступника. Установив точное географическое положение абонентского устройства, при содействии с подразделениями уголовного розыска, удалось обнаружить не только искомое устройство, но и преступника[165]. Телефонные мошенничества характеризуются тем, что на первоначальном этапе расследования таких преступлений известен только факт совершения вызова, отправки SMS, перевода денежных средств и т.п., абонентский номер и IMEI код устройства потерпевшего, абонентский номер лица, совершившего преступления, а также время совершения преступления. Естественно, что первым шагом будет производство тактической операции по установлению лиц, причастных к совершению преступления.

Таким образом, в структуру тактической операции будут включены осмотр места происшествия, опрос потерпевшего, установление всех интересующих следствие фактов о событие преступления (время, место, какое количество звонков было совершено, каким способом переводились денежные средства, с каких номеров были совершены звонки), о лице, совершившем или причастном к преступлению, по крайней мере, проверка принадлежности к какому сотовому

[165] Уголовное дело № 53078-2009 г. Архив Протвинского районного суда Московской области.

оператору относится его абонентский номер. Кроме того, необходимо установить были ли еще заявления о подобных преступлениях в ближайшее время, и какая информация есть по данным преступлениям (возможно, тот же способ совершения или фигурирует один и тот же абонентский номер, район происшествия). Все эти мероприятия будут вспомогательными, а центральным ядром тактической операции будет получение информации о соединениях между абонентами и (или) абонентскими устройствами. Именно по его результатам будет с точностью известно на кого и когда зарегистрирован абонентский номер. Систематизировав вышесказанное, нами предлагается схема тактической операции по установлению лиц, причастных к совершению преступления, куда в качестве основного (центрального) следственного действия входит получение информации о соединениях между абонентами и (или) абонентскими устройствами[166].

В рамках реализации тактической операции по установлению лиц, причастных к совершению преступления, куда входит получение информации о соединениях между абонентами и (или) абонентскими устройствами следует обращать внимание на тот факт, что преступники тщательно конспирируют свою деятельность. Готовясь к совершению преступления, они приобретают SIM-карты по поддельным документам или с помощью знакомых, оформляя на них, а также пользуясь халатностью лиц, осуществляющих продажу SIM-карт, оформляют вовсе без документов, на вымышленные имена, занимаются перепрошивкой идентификационных кодов «IMEI», приобретают несколько абонентских устройств и SIM-карт. В таком случае, основополагающей будет выступать информация о местоположении оборудования, с которого осуществлялись звонки в определенное время с известного абонентского номера. Возможны ситуации, когда потерпевшему звонили с разных номеров, но из одной и той же точки, тогда путем производства оперативно-розыскных мероприятий есть вероятность выявить возможное местонахождения сотового телефона, с которого были

[166] Схема тактической операции по установлению лиц, причастных к совершению преступления (Приложение 6)

совершены звонки, и возможных участников преступления. Кроме того, если по результатам рассматриваемого следственного действия станет известно, что абонентский номер еще активен в сети, то появляется возможность отследить с кем еще состоялись контакты. Представленные данные от оператора сотовой связи о местоположении абонента, осуществляющего звонки, позволяют определить конкретное место и проверить наличие там камер видеонаблюдения или свидетелей. Эти сведения расширяют круг ориентирующей информации и новых фактов по делу, обогащают доказательственную базу, а также влияют на дальнейшие действия.

Показательным примером использования получения информации о соединениях между абонентами и (или) абонентскими устройствами в рамках тактической операции по установлению лиц, причастных к совершению преступления, является расследование по уголовному делу об убийстве российского политики Бориса Немцова. 27 февраля 2015 года, примерно 23.31, на Большом Москворецком мосту совершено убийство Бориса Немцова. Исходя из показаний свидетелей и изъятой записи с камеры видеонаблюдения известно, что Борис Немцов возвращался домой со своей подругой, когда примерно на середине моста неизвестный произвел шесть выстрелов, три из которых поразили цель. Затем преступник скрылся на подъехавшем за ним белом автомобиле.

Следствием были запрошены данные системы «Поток» – с моста съезжал серебристый автомобиль ZAZ Chance. 1 марта 2015 года (через день после убийства) машину нашли брошенной в Трубниковском переулке. Все обнаруженные в ней биологические следы отправлены на экспертизу. Далее были запрошены все видеозаписи, свидетельствовавшие о передвижениях Немцова в тот вечер до момента убийства. Были установлено, что один неизвестный на тот момент мужчина появлялся рядом с Немцовым до убийства и после на месте совершения преступления.

Кроме других мероприятий следователями была запрошена детализация всех абонентских соединений в районе убийства. После кропотливого анализа, представленной детализации было установлено 2 абонентских номера, которые

были активны на месте преступления и были отключены сразу после убийства. Владельцы абонентских номеров вымышлены, очевидно, что телефоны приобретались специально, в рамках подготовки к совершению преступления. Лишь небольшая техническая деталь позволила установить личности преступников. Следователи заметили, что у одного из абонентов поменялся IMEI-номер. Вероятно, в телефоне села батарейка и SIM-карту просто переставили в другой аппарат. Следствием было установлено, что с данным IMEI-кодом использовалась SIM-карта, зарегистрированная на Губашева Шадида Шахидовича. Затем, используя данные детализации вызовов, были установлены и другие соучастники преступления, которые, как известно, дали признательные показания, подтвержденные иными вещественными доказательствами[167].

Рассматривая тактическую операцию по изобличению подозреваемых (обвиняемых) заметим, что, как правило, к ней прибегают в условиях противодействия расследованию одного лица или группы лиц. Такие ситуации складываются, когда подозреваемые (обвиняемые), покрывают соучастников, умышленно утаивают его местонахождение, при этом поддерживают связь непосредственно или через посредника. Для изобличения подозреваемого в таких ситуациях, немаловажную роль играют личные наблюдения следователя за поведением субъекта. Например, при ответах на вопросы, касающиеся местонахождения интересующих следствие предметов или лиц, скрывающихся от уголовного преследования в ходе допроса, лицо проявляет неуверенность, растерянность. Или у допрашиваемого проявляется реакция, подтверждающая его осведомленность при предъявлении ему косвенных доказательств. Признаками такой реакции могут выступать затянутость ответов, длительные паузы в ответах, несвязность фраз, внешние проявления волнения и озабоченности (цвет лица, жесты и т.п.).

При проявлении вышеуказанных признаков целесообразно получить информацию, изобличающую подозреваемого (обвиняемого), даже если она будет

---

[167] Дело об убийстве Бориса Немцова // Российская газета - Федеральный выпуск №7395 (229) – [Электронный ресурс]. –https://rg.ru/2007/09/25/svyaz-pravila-dok.html.

носить косвенный характер. В данном случае тактическая операция будет дополнена получением информации о соединениях между абонентами и (или) абонентскими устройствами в целях установления фактов соединений лица с возможными соучастниками или иными лицами, сведения о которых послужат ориентирующей информацией. Исходя из этих данных, выстраивается тактика повторного допроса или принимается решение о вызове собственника установленного абонентского номера в качестве свидетеля. Если получена косвенная информация об абонентских соединениях или устройствах, то нельзя ей пренебрегать, так как она может быть основой такого тактического приема как внезапное предъявление доказательств изобличающих лицо.

В ситуациях, когда результаты получения информации о соединениях между абонентами и (или) абонентскими устройствами говорят о постоянной связи лиц, но допрос и иные следственные действия не позволяют изобличить интересующих лиц, возможно добавление в структуру тактической операции контроля и записи телефонных переговоров. В данном случае результаты детализации вызовов будут основанием для указанного следственного действия.

В качестве изобличающей информации, получаемой от оператора сотовой связи, могут выступать и биллинговые данные, отображающие примерный маршрут владельца абонентского устройства и конкретное время переговоров с привязкой к координатам местности. Эти сведения в совокупности с другими доказательствами не только позволяют восстановить цепочку событий преступления, но выступают в роли криминалистически значимой информации. Такие сведения могут якобы случайно разглашены подозреваемому, например, следователь при разговоре с коллегами упоминает, что исходя из данных о месторасположении приемопередающих базовых станций, на местности организуется поисковая операция. В процессе такого разговора может называться район, здания и другие расположенные вблизи от места сокрытия объектов или лиц. Возможна также демонстрация обстановки случайной подготовки к проведению поисковых мероприятий: определение границ поиска, разграничения обязанностей участников и т.п. Эти факты, могут вынудить подозреваемого

связаться и предупредить скрывающееся лицо, что отобразится в последующей детализации или послужат поводом для дачи признательных показаний. Информация о местоположении абонента или конкретная географическая точка на местности являются основанием для производства поисковых мероприятий в помещениях и территориях, где скрываются разыскиваемые лица. В ситуациях, когда они находятся на участках местности или помещениях, доступ в которые затруднен, его собственники, владельцы либо другие лица противодействуют обследованию помещений сотрудниками органов расследования, возникает необходимость проведения обыска. Завершающим этапом такой тактической операции будет задержание разыскиваемого лица.

Таким образом, тактическая операция по изобличению подозреваемого, обвиняемого может объединять в себе целый комплекс следственных и оперативно-розыскных мероприятий. Наряду с допросом, очными ставками, обыском, выемкой, получением информации о соединениях между абонентами и (или) абонентскими устройствами, контролем и записью переговоров, могут проводиться опросы, наводятся справки о личности или деятельности интересующих следствие лиц, могут быть исследованы предметы и документы, подтверждающие или опровергающие виновность лица. Однако, руководствуясь принципом экономии сил и средств и учитывая постоянную загруженность следователя, целесообразно из всего возможного комплекса мероприятий, выбирать такое их сочетание, при котором в максимально короткий срок, будет достигнута цель тактической операции. Схема рассмотренной тактической операции видится нам, следующим образом. Цель – изобличение лица достигается путем проведения комплекса мероприятий, включающим получение детализации вызовов, данных о местонахождении лица в интересующее следствие время, поиск свидетелей, наведение справок о личности подозреваемого, исследование предметов или документов, свидетельствующих о виновности лица, обыск, выемку, очную ставку и при необходимости контроль и запись переговоров. Все полученные доказательства могут быть использованы при

допросе подозреваемого, что позволит изобличить виновного. Завершается тактическая операция предъявлением обвинения и допросом обвиняемого[168].

Проверка алиби – одна из самых распространенных тактических операций, проводимых при расследовании. Понятие «алиби» закреплено в статье 5 УПК РФ и означает нахождение подозреваемого или обвиняемого в момент совершения преступления в другом месте[169]. Как верно отмечает, О.Я. Баев, алиби может быть как истинным, так и ложным. В первом случае, это средство защиты от необоснованного уголовного преследования, во втором – способ противодействия[170].

Тактическая операция по проверке алиби включает в себя деятельность по выявлению противоречий, установление новых обстоятельств или источников информации, реализацию различных методов проверки, отождествление фактов. Как тактической операции, проверка алиби требует неотложности в проведении, мобильности, использования оперативных и технических возможностей правоохранительных органов.

Чтобы проверить достоверность алиби необходимо установить три основных элемента: время, место совершения преступления и место, где находился подозреваемый в указанное время. Как правило, на момент, когда необходимо проверить алиби лица, следователю уже известно время и место совершения преступления и остается только установить и сопоставить где находился в данный момент подозреваемый. В силу повсеместности применения средств связи и иных новшеств компьютерной техники, подозреваемые (обвиняемые) в обоснование заявляемого ими алиби все чаще ссылаются на то, что в момент совершения преступления они работали на персональном компьютере, пользовались мобильным телефоном, находились в поле зрения

---

[168] Схема тактической операции по изобличению подозреваемых (обвиняемых) (Приложение 7)

[169] Уголовно-процессуальный кодекс Российской Федерации (действующая редакция). – [Электронный ресурс]. − URL: http:/www.consultant.ru.

[170] Баев О.Я. Следователь (основы теории и практики деятельности). Научно-практическое издание. – М.: Прометей, 2017. – С. 385.

камер видеонаблюдения, авторизовались в системах контроля доступа в помещение и т.п.

Таким образом, после заявленного алиби, целесообразно допросить свидетелей или лиц, подтверждающих показания подозреваемого, в некоторых случаях установить наличие и изъять видеозаписи с камер видеонаблюдения с мест, которые указывает подозреваемый. Получить информацию о соединениях между абонентами и (или) абонентскими устройствами необходимо, предварительно выяснив у допрашиваемого, каким абонентским устройством он пользуется, с какой SIM-картой, на чье имя составлен договор о предоставлении услуг связи, не менял ли он телефон. Детализация вызовов и сведения о местоположении абонента выступает весомым доказательством и действительно может либо подтверждать алиби, либо опровергнуть его. Однако, следует учитывать, что в условиях сложных конфликтных ситуаций, когда противоборствующий субъект намерен стоять на своем до конца, несмотря на наличие доказательств изобличающих его вину, целесообразно расширить тактическую операцию иными следственными действиями и оперативно-розыскными мероприятиями. В целях пополнения доказательственной информации в рамках проверки алиби лица, после получения детализации, рассматриваемая тактическая операция может быть дополнена опросами иных участников расследования, проведением очных ставки, следственным экспериментом или повторным допросом подозреваемого и иных лиц[171]. Приведем пример из практики. В марте 2012 года в Брянске мать девятимесячной девочки Светлана Шкапцова сообщила в полицию, что ребенка похитили, когда она оставила коляску у зоомагазина. В рамках расследования ее сожитель, ранее судимый Кулагин заявил алиби о том, что на момент совершения преступления находился в командировке, что подтверждалось рабочим графиком и данными полученными от оператора сотовой связи, свидетельствующими о нахождение абонентского устройства в Москве. Однако следователи все же предполагали, что родители дочери, что-то скрывают. В рамках тактической операции по проверки

[171] Схема тактической операции по проверке алиби лица (Приложение 8).

алиби Кулагина, в их квартире провели повторный обыск, в ходе которого был обнаружен разбитый сотовый телефон. Компьютерно-техническая экспертиза позволила восстановить все данные, в том числе стертые из памяти фотографии, где Кулагин был переодет в женскую одежду (парик, пальто, шарф). В ходе поквартирного обхода установили двух свидетелей, которые видели и опознали по фотографии переодетого в женскую одежду мужчину. Как выяснилось, начальником смены по месту работы Кулагина в Москве оказался его отец, который пояснил, что Кулагин оставил ему сотовой телефон и попросил отвечать на звонки жены, а затем больше не появлялся. С учетом имеющихся данных, при дальнейшей работе удалось добиться признательных показаний от жены, которая рассказала, как Кулагин будучи в состоянии опьянения, несколько раз ударил девочку, о чего последняя скончалась. После этого родители решили сымитировать похищение ребенка[172].

В качестве дополнения отметим, 58,1 % опрошенных практических сотрудников используют получение информации и соединениях между абонентами и (или) абонентскими устройствами для проверки алиби лица[173].

Говоря о роли и месте рассматриваемого следственного действия в структуре тактических операций, нельзя обойти стороной проверку признательных показаний подозреваемого (обвиняемого) и других лиц. Нет сомнений, что данная тактическая операция крайне необходима при расследовании уголовных дел[174]. Ведь, если лицо признается в совершении преступления, то только ему достоверно известны все детали и обстоятельства. Но признательные показания приобретают по-настоящему самостоятельную доказательственную ценность только в совокупности с иными подтверждающими их сведениями. В этой связи, верно пишет В.Н. Перекрестов: «Признание вины –

---

[172] Маркин В. И.Самые громкие преступления XXI века в России / Владимир Маркин. — Москва: Издательство «Э», 2016. — 352 с. — (Тайны Следственного комитета с Владимиром Маркиным).

[173] См.: Результаты изучения уголовных дел, связанных с использованием средств сотовой связи, в процессе раскрытия и расследования преступлений (Приложение 2).

[174] Баев О.Я. Следователь (основы теории и практики деятельности). Научно-практическое издание / О.Я. Баев. – Москва: Прометей. – 2017. – 370.

традиционно считается источником доказательств при условии, что оно сопровождается сведениями о противоправных действиях, совершенных обвиняемым (подозреваемым), проверяется и оценивается в совокупности с другими доказательствами, добытыми по уголовному делу»[175].

Тактическая операция по проверке признательных показаний имеет важное значение при расследования и раскрытия преступления, потому что ее цель заключается в установлении истины и подтверждении виновности лица. Перед проведением данной тактической операции необходимо удостоверится, что показания лица, содержат в себе ответы на ряд важнейших вопросов: когда, где, при каких условиях и обстоятельствах было совершено преступление, кем и каким образом продумывались действия, направленные совершение преступления, какие средства, орудия использовались и каким путем были добыты, кто еще был задействован, какую роль выполняли соучастники, как осуществлялось взаимодействие, какие действия были направлены на сокрытие следов, какие технические средства использовались, куда сбыто похищенное имущество, приметы соучастников и их местонахождение.

Несомненно, что тактическая операция по проверке признательных показаний лица является сложной, требующей использования значительного числа сил и средств правоохранительных органов. Следователю необходимо приложить усилия по проверке всех обстоятельств, которые отражаются в признательных показаниях. Ведь лицо, может намеренно взять вину на себя в силу различных обстоятельств, например, угрозы от соучастников преступления, родственные связи с лицом, совершившим преступление, денежное вознаграждение, намерение ввести следствие в заблуждение и в дальнейшем отказаться от своих показаний, скрыть более тяжкое преступление, попав в места заключения и т.п.

---

[175] Перекрестов В. Н. Уголовно-процессуальное значение признания вины в России: автореф. … дис. канд. юр. наук. Саратов, 2013. С. 9.

Представляется, что такая тактическая операция предполагает всевозможные сочетания следственных действий, оперативно-розыскных мероприятий, иных процессуальных и других действий.

Считаем, что комплекс мероприятий такой тактической операции, будет зависеть от конкретной следственной ситуации и эффективности применения следователем тактических комбинаций. Получив в рамках тактической операции информацию о проверяемых обстоятельствах, следователь, усомнившись в правдивости показаний лица, проводит повторный допрос, оперируя ставшими известными сведениями. При этом, особое значение при проверке признательных показаний, приобретает не тактическая операция, а не менее эффективные тактические комбинации, используемые в рамках следственных действий. Они более простые по структуре, не требуют сложной подготовки, но достаточно действенные. В качестве ремарки отметим, что тактическая комбинация - комплекс тактических приемов и следственного действия, объединенных одним замыслом, проводимых по единому плану, с учетом следственной ситуации и направленных на решение сложной промежуточной задачи[176].

В рамках тактической комбинации при последующих следственных действиях, например, повторном допросе лица, дающего ложные признательные показания, проверке показаний на месте, очной ставке следственном эксперименте, следователь использует не только результаты получения информации о соединениях между абонентами и (или) абонентскими устройствами и иные доказательства, но и подходящие тактические приемы.

Тактическая комбинация может сочетать в себе следующие тактические приемы:

а) производство «тактических» очных ставок по существенным противоречиям в показаниях допрошенных лиц (ч. 1 ст. 192 УПК РФ). Их цель – создать психологический дискомфорт, расшатать волю к сопротивлению;

---

[176] Драпкин Л.Я., Долинин В.Н. Тактика следственных действий: учебно-практическое пособие. – Екатеринбург: издательский дом Уральского государственного университета, 2015. – С. 10.

б) демонстрация доказательств не полностью, «как бы невзначай», к примеру, сообщить лицу, что следствию стало известно об использовании им второго абонентского номера или устройства, но не говорить, что по ним уже получены сведения о соединениях, опровергающие показания;

в) упоминание об имеющихся доказательствах или их простое перечисление с указанием источников происхождения, например упоминание о входящих вызовах, о местоположении абонентского устройства лица в определенное время;

г) создание информационной неосведомленности о результатах обысков, проведенных в отсутствие подозреваемых (обвиняемых) в соответствии с п. 11 ст. 182 УПК РФ, и ее применение в ходе допроса;

д) умелое использование результатов некоторых других процессуальных действий, особенно результатов судебных экспертиз, контроля и записи переговоров, получения информации о соединениях между абонентами и (или) абонентскими устройствами;

е) передача косвенной, скрытой информации, действующей «в обход» доминирующей у конфликтующего субъекта психологической установки на умолчание или дачу ложных показаний, в силу сложных ассоциативных отношений приводящая к неизбежному и внезапному признанию. Именно наличие информация о соединениях между абонентами и (или) абонентскими устройствами, является косвенным доказательством, позволяет реализовать данный тактический прием.

По нашему мнению, именно через тактические комбинации, с учетом уже имеющихся результатов следственных действий, в том числе и получения информации о соединениях между абонентами и (или) абонентскими устройствами, можно достичь цели тактической операции по проверке признательных показаний лица в максимально короткие сроки, не используя при этом всего спектра процессуальных и иных действий. Схема рассмотренной тактической операции разработана и указана в соответствующем приложении[177].

[177] Схема тактической операции по проверке признательных показаний подозреваемого (обвиняемого) и других лиц (Приложение 9).

Очевидно, что перечень тактических операций, в рамках которых можно рассмотреть вопрос о роли получения информации о соединениях между абонентами и (или) абонентскими устройствами в их структуре, может быть расширен. Кроме отмеченных, данное следственное действие включается в структуру тактических операций по розыску и задержанию лица, поиску похищенного имущества или безвестно отсутствующих лиц и др.

Вышесказанное позволяет сделать вывод о том, что являясь средством достижения цели тактической операции, получение информации о соединениях между абонентами и (или) абонентскими устройствами, может выступать в качестве основного (центрального), а также в качестве подготовительного или вспомогательного следственного действия, по результатам которого будут предпринято решение о дальнейшем ходе расследования.

К имеющим центральное значение в структуре тактической операции, относятся те следственные действия, которые позволяют полностью решить главные задачи. Например, в рамках тактической операции по проверке алиби, связанного с использованием средств сотовой связи, результаты следственного действия, предусмотренного статьей 186.1 УПК РФ, подтвердились иными доказательствами и позволили его опровергнуть. Также, если необходимо получить доказательственную информацию о принадлежности сотового телефона тому или иному лицу, определить местоположение устройства в определенный период времени или проверка показаний невозможна без информации, содержащейся в базе данных оператора сотовой связи, то данное следственное действие, позволяя решить эти задачи в полном объеме, приобретает центральное значение.

Однако, проведенное исследование, а также результаты анкетирования[178], свидетельствуют о том, что получение информации о соединениях между абонентами и (или) абонентскими устройствами чаще выступает в качестве

[178] 58,1% опрошенных практических сотрудников поддержали позицию о том, что получение информации о соединениях между абонентами и (или) абонентскими устройствами выступает в качестве вспомогательного мероприятия в структуре тактической операции. (Приложение 1).

вспомогательного мероприятия в структуре тактических операции. Это обусловлено тем фактом, что данное следственное действие используется при расследовании любого преступления, где упоминается об использовании мобильного телефона, SIM-карты или есть сведения, что участники контактируют посредством сотовой связи и т.п. В этих случаях производство следственного действия, предусмотренного ст. 186.1 УПК РФ, необходимо для восстановления полноты картины преступного события, получения информации об обстоятельствах, подлежащих установлению, подтверждающих данные о лице или иные сведения, которые будут носить ориентирующий характер, для предупреждения и преодоления противодействия, оказываемого участниками расследования или для организации поиска. Результатом его производства могут быть сведения о личности, местонахождении абонентского устройства, неизвестного или скрывающегося от следствия субъекта, объектов. Как правило, такие результаты служат основанием для проведения других следственных действий или оперативно-розыскных мероприятий.

Таким образом, в зависимости от сложившейся ситуации, рассматриваемое следственное действие в структуре тактической операции выступает в качестве вспомогательного либо центрального звена, а информация, полученная в ходе тактической операции с использованием рассматриваемого следственного действия, носит как ориентирующий характер, так и может выступать в качестве основополагающей, на которой выстраиваются версии. Важность и необходимость данного вопроса очевидна, так как основными целями тактических операций, куда входит данное следственное действие, выступают расширение доказательственной базы, восполнение дефицита информации, а также подтверждение или опровержение уже имеющихся фактов по расследуемому уголовному делу.

ГЛАВА 3. ИСПОЛЬЗОВАНИЕ РЕЗУЛЬТАТОВ ПОЛУЧЕНИЯ ИНФОРМАЦИИ О СОЕДИНЕНИЯХ МЕЖДУ АБОНЕНТАМИ И (ИЛИ) АБОНЕНТСКИМИ УСТРОЙСТВАМИ В ПРОЦЕССЕ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

§ 1. Организация и тактика проведения отдельных следственных действий с учетом информации о соединениях между абонентами и (или) абонентскими устройствами

Телекоммуникационная отрасль – одна из самых быстро развивающихся отраслей современной экономики. Сотовая связь непрерывно прогрессирует с каждым днем, количество абонентов постоянно растет, услуги становятся разнообразнее и более доступными на все больших территориях. Как уже ранее отмечалось, мобильные телефоны активно используются не только в повседневной деятельности людей, но и в криминальном обиходе в качестве средства совершения преступления или как предмет посягательства. Таким образом, изучение свойств и качеств сотовой связи, а также технических средств мобильной связи является не просто одной из задач правоохранительных органов, но и необходимостью. В условиях постоянного увеличения количества технических средств коммуникаций, сведения, получаемые от оператора связи, играют важную роль в доказывании по уголовным делам. Особенно следует отметить, влияние информации, полученной от оператора сотовой связи на дальнейший ход расследования, а также на выбор и производство последующих следственных действий. Зачастую, именно от имеющихся сведений или обнаруженной аппаратуры (ее частей) на месте происшествия зависит организация и тактика отдельных следственных действий.

Основным следственным действием, непосредственно связанным с получением и анализом информации, транслируемой с помощью средств телекоммуникации, является получение информации о соединениях между абонентами и (или) абонентскими устройствами. Тем не менее, в ряде случаев следователи получают и исследуют данную информацию и путем проведения иных следственных действий. Иные следственные действия могут также

производиться в системной взаимосвязи, как в рамках подготовительного этапа по отношению к получению информации о соединениях между абонентами и (или) абонентскими устройствами, так и в рамках проверки и анализа информации, полученной в результате производства указанного следственного действия. В первом случае они преследуют цель получения соответствующей информации об абоненте, абонентском терминале или абонентском номере, необходимой для данного следственного действия. Например, в результате допроса потерпевшего или свидетеля выясняется телефонный номер лица, переговоры которого имеют значение для установления обстоятельств преступления. Во втором случае информация, полученная в результате рассматриваемого следственного действия, проверяется и подтверждается результатами других следственных действий. Например, в детализации отражены частые звонки между соучастниками, что подтверждает их постоянную и устойчивую связь или позволяет выявить абонента неизвестного следствию, разработка которого позволила установить его причастность и роль в группе. Последующий обыск по месту жительства установленного лица, выполняющего функции организатора в преступной группе, позволит обнаружить упаковку от SIM-карт телефонных номеров, которыми пользовались различные соучастники. Это подтверждает, что данное лицо в организованной преступной группе, выполняло ряд организационных полномочий, в том числе по принятию различных мер конспирации между соучастниками, а также по обеспечению соучастников средствами связи[179].

Рассмотрим осмотр места происшествия, как следственное действие, в рамках которого может быть получены сведения об абонентах или их устройствах. Основная цель осмотра места происшествия – обнаружение следов преступления и других фактических данных, имеющих значение для уголовного дела и входящих в предмет доказывания. Это одно из первоначальных следственных действий, с помощью которого происходит обнаружение, фиксация и изъятие следов. Обнаруженные следы, выступая в качестве криминалистически значимых

[179] Материалы уголовного дела № 4717453. Архив ГСУ при ГУ МВД России по Ростовской области. 2013 г.

источников доказательственной информации, в совокупности предопределяют направленность расследования преступления. Особую важность данное следственное действие приобретает при расследовании преступлений, совершенных в условиях неочевидности.

Полученные в ходе осмотра места происшествия сведения позволяют выдвинуть версии, наметить основные пути их проверки, определить круг лиц, причастных к совершению преступления, в целом способствуют раскрытию преступления и изобличению виновных. Эффективность и качество осмотра места происшествия во многом зависит от применяемых следователем, с учетом конкретного случая, тактических приемов и рекомендаций, а также соблюдения тактических положений следственного осмотра.

При осмотре места происшествия могут быть обнаружены мобильные телефоны, их части или SIM-карты оставленные, выброшенные, утерянные или умышленно спрятанные участниками преступления. Так, 57% анкетируемых отметили, что при осмотре места происшествия получили в распоряжение объект, содержащий информацию о телекоммуникационных контактах[180]. Для производства осмотра места происшествия нередко привлекается специалист, который вправе использовать поисковые технические устройства для обнаружения и фиксации предметов и следов. Например, рационально применение металлоискателя в лесистой или поросшей кустарником местности, если известен факт, что в ходе совершения преступления был утерян сотовый телефон или умышленно выброшена SIM-карта. Об использовании такого рода устройств делается запись в протоколе осмотра места происшествия. В случае обнаружения сотового телефона, в протоколе подробно описывается его месторасположение, внешние признаки и функциональное состояние. Следует обратить внимание на то, что кроме SIM-карты, кода IMEI и других характеристик, корпус или детали мобильного устройства могут содержать материальные следы (следы пальцев рук, повреждения или биологические следы - кровь, пот, волосы). В связи с этим рекомендуется перед изучением внутренней составляющей устройства, тщательно

[180] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

произвести его внешний осмотр, и при необходимости, надлежаще упаковать и назначить соответствующие экспертизы. Если обнаруженная SIM-карта в рабочем состоянии, есть вероятность узнать данные о ее владельце, а соответственно появляются основания для получения информации от оператора связи. На SIM-карте может содержаться информация об операторе связи, сведения о входящих и исходящих SMS сообщениях, о примерном местонахождении абонента, путем установления последней базовой станции, о контактах, сохраненных на SIM – карте. Некоторые авторы полагают, что для установления круга абонентов, активность которых проявлялась до, в момент или после совершения преступления и, следовательно, фиксировалась базовыми станциями, расположенными около места происшествия, следователю в ходе осмотра необходимо произвести не менее трех контрольных звонков, о чем в протоколе делается соответствующая пометка[181]. В тех случаях, когда на момент проведения осмотра места происшествия номер абонента, о котором в последующем должна быть получена информация от оператора связи, неизвестен, необходимо производить контрольные звонки с SIM-карт всех региональных операторов сотовой связи. Заметим, что с 2012 года каждый абонент имеет право сохранять свой абонентский номер, даже в случае перехода на услуги другого мобильного оператора[182]. Данный факт необходимо учитывать при исследовании детализации телефонных соединений и при получении информации о конкретных абонентах.

Положительный результат в процессе доказывания по уголовному делу будет достигнут, только если следователь использовал все ставшие известные сведения в ходе даже повторного осмотра. Тщательно проведенный осмотр места происшествия всегда позволяет обнаружить следы преступника, потерпевшего и установить объективную сторону преступления. Осмотр места происшествия

---

[181] 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: монография. – М.: Юрлитинформ, 2015. С. 66.

[182] О внесении изменений в Федеральный закон «О связи» и статьи 333.33 и 333.34 части второй Налогового кодекса Российской Федерации»: федеральный закон от 25.12.2012 № 253-ФЗ. – [Электронный ресурс]. − URL: http:/www.consultant.ru.

остается полезным даже, если не удается отыскать материальные следы, так как дает возможность следователю подробно изучить обстановку и уяснить сущность совершенного деяния. Добавим, что промедление с производством осмотра места происшествия может повлечь утрату материальных следов, нарушение обстановки, которая была на момент совершения преступления, поэтому следует проводить осмотр сразу же после опроса очевидцев либо потерпевшего.

Как уже отмечалось, в ходе осмотра места происшествия может быть обнаружен сотовый телефон, который непосредственно является источником процессуальной информации или выступает в качестве средства, орудия преступления. Также сотовый телефон может быть изъят при производстве личного обыска у подозреваемого. В таких ситуациях необходимо более тщательно и детально описать и зафиксировать внешние признаки, функциональное состояние и, если это возможно информационное содержимое устройства в ходе осмотра предметов.

Последовательность осмотра мобильного телефона можно разделить на три стадии:

1. Внешний осмотр. На этой стадии проведения внешнего осмотра следователь изучает и фиксирует общие признаки: тип и состояние сотового телефона, при этом в протоколе указывается марка, модель, форма аппарата, цвет основных частей, размер; наличие объективов тыльной и (или) лицевой фото/видеокамеры (вспышки), фирменных наименований, логотипа, обозначений; количество и расположение функциональных, встроенных, сенсорных клавиш (джойстика); разъемов Mini (Micro) USB, зарядного устройства, стереонаушников; наличие отверстий для динамика, микрофона, внешней освещенности. Отдельно указываются особые приметы наружного строения — повреждения: сколы, царапины, потертости, отсутствие должных элементов; наличие дополнительных атрибутов и технических составляющих — чехла, шнурка, брелока, гарнитуры, полимерных наклеек, графических вставок, надписей, инкрустации драгоценными металлами и др. В ходе внешнего осмотра проводится детальная фотосъемка внешней, оборотной, боковых панелей мобильного телефона. В случае если

осматриваемый телефон раскладного («бабочка») или раздвижного типа («слайдер»), то телефон фотографируется в первоначальном и раскладном/раздвижном состоянии.

2. Конструктивный осмотр. На данной стадии производится осмотр конструкции телефона по частям — задней крышки телефона и (или) аккумуляторной батареи (в определенных моделях аппаратов сотовой связи батарея встроена в корпус, либо в заднюю крышку), флэш-карты, SIM-карт(ы). При осмотре аккумуляторной батареи в протоколе следует указать ее идентификационный номер, тип, марку, модель, мощность, иную информацию, указанную на корпусе. Также в протоколе указывается цвет и родовой материал, из которого изготовлена батарея. При осмотре флэш-карты (MiniSD) необходимо обратить внимание на ее идентификационный номер, объем, цвет и родовой материал корпуса. SIM-карта, обнаруженная в телефоне, осматривается аналогичным образом. Как правило, на корпусе SIM- карты имеется логотип оператора сотовой связи, описание которого также обязательно в протоколе.

В ходе конструктивного осмотра проводится детальная фотосъемка внешней и оборотной стороны батареи, флэш-карты, SIM-карты, а также тыльной стороны корпуса мобильного телефона (без задней крышки), так чтобы на снимке был виден IMEI-номер аппарата.

3. Осмотр информационной среды. Осмотр информационной среды телефона включает изучение и фиксацию сведений, которые содержатся в памяти мобильного телефона, флэш-карты, SIM-карты. В случае если в ходе осмотра следователю удалось включить мобильный телефон, и получен доступ к сведениям, которые в нем находятся, в протоколе в хронологическом порядке фиксируются все производимые в дальнейшем с аппаратом манипуляции (Приложение 5) [183].

В следственной практике нередко возникают ситуации, в которых в ходе производства первоначальных следственных действий изымается сразу несколько аппаратов сотовой связи во включенном состоянии. Выключать в таких случаях

[183] Образец протокола осмотра предмета (документа). См. Приложение 5.

мобильные телефоны до осмотра нецелесообразно (отключение может произойти при извлечении батареи, SIM-карты, при осмотре IMEI-кода на наклейке, расположенной во внутренней части панели телефона и т.д.), так как при последующем включении потребуются коды блокировки (PIN-код), которые могут быть известны только его последнему пользователю (подозреваемому, свидетелю или потерпевшему). Отказ последнего в предоставлении информации по разблокировке телефона может исключить возможность незамедлительного полноценного исследования его информационного содержимого (электронной записной книжки, входящих и исходящих соединений, SMS-, MMS-сообщений, E-mail, голосовой почты, фото-, видеофайлов, диктофонных записей, органайзера и др., в зависимости от модели телефона). Подчеркнем, что если к моменту осмотра телефон был включен, то конструктивный осмотр следует проводить только после изучения его информационной среды.

Представляется особо значимым акцентировать внимание на том, что если для уголовного дела имеют значение данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи, то, в случае отсутствия согласия законного владельца мобильного телефона, следователь может осматривать подобного рода информацию только по решению суда. Обязательность исполнения этого положения корреспондируется с позицией Конституционного Суда Российской Федерации, выраженной в определении от 2 октября 2003 г. № 345-0: «...информацией, составляющей охраняемую Конституцией Российской Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения. Иное означало бы несоблюдение требования статьи 23 (часть 2) Конституции Российской Федерации о

возможности ограничения права на тайну телефонных переговоров только на основании судебного решения»[184].

Осмотр информационной среды необходимо начать с указания в протоколе процедуры разблокировки клавиатуры телефона, перечисления графических и текстовых элементов, которые отобразились на его экране после разблокировки. Затем осуществляется проверка IMEI- номера мобильного телефона нажатием комбинации клавиш *#06# (пятнадцатизначный номер должен отобразиться на экране телефона) или в настройках мобильного телефона.

В случае если телефон не защищен паролем, то в протоколе осмотра последовательно указывается информационное содержимое телефона — список контактов, сообщений, наличие изображений, фотографий, видеороликов и т.д. При описании определенного контакта указывается его вид (входящий, исходящий, пропущенный), время, длительность, данные абонента, с которым осуществлен контакт, а также его абонентский номер (описание сообщения исключает указание длительности, но включает текстовое (SMS) и (или) графическое содержимое (MMS).

Описание графических изображений, фотографий состоит из следующих элементов: указание того, что или кто изображен, тип, размер, время создания файла (описание видеороликов включает, помимо указанного, их длительность)[185].

В ходе осмотра информационной среды телефона проводится поэтапная детальная фотосъемка экрана мобильного телефона с информацией, представляющей значение для уголовного дела. Для визуальной фиксации большого объема сведений, содержащихся в информационной среде телефона, следует применять видеосъемку. При этом следователь в обязательном порядке комментирует все действия, которые направлены на получение той или иной информации с помощью манипуляций с телефоном.

---

[184] Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 г. «О связи: определение Конституционного Суда РФ от 2 октября 2003 г. № 345-0 // Вестник Конституционного Суда РФ. 2004. № 1. С. 51.

[185] Образец протокола осмотра предмета (документа). См. Приложение 5.

Следует напомнить, что для извлечения и анализа информационных данных из средства сотовой связи любого типа и вида в следственной и экспертной практике широко используются специальные устройства («Мобильный криминалист», «UFED», «XRY» и др.), позволяющие войти в операционную систему в обход паролей и логинов (распознавая их), работать с мобильными устройствами без аккумулятора либо отдельно с SIM-картой[186]. Поэтому, в случае если доступ к информационной среде мобильного телефона затруднен, для участия к осмотру необходимо привлечь специалиста, имеющего навыки пользования данными устройствами. Например, UFED – Universal Forensic Extraction Device. Указанную технологию активно применяют специалисты подразделений Главного управления криминалистики Следственного комитета Российской Федерации.

UFED представляет собой функциональное и технологически совершенное программное решение в области мобильной криминалистики. Данный комплекс позволяет высокотехнологичное извлечение информации, ее расшифровку, анализ и составление отчётов о полученных оперативных сведениях. С помощью UFED можно извлечь файловую систему, а также пароли ко всем данным (даже если они были удалены) из огромного числа устройств, включающих традиционные и обычные мобильные телефоны, смартфонов, портативных устройств GPS, планшетов и телефонов китайской сборки на основе микропроцессора. Благодаря собственному аппаратному обеспечению, встроенному аккумулятору, интуитивно понятному клиенту GUI и сенсорному экрану, UFED ускоряет процесс расследования, соответствуя требованиям криминалистических исследований мобильных устройств. UFED объединяет целый комплекс простых и эффективных в использовании приложений для следователей, которые хотят расследовать дело как можно быстрее:

---

[186] Скобелин С.Ю. Юридическая основа и процессуальное оформление извлечения и анализа данных из мобильных устройств // Расследование преступлений: проблемы и пути их решения: сб. науч.-пракг. трудов. Вып. 1. М.: Буки Веди, 2013. С. 183.

- UFED Physical Analyzer – приложение, предназначенное для расшифровки и анализа данных и составления отчёта;

- UFED Phone Detective – современное приложение, позволяющее моментально идентифицировать телефон;

- UFED Reader – приложение, с помощью которого уполномоченный сотрудник может поделиться с другими полученной информацией.

UFED позволяет извлечь любой сегмент из памяти мобильного устройства и использует методы углубленного декодирования, анализа и создания отчетов. С его помощью можно получить сведения об IMEI коде мобильного устройства, о SIM-карте, входящих и исходящих вызовах и SMS, MMS сообщениях, об использованном интернет трафике, включая открывавшиеся страницы, о контактах, записанных в телефонной книге и на модуле SIM-карты, обо всем содержимом памяти устройства (аудио- и видео файлы, пароли, текстовые сообщения, записи календаря, служебные данные и т.п.). Комплекс UFED открывает доступ к GPS-координатам местоположения мобильного устройства, список действий производимых с телефоном, а также к содержанию переписки в социальных сетях, осуществляемой через исследуемое мобильное устройство. Как известно, информация, хранящаяся в мобильных устройствах, имеет достаточно весомое значение для уголовного дела. И, как верно подмечают Бурцева Е.В., Рогова И.А., данные сведения способствуют оптимизации планирования расследования преступления, проверке следственных версий и в целом – закреплению доказательственной базы по уголовному делу, а также подтверждают факт совершения лицом преступления (например, фото или видеосъемка преступления, переписка с заказчиком убийства, SMS – сообщения с угрозами в адрес потерпевшего и т.п.) или наоборот опровергают его причастность к совершению противоправных действий[187]. В подтверждение вышесказанного,

[187] Бурцева Е.В., Рогова И.А. Проблемы получения информации, содержащейся в электронных мобильных устройствах, с применением универсального устройства извлечения судебной информации (UFED) / Materialy X mezinarodni vedecko-prakticka konf.: Efektivni nastroje modernich ved. - 2014 (27.04.2014-05.05.2014). Dil 11. Pravni vedy Administrativa. - Praha. Publishing House «Education and Scietnce» s.r.o. – С. 54.

приведем пример из практики. В ходе следствия Красногвардейским МСО Главного следственного управления уголовного дела по обвинению троих местных жителей в совершении преступлений, предусмотренных п. «а» ч. 2 ст. 131 УК РФ и п. «а» ч. 2 ст. 132 УК РФ, по факту изнасилования и насильственных действий в отношении односельчанки, в ходе осмотра места происшествия изъяты сотовые телефоны подозреваемых. Изъятые мобильные устройства связи были осмотрены сотрудниками управления криминалистики Главного следственного управления с применением UFED, что позволило обнаружить в памяти одного из телефонов видеозапись совершенных преступных действий в отношении потерпевшей[188]. Так было получено неопровержимое доказательство вины подозреваемых в совершенном преступлении. В последующем данное уголовное дело направлено для рассмотрения в Красногвардейский районный суд Республики Крым, где обвиняемым вынесли приговор.

Однако, остается открытой проблема процессуального оформления извлечения данных, получаемых с использованием криминалистической техники. Если порядок получения информации о соединениях между абонентами и (или) абонентскими устройствами закреплен в ст. 186.1 УПК РФ, то извлечение содержательной информации (фото, видео, переписка в социальных сетях и т.п.) из мобильных устройств связи с помощью UFED законодателем не урегулировано. Так, криминалистическая техника для извлечения информации из мобильных устройств используется в рамках:

- осмотра предметов (ч. 2 ст. 176 УПК РФ);

- назначения и проведения экспертизы (компьютерно-технической);

- в ходе ОРМ (ст. 6 Федерального закона от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности»[189].

---

[188] Обзор применения криминалистической техники Главным управлением Следственного комитета Республики Крым. – [Электронный ресурс]. − URL: http:/ http://crim.sledcom.ru/Kabinet_kriminalistiki.

[189] Бурцева Е.В., Рогова И.А. Проблемы получения информации, содержащейся в электронных мобильных устройствах, с применением универсального устройства извлечения судебной информации (UFED) / Materialy X mezinarodni vedecko-prakticka konf.: Efektivni nastroje modernich ved. - 2014 (27.04.2014-05.05.2014). Dil 11. Pravni vedy Administrativa. - Praha. Publishing House «Education and Scietnce» s.r.o. - C. 56.

На наш взгляд, для решения данной проблемы целесообразно обобщить и унифицировать практику применения специальных криминалистических устройств для извлечения информации, содержащейся в электронных мобильных устройствах, а также разработать единый подход в процессуальном оформлении получения данных сведений в рамках производства компьютерно-технической экспертизы.

Информация о соединениях между абонентами и (или) абонентскими устройствами также представляет интерес при производстве допроса в различных ситуациях. Являясь наиболее распространенным процессуальным действием, производящимся по каждому уголовному делу, допрос служит средством получения новых обстоятельств, проверки и уточнения уже имеющихся доказательств[190]. По итогам анкетирования, можно сделать вывод о том, что результаты получения информации о соединениях между абонентами и (или) абонентскими устройствами использовались следователями (дознавателями) при допросе обвиняемого (подозреваемого) в 90% случаев, потерпевшего (свидетеля) – 80%[191].

Допрос далеко не всегда выступает как надежное и эффективное средство получения интересующих сведений, особенно в конфликтных ситуациях, когда цели следователя и допрашиваемого противоположны. В связи с этим необходимо правильно определить предмет допроса, оптимально использовать тактические приемы допроса, учитывая психологические аспекты в процессе его производства. От вышеперечисленного зависит полнота, достоверность показаний, и в целом, результативность допроса. Тактика допроса в бесконфликтной ситуации с учетом сведений об абонентах и (или) абонентских устройствах должна быть выстроена следующим образом:

---

[190] Драпкин Л.Я. Тактика следственных действий: учебное пособие / Л.Я. Драпкин. – Екатеринбург: Уральский юридический институт МВД России. 2014. С. 67-68.

[191] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

- необходимо установить психологический контакт с допрашиваемым, показывать заинтересованность к его судьбе, проявляя при этом уважение и добросовестность;

- нельзя задерживать допрос. Начало должно быть заранее продумано, не стоит отвлекаться во время допроса на разговоры или другие дела. Следует учесть, что даже внешний вид следователя является важным звеном для установления психологического контакта;

- должное внимание необходимо уделить подготовке допроса, ознакомление с анкетными данными допрашиваемого лица, запись их в протоколе и предупреждение об уголовной ответственности за отказ от дачи показаний и дачу ложных показаний должны проходить в спокойной, доброжелательной обстановке, чтобы закрепить психологический контакт;

- ставшие известными сведения от оператора сотовой связи, при допросе будут носить роль подтверждающей информации его показаний, поэтому необходимо тактически правильно ее преподнести, чтобы прослеживалась логика и последовательность задаваемых вопросов;

- изначально, зная предмет допроса, следователь должен продумать порядок вопросов, касающийся наличия мобильного телефона допрашиваемого, его звонков, местонахождения во время разговоров с тем или иным лицом;

- следует также учесть, что допрашиваемый может искусственно создать бесконфликтную ситуацию и использовать доверие следователя, поэтому весь процесс производства допроса, начиная с подготовки, оперативные данные и иная информация, контрольные и проверочные вопросы, должны быть продуманы таким образом, чтобы выявить подлинную позицию допрашиваемого.

Выделим ряд тактических приемов, которые помогут следователю в такой ситуации: детализация и конкретизация показаний, использование ассоциативных связей, получение объяснений и уточнений по уже имеющимся доказательствам, применение наглядности. С помощью имеющейся информации о соединениях между абонентами и (или) абонентскими устройствами особенно эффективно использовать такой тактический прием как создание впечатления о большей

осведомленности следователя. Говоря о детализации, следователь также может упомянуть о возможности определения местоположения звонящего в определенный период времени, что будет выступать хорошим стимулом допрашиваемому для дачи правдивых показаний.

При первоначальном допросе потерпевшего, через короткий промежуток времени после происшествия, нередко даются неточные или недостоверные показания о случившемся. Если лицо еще не успело «прийти в себя», находится в шоковом состоянии, испытывает физическую боль от причиненных телесных повреждений, то не исключено, что некоторые важные детали совершения преступления или признаки похищенного имущества могут быть искажены при допросе. В следственной практике имеются примеры таких ситуаций. Так, в феврале 2015 года, М. находился на пересечении ул. Ленина и ул. Московская г. Екатеринбурга. Ему навстречу шел А. Приближаясь к М., последний оступился и упал на землю. М. помог А. подняться и, увидев в левом нагрудном кармане рубашки А. сотовый телефон «Samsung Galaxy S», похитил его. После этого, с целью пресечения попытки его преследования, толкнул А., применив в отношении последнего насилие, не опасное для жизни и здоровья. В ходе первоначального допроса потерпевший пояснил, что не помнит модель и характерные внешние признаки похищенного сотового телефона, а также дал недостоверные сведения о времени совершения преступления, не запомнил каких – либо отличительных черт преступника, так как не ожидал нападения, и кроме того, когда упал, ударился головой о землю. В данном случае, следователь, получив детализацию вызовов по абонентскому номеру, принадлежащему А., вызвал потерпевшего для повторного допроса, где предъявил ему сведения о последних звонках и примерном периоде времени и местонахождении до совершения нападения и непосредственно во время него. После чего, А. смог восстановить цепочку событий предшествующих нападению на него, а также подробно описал некоторые внешние признаки похищенного[192].

[192] Постановление Кировского районного суда г. Волгограда от 04 июня 2015 года по делу №1 –107/2015. [Электронный ресурс]. - URL: https://rospravosudie.com.

Как видно из представленного примера, для подтверждения или опровержения фактов, данных допрашиваемым, может послужить информация о соединениях абонента. Следователь, оперируя полученными сведениями, может выбрать наиболее эффективную тактику допроса. Установив психологический контакт и убедившись, что допрашиваемый в нормальном расположении духа, ему предлагается самостоятельно рассказать об обстоятельствах дела. Далее следователь конкретизирует интересующие его детали. Целесообразно спросить, каким сотовым телефоном или SIM-картами пользовался (пользуется) потерпевший (свидетель), какие осуществлялись последние соединения. При хищении сотового телефона, кроме внешних признаков, необходимо выяснить его стоимость на момент покупки и на момент совершения преступления, в каком размере оставались денежные средства на абонентском счету, предприняты ли меры по блокированию SIM-карты (SIM-карт).

В некоторых ситуациях потерпевший (свидетель) видел, как преступник во время совершения преступления пользовался сотовым телефоном, тогда есть необходимость уточнить место, примерное время, продолжительность разговоров. Немаловажное значение имеет номер IMEI, а также был ли он изменен при пользовании владельцем мобильного устройства. По IMEI коду можно обнаружить и идентифицировать похищенный телефон. Нередко в целях сокрытия следов преступления и сбыта, номер IMEI похищенного сотового телефона изменяют, а от SIM-карты избавляются, в таком случае шансы найти похищенное имущество значительно уменьшаются.

Если же получение информации о соединениях между абонентами и (или) абонентскими устройствами принесло положительный результат и представленная детализация содержит данные о пользователях, которые осуществляли звонки, то следователю необходимо привлечь сотрудников оперативных подразделений для установления лица, использующего похищенный телефон. Благодаря проведению таких оперативно-розыскных мероприятий как наведение справок, получение компьютерной информации, прослушивание телефонных переговоров, есть вероятность установления либо подозреваемого,

либо сведений о том, что похищенный аппарат, использует лицо, не причастное к совершению преступления. В первом случае, подозреваемым может оказаться несовершеннолетний, студент или лицо, ранее не привлекавшееся к уголовной ответственности, которые пользуются абонентским номером потерпевшего до обнуления средств на счету. К ним также можно отнести лиц, которые используют похищенный телефон, но со своей SIM-картой. В перечисленных ситуациях следует действовать оперативно, принимая тактически правильные решения, так как преступник или причастные к совершению преступления лица в любой момент могут избавиться от похищенного имущества и SIM-карты либо изменить номер IMEI. Значительную роль в таких случаях играет фактор внезапности, фиксация местоположения абонента, предоставление детализации звонков во время допроса как доказательства вины подозреваемого, а также информационное содержимое абонентского устройства.

Во втором случае, лицо, как правило, не знает о том, что сотовый телефон приобретен преступным путем, либо допускает, но не придает этому значения. К ним относятся знакомые, родственники преступника, покупатели телефона в ломбарде, комиссионном магазине или у граждан, осуществляющих продажу на улице, на вокзалах, площадях и т.д. При допросе указанных лиц, следует узнать как можно больше информации о том, каким образом, где и у кого был приобретен сотовый телефон. В таких случаях при допросе необходимо выяснить следующее:

- как сотовый телефон оказался у допрашиваемого;

- кто ему его передал, подарил, отдал или продал, а также при каких обстоятельствах это произошло;

- знает ли допрашиваемый о предыдущей судьбе используемого им сотового телефона, и то, как он достался лицу ему передавшему;

- если выяснился факт о том, что телефон был продан допрашиваемому, то устанавливается тот, кто ему его продал, описание внешности, приметы, личные данные, где, когда именно имело место событие, за какую цену было приобретено устройство;

- если выясняется, что допрашиваемый нашел сотовый телефон, то необходимо узнать все обстоятельства, при которых это произошло, а также лиц, кто может данный факт подтвердить;

- в ситуациях, когда телефон был приобретен или на данный момент находится в ломбарде, комиссионном магазине и т.п., необходимо установить наличие документов, которые при этом составлялись (чек, договор купли/продажи, гарантийный талон и т.п.).

Затем по поручению следователя органы дознания проверяют всех лиц, которые могли продать, подарить или купить похищенное имущество. Как правило, это позволяет выйти на преступника или установить лиц, которые располагают сведениями о нем. Кроме того, целесообразно также установить и допросить тех лиц, с которыми была связь с похищенного телефона, так как это может помочь в изобличении преступника. При этом, если следователь выяснил кем используется на данный момент похищенный сотовый телефон, лицо следует вызывать на допрос без указания причины вызова, так как есть вероятность, что гражданин избавиться от разыскиваемого сотового телефона до допроса.

Информация, полученная от оператора сотовой связи, имеет особое значение при допросе, в ситуациях, когда оказывается противодействие расследованию. Особенно часто такие ситуации возникают, когда подозреваемые пытаются утаить сведения о соучастниках или лиц, причастных к совершению преступления. Не исключены случаи, когда свидетели или потерпевшие скрывают известную им информацию имеющую значение для уголовного дела. В связи с этим, следователю необходимо тщательно анализировать полученную детализацию.

Основой тактики допроса в конфликтных ситуациях является проникновение следователя в планы и намерения противостоящей стороны. Для успешного преодоления конфликтных ситуаций существует целая система тактических приемов. Мы остановимся только на тех, которые могут использоваться с учетом известной следователю информации о соединениях между абонентами и (или) абонентскими устройствами.

К таким тактическим приемам в первую очередь отнесем те, которые направлены на создание у конфликтующего представления о степени осведомленности следователя. Цель таких приемов создать желаемое ощущение у допрашиваемого об объеме имеющихся в его распоряжении доказательств, что в конечном итоге должно убедить конфликтующего о бесперспективности своей позиции. Типичными приемами данной группы являются вопросы о принадлежности того или иного абонентского номера конкретному лицу, о частоте переговоров с тем или иным номером, количестве исходящих, входящих, SMS – сообщений, демонстрация данных о том в какой период времени и с кем состоялись разговоры, а также информации о геолокации. Эти приемы дополняются оперированием во время допроса второстепенными фактами, демонстрацией иных доказательств, основанных на материалах дела, но таким образом, чтобы это было как бы невзначай, например, перечисление источников, ссылка на специальные технические средства, их возможности, упоминание об имеющихся доказательствах. Создание ошибочного впечатления о степени осведомленности следователя, формирует у допрашиваемого чувство уверенности в правильности его позиции, что в разы усиливает доказательственное значение, всех сведений, при внезапном их предъявлении. Неожиданные факты об абонентских соединениях или данные о совершенно ином местонахождении допрашиваемого на момент совершения преступления могут сильно повлиять на противоборствующий следователю субъект, в результате чего у последнего теряется воля к сопротивлению, тем самым допрашиваемый полностью проигрывает следователю не только в тактическом плане, но и в психологическом и информационном соперничестве.

Тактическая внезапность нередко может послужить предпосылкой для всплеска эмоции, возмущения, а соответственно, неконтролируемого «проговора» конфликтующей стороны, что влияет на потерю ориентации в допросе и на негативную позицию допрашиваемого. Следователь может сымитировать ситуации, в которой у допрашиваемого создается ложное впечатление о его положении, у последнего будет чувство постоянного ожидания решающего

доказательства. Так, ему могут быть предъявлены детализация вызовов признавшегося в содеянном сообщника или показания с его признанием, которые подтверждаются, в том числе данными, полученными от оператора связи. Возникновение «комплекса неизвестности», как его обозначил Л.Я. Драпкин, действительно, понижает четкость и целеустремленность действий противоборствующего допрашиваемого[193].

В рамках реализации тактической операции по проверке алиби лица, при допросе нередко используются результаты следственного действия, предусмотренного статьей 186.1 УПК РФ. Данный факт подтверждает следующий пример из практики. Между Карабейниковым и его знакомым возник конфликт, в ходе которого Карабейников нанес последнему 38 ударов ножом по различным частям тела. Будучи допрошенным в качестве подозреваемого по делу Карабейников указал, что убийство не совершал, в указанный период времени в районе места происшествия не находился, с потерпевшим не встречался, по сотовой связи в день убийства с ним не созванивался, свой мобильный телефон потерял за несколько дней до случившегося. Исходя из нескольких допросов, было ясно, что Карабейников дает логичные и последовательные показания, которые также подтверждаются некоторыми свидетелями. Однако, данные детализации, полученные следователем от оператора сотовой связи, позволили установить, что Карабейников пользовался несколькими абонентскими устройствами и SIM-картами, одна из которых, исходя из информации о месторасположении приемопередающих базовых станций, была активна на момент убийства в районе места совершения преступления. Согласно детализации, все SIM-карты срабатывают в разное время в одном месте, зона действия данной вышки организации связи охватывает место жительства Карабейникова[194].

---

[193] Драпкин Л.Я. Тактика следственных действий: учебное пособие. – Екатеринбург: Уральский юридический институт МВД России. 2014. С. 52.

[194]Уголовное дело № 53043-2012 г. Архив Видновского городского суда Московской области. [Электронный ресурс]. − URL: http://rospravosudie.com.

Благодаря тактически грамотным действиям следователя, при допросе удалось создать впечатление осведомленности об обстоятельствах преступления. Следователь пошагово представлял данные детализации с информацией о местоположении, звонках с указанием даты и времени, IMEI кодов сотовых телефонных аппаратов, принадлежащих Карабейникову и сведения о SIM-картах, используемых им в своих устройствах. В результате при допросе были получены признательные показания Карабейникова.

Очевидно, что успешность производства допроса во многом зависит от осведомленности следователя и имеющихся у него фактических данных, касающихся события преступления. В совокупности с правильно выстроенной тактикой допроса, а также психологическими приемами, эффективность и результативность данного следственного действия повышается в разы. Особенно это прослеживается при производстве допроса в рамках тактической операции. Чаще всего допрос проводится в комплексе с предъявлением на опознание, очными ставками, следственным экспериментом, различными ОРМ, перечень может варьироваться в зависимости от конкретной тактической операции. Приведем еще один пример из следственной практики. Зубакин и Варенцов незаконно приобретали, использовали и распространяли программное обеспечение компании «Майкрософт», «Адоб Системс Инкорпорейтед», Корпорация «Корел», ЗАО «1С», без согласия последних. В целях сбыта в крупном размере преступники разработали план совместных действий и распределили роли. Варенцов реализуя совместный преступный план с Зубакиным, пришел по назначенному адресу, где установил на жесткий диск персонального компьютера (Далее ПК) контрафактные программные продукты для ПК. Варенцов в момент установки программных продуктов для ПК, неоднократно созванивался с Зубакиным для консультации по воспроизведению контрафактных продуктов программ для ПК на жесткий диск ПК. Где после установления программ получил денежные средства в сумме 1000 рублей, после чего был задержан сотрудниками полиции (кроме акта проведения ОРМ и видеозаписи, данный факт подтверждался детализацией вызовов Зубакина и

Варенцова). Однако Варенцов отрицал причастность к преступлению и связь с Зубакиным. Следователи не имели достаточной доказательственной базы в отношении Зубакина, руководителя преступной группой. Проделав тщательный анализ полученной детализации соединений с абонентских номеров преступников, следователем было установлено, что Зубакин действительно общался по вопросу установки контрафактных программ для ПК с Варенцовым, а также консультировал его в момент проведения ОРМ «проверочная закупка». Было также установлено, что Зубакин в одном абонентском устройстве (IMEI 353639017426709) использовал два абонентских номера, один из которых использовался по настоящее время. Кроме того, анализируя детализацию телефонных соединений телефонов Зубакина и Варенцова, был сделан однозначный вывод, что на протяжении периода времени интересующего следствие времени оба абонентского номера регулярно выходили на связь с телефона IMEI 353639017426709 – телефона Зубакина, что опять же подтверждалось детализацией. Преступники признали вину в суде, когда стало очевидно, что все их показания опровергаются данными детализации вызовов[195].

Следует также добавить, что в ряде случаев полнота доказательственной базы и других, представляющих интерес сведений, зависит именно от информации о соединениях между абонентами и (или) абонентскими устройствами. Такая информация, являясь неопровержимой, нередко может повлиять на тактику допроса, на его последовательность. Кроме того, следователь, грамотно используя данные детализации и оперируя нужными тактическими приемами, может преодолеть оказываемое противодействие, опровергнуть ложное алиби преступника и успешно получить от допрашиваемого правдивую, интересующую информацию.

От имеющихся в распоряжении следователя данных, полученных от оператора сотовой связи, нередко может зависеть организация и тактика очной ставки. В рамках указанного следственного действия проводится поочередный

---

[195] Уголовное дело № 163508. Свердловский областной суд – [Электронный ресурс]. – www.ekboblsud.ru/doc/sudpr/pr_obzor_ug.doc.

допрос, в присутствии друг друга, дух ранее допрошенных лиц из числа потерпевших, свидетелей, подозреваемых, обвиняемых, в показаниях которых имеются существенные противоречия. Присутствие при допросе другого участника преступного события затрудняет дачу ложных показаний, создает неустойчивую волевую ситуацию для конфликтующего субъекта, тем самым подводит последнего к изменению позиции на бесконфликтную. При подготовке к очной ставке изучаются данные ранее показания лиц, между которыми запланировано проведение следственного действия и иных лиц, выясняются противоречия, формулируются вопросы, их последовательность, выбор места проведения и применяемых технических средств. Очная ставка проводится при наличии у следователя достаточной совокупности доказательств для верной оценки показаний ее участников. Очевидно, что информация о соединениях между абонентами и (или) абонентскими устройствами в совокупности с другими доказательствами, может быть использована для подготовки вопросов для допрашиваемых или как косвенная или прямая улика при проведении очной ставки.

Основной этап очной ставки начинается с вызова ее участников. Следователь информирует о цели вызова и спрашивает, знакомы ли участники очной ставки друг с другом. В одном случае, участники подтверждают свое знакомство, тогда выясняется как давно, при каких обстоятельствах познакомились, есть ли неприязненные отношения друг к другу. В другом случае, оба или один из участников могут заявить о том, что не знакомы.

Имея в распоряжении доказательства об их связи друг с другом, в том числе и детализацию, свидетельствующую о неоднократных соединениях между ними, тактический алгоритм очной ставки может состоять из следующих элементов:

1. Постановка вопросов лицу, который, по мнению следствия, дает правдивые показания, с учетом всех имеющихся доказательств. Здесь можно подробно узнать о местоположении лица в определенный момент времени, о датах соединений, о том, как поддерживалась связь с других участников очной ставки, как он может подтвердить свои показания и любые другие сведения, которые

подтверждаются данными детализации. В совокупности с другими доказательствами и соответствующими вопросами это позволяет минимизировать влияние на него другого конфликтующего участника и воздействовать на последнего, располагая к изменению негативной позиции. Однако, из тактических соображений, первым рекомендуется допрашивать лицо, в показаниях которого имеются противоречия. Это обусловлено следующим: участник, который дает правдивые показания, сможет сориентироваться и, более аргументировано, опровергнуть ложные показания.

2. Соблюдение строгой, запланированной логической последовательности вопросов.

3. Максимальная детализация вопросов, связанных с датами, адресами, временем и т.п. Особенно, если эти характеристики находят подтверждение в результатах иных следственных действий, а частности получения информации о соединениях между абонентами и (или) абонентскими устройствами.

4. Поэтапная конкретизация показаний при проведении очной ставки.

5. Обращение к другим показаниям участников преступления.

6. Использование внутренних противоречий в показаниях допрашиваемого.

7. Активное использование доказательств (записи с камер видеонаблюдения, результаты экспертиз, информация об абонентах и их соединениях, аудиозаписи и т.д.).

8. Привлечение оперативных сотрудников.

9. Проведение очной ставки сразу после задержания или в рамках тактических операций.

Таким образом, как и при допросе лица в конфликтной ситуации, результаты получения информации о соединениях между абонентами и (или) абонентскими устройствами в рамках проведения очной ставки могут иметь важное значение для подготовки вопросов, конкретизации, подтверждения или опровержения показаний допрашиваемых.

Иными следственными действиями, в ходе производства которых возможны получение и анализ информации о соединениях между абонентами и (или)

абонентскими устройствами или после производства которых, необходимо проведение следственного действия, предусмотренного статьей 186.1 УПК РФ, является обыск и выемка, а также осмотр предмета – средства сотовой связи. К примеру, в результате обыска по месту жительства организатора, руководителя и активного участника организованной преступной группы - С, были обнаружены боксы из-под SIM-карт мобильных телефонов, а также иные электронные носители информации. Это способствовало доказыванию обстоятельств преступной деятельности С. по организации и консолидации, сплочению соучастников, приданию их деятельности согласованного характера, обеспечению членов преступной группы средствами связи. Являясь руководителем преступной группы, С, наряду с прочими противоправными действиями в рамках создания условий для организованной преступной деятельности, ввел элементы конспирации в деятельность преступной группы, специализирующейся на совершении экономических преступлений, связанных с обналичиванием денежных средств, непосредственно руководил деятельностью соучастников. Результаты обыска и получения информации о соединениях между абонентами и (или) абонентскими устройствами послужили доказательствами по данному уголовному делу[196].

Согласно материалам другого уголовного дела, в результате выемки у потерпевших, которыми явились родители похищенного несовершеннолетнего, в распоряжение следователя оказались компакт диски с аудиозаписью их абонентских соединений с похитителем, в ходе которых он выражал требования и угрозы расправы. Подтверждением сведений послужила детализация вызовов, с данными о местоположении и временными показателями.[197].

Предположим, что в результате обыска, проведенного как по месту жительства, так и по месту иного пребывания лица, обладающего предметами или

---

[196] Материалы уголовного дела № 4717453. Архив СЧ ГСУ при ГУ МВД Ростовской области. 2013 г

[197] Приговор по уголовному делу в отношении Брыкова В.П., обвиняемого в совершении преступлений, предусмотренных п.п. «в, д, з» ст. 126, п.п. «в, к» ч. 2 ст. 105, п. «б» ч. 3 ст. 163 УК РФ. Архив Ростовского областного суда г. Ростова-на-Дону. 2006 г.

документами, имеющими значение для расследования, или в результате личного обыска, а равно - в результате выемки по месту нахождения родственников, коллег либо иных знакомых такого лица, в распоряжении следователя оказалось средство сотовой связи.

Необходимость в получении судебного решения на изъятие путем обыска или выемки сотового телефона возникает в целом ряде случаев. Так, судебное решение, по общему правилу, требуется при производстве обыска или выемки в жилище, осмотра жилища, в случае, если лица, проживающие по данному адресу, возражают против следственного осмотра.

Вместе с тем, ч. 3 ст. 183 УПК РФ предусматривает юридические основания (в виде судебного решения, принимаемого в порядке ст. 165 УПК РФ) для производства выемки предметов и документов, содержащих охраняемую федеральным законом тайну. Сотовый телефон или иное электронное средство телекоммуникационной связи содержит не только информацию о телекоммуникационных контактах данного абонента с другими лицами, но и, при соответствующих настройках - входящие и отправленные SMS и иные сообщения. Полагаем, что вследствие провозглашенных Конституцией РФ свободы слова, тайны телефонных и иных переговоров, телеграфных и иных сообщений, сведения, отображенные в памяти сотового телефона или иного подобного носителя электронной информации, также относятся к категории охраняемой законом тайны.

Как представляется, если следователем было получено судебное решение о производстве обыска или выемки в жилище либо осмотра жилища на основании мотивированного соответствующего постановления следователя, и в результате этих следственных действий предполагалось обнаружить и изъять указанное средство связи (наряду с другими документами и предметами, имеющими значение для расследования), то, отсутствует необходимость в получении судебного решения специально на производство следственного действия, непосредственной целью которого является изъятие данного средства связи. А вот если планируется произвести выемку не по месту жительства, а по месту иного

пребывания (например, в служебном кабинете) лиц, при которых имеется средство телефонной или иной связи, имеющее значение для установления обстоятельств преступления, то, как нам представляется, следователю необходимо инициировать процесс получения судебного решения о производстве выемки предметов и документов, содержащих охраняемую законом тайну (ч. 3 ст. 183 УПК РФ). К сожалению, этот нюанс не всегда принимают во внимание на практике, осуществляя выемку сотовых телефонов или иных средств электронной связи в общем порядке, на основании лишь постановления следователя (дознавателя).

Характерно, что ч. 5 ст. 165 УПК РФ, предусматривая перечень исключительных случаев, вызванных ситуациями, не терпящими отлагательства, при которых следственные действия, требующие по общему правилу принятия судебного решения, могут быть произведены без получения такового, включает такие следственные действия, как осмотр жилища, обыск или выемка в жилище, личный обыск. А вот выемка предметов и документов, содержащих охраняемую законом тайну, в данном перечне отсутствует.

Поэтому изъятие сотового телефона или иного подобного носителя электронной информации (содержащего сведения о телекоммуникационных контактах его владельца с другими абонентами) в форме производства простой выемки, т.е. на основании постановления следователя (дознавателя) будет неправомерно даже, если субъект расследования намеревался впоследствии, в течение 24 часов с момента начала данного следственного действия, уведомить судью и прокурора.

В соответствии с п. 6 ч. 2 ст. 29 УПК РФ получение судебного решения требуется и, по общему правилу, для производства личного обыска, в ходе которого также нередко изымаются находящиеся при подозреваемому, обвиняемом электронные средства связи. Вместе с тем, ч. 2 ст. 184 УПК РФ содержит ряд исключений из вышеуказанного общего правила, допускающих производство личного обыска без вынесения соответствующего постановления (и тем более, минуя режим судебного рассмотрения). Эти исключения предусматривают:

- задержание лица или его заключение под стражу;

- наличие достаточных данных полагать, что лицо, находящееся в помещении или ином месте, в котором производится обыск, скрывает при себе предметы и документы, имеющие значение для уголовного дела.

Практика показывает, что указанные ситуации, признанные законодателем как исключительные, на самом деле носят постоянный и системный характер. Законодатель допускает возможность производства обыска в помещении, в котором в этот момент могут присутствовать самые различные лица, в т.ч. и не наделенные каким-либо уголовно-процессуальным статусом (ч. 8 ст. 182 УПК РФ). Следовательно, проведение личного обыска лица, оказавшегося в помещении, в котором осуществляется обыск, с целью изъятия имеющегося у него сотового телефона или иного электронного средства связи, содержащего информацию, имеющую значение для расследования (например, SMS, отправленную с абонентского номера или устройства, принадлежащего лицу, проходящему по уголовному делу), вполне возможно.

В соответствии с уголовно-процессуальным законом, при изъятии путем выемки или обыска электронного средства, к которому вполне возможно отнести и сотовый телефон, присутствует специалист (ч.ч. 9.1. ст. 182; 3.1 ст. 183 УПК РФ).

В то же время обнаружение сотового телефона или иного электронного средства связи возможно и в результате проведения такого следственного действия, как осмотр места происшествия, например, в случаях, если это средство связи находилось на месте происшествия при погибшем, либо оказалось случайно оброненным лицом, причастным к совершению преступления.

При осмотре места происшествия, объектом которого являлся автомобиль, принадлежащий организатору и руководителю организованной преступной группы - гр. С, находящийся на пересечении двух центральных улиц в г. Ростове-на-Дону, были изъяты, наряду с другими объектами, имеющими значение для уголовного дела, два мобильных телефона «Нокиа». В сочетании с обнаруженными путем обыска по месту жительства данного лица боксами из-под

SIM-карт, это способствовало доказыванию роли, статуса и обязанностей данного лица в организованной преступной группе.

В подобных ситуациях обнаруженное средство связи подлежит изъятию; при изъятии с места происшествия оно в обязательном порядке должно быть упаковано и опечатано для исключения возможности доступа к нему посторонних лиц, либо, напротив, лиц, имеющих определенный личный интерес к результатам расследования.

Кроме того, обнаружение сотового телефона или иного средства связи теоретически возможно на месте производства таких следственных действий, как проверка показаний на месте или следственный эксперимент. Так, в соответствии с ч. 1 ст. 194 УПК РФ, одной из целей проверки показаний на месте является установление новых обстоятельств, имеющих значение для уголовного дела. Кроме того, в рамках рабочего этапа проверки показаний на места проверяемое лицо вправе не только воспроизвести на месте обстановку и обстоятельства исследуемого события, но и указать на предметы, документы, следы, имеющие значение для уголовного дела. Показывая, например, место совершения разбойного нападения, убийства и т.п., а равно место сокрытия похищенных предметов, находившихся на жертве, подозреваемый (обвиняемый) может указать и на находящийся в данном месте сотовый телефон, принадлежавший потерпевшему. Вероятность обнаружения на месте проведения проверки показаний на месте сотового телефона, иного средства связи, а равно комплектующего устройства или иного аксессуара к средству связи (SIM -карты, паспорта от сотового телефона, иных подобных предметов или документов) усиливается, если этим местом выступает жилище лица, проходящего по уголовному делу либо его родственника или близкого лица.

Независимо от вышеизложенных процессуальных форм изъятия сотовых телефонов или иных электронных средств телекоммуникационной связи (обыск, выемка, личный обыск осмотр места происшествия и др.), изъятый носитель электронной информации подлежит осмотру, осуществляемому по правилам осмотра предметов. Проанализированные материалы уголовных дел

подтверждают, что следователи действительно осуществляют осмотр предметов, объектами которых являются мобильные телефоны, изъятые в результате осмотра места происшествия - автомобиля, принадлежащего подозреваемому, а также боксы для SIM-карт, изъятые по месту жительства этого же лица.

Осмотр указанных и подобных объектов на практике зачастую осуществляют в рамках самостоятельных следственных действий, иногда осматривают в рамках одного следственного осмотра несколько объектов, одновременно изъятых в результате производства какого-либо одного следственного действия (осмотра места происшествия, вещей, документов, обыска, выемки), к ним нередко прилагаются фототаблицы (Приложение 10)[198].

Вместе с тем, полагаем не только целесообразным, а также и весьма результативным, осуществлять осмотр группы объектов, хоть и изъятых путем производства различных следственных действий, и даже в разных местах, но структурно дополняющих друг друга в рамках функционирования единого абонентского устройства. Примерами таких объектов могут являться мобильные телефоны и различные комплектующие изделия к ним, аксессуары, подходящие именно к определенной модели телефона, а равно, упаковки (боксы) для SIM-карт. Так, последние могут содержать телефонный номер пользователя, что позволяет установить контроль в той или иной форме за информацией о соединениях между определенным абонентским устройством, а также позволяет разоблачить попытку виновных лиц инсценировать неосведомленность и непричастность к телекоммуникационным контактам соучастников.

Данный метод криминалистического анализа лишь постепенно внедряется в практическую деятельность субъектов расследования, и, как показывает эмпирический анализ, осуществляется далеко не во всех ситуациях, требующих его осуществления.

Вышесказанное свидетельствует о том, что информация о соединениях между абонентами и (или) абонентскими устройствами может быть получена не только в рамках статьи 186.1 УПК РФ, но и при производстве других

[198] Фототаблица к протоколу осмотра вещей и предметов (Приложение 10).

следственных действий, в ходе которых обнаруживается сотовый телефон, комплектующие к нему или SIM-карта. Данные предметы являются источником сведений об устройстве, об абоненте, идентификационных данных, возможно даже носителями следов пальцев рук, биологических следов. Однако, для полноты картины при обнаружении вышеуказанных предметов, необходимо получение информации о соединениях между абонентами и (или) абонентскими устройствами в целях уточнения полученной информации. Кроме того, результаты указанного следственного действия нередко могут повлиять на принятие решения о последующих следственных действий или тактику проведения некоторых из них.

§ 2. Использование результатов следственного действия, предусмотренного статьей 186.1 УПК РФ, при расследовании отдельных видов преступлений

Одной из актуальных проблем в деятельности правоохранительных органов является противодействие мошенничествам, совершенным с использованием средств сотовой связи, сети Интернет, платежных терминалов, квалифицируемым по различным частям ст. 159 УК РФ. Лицо, совершившее преступление значительное время остается вне поля зрения правоохранительных органов, в связи с чем, как правило доказать его причастность к совершенному преступлению довольно сложно.

Средства связи (сотовые телефоны) нередко становятся средством или орудием совершения преступлений, что характерно для указанного вида преступлений. С 2008 года данный вид мошенничества начал активно совершенствоваться и получил распространение на территории Российской Федерации. Среди большого многообразия мошеннических действий данный вид получил название «телефонное» мошенничество, поразив практически все регионы России. Как сообщает РИА Новости со ссылкой на заместителя начальника Главного управления уголовного розыска МВД РФ Александра Фролова, за 2016 год количество мошенничеств, в которых используются

устройства мобильной связи, выросло в 1,5 раза. Всего в России было совершено 38 тысяч преступлений мошеннического характера с использованием средств сотовой связи. Это около 22% от всех мошенничеств, совершенных в России. По сравнению с 2015 годом рост составил более 50%[199]. Согласно справочно-аналитическим материалам годовой отчетности МВД России в 2016 г. на территории Российской Федерации существенное внимание уделялось раскрытию хищений, совершенных путем мошенничества, в том числе с использованием банковских карт, средств мобильной связи, через Интернет-ресурсы. В результате принятых мер раскрыто 2,9 тыс. фактов мошенничества с использованием средств сотовой связи, выявлено 542 лица, в том числе 37 – содержащихся в учреждениях ФСИН России. Общее число мошенничеств, уголовные дела по которым направлены в суд, возросло на 1,8%[200].

Что касается регионального уровня, то, например, в производстве органов предварительного следствия и дознания ГУ МВД России по Свердловской области за 2016 год находилось 813 уголовных дел о мошенничествах, совершенных с использованием средств мобильной связи, сети Интернет, платежных терминалов. В следственных подразделениях области находилось в производстве 672 уголовных дела, направлено в суд 17 уголовных дел на 45 преступных эпизодов, 2 уголовных дела на 7 эпизодов, по которым установлены лица, совершившие преступления, переданы по территориальности (Курганская, Иркутская области)[201]. Как свидетельствует практика, определенная доля мошенничеств с использованием средств сотовой связи совершается осужденными, отбывающими наказание в исправительных учреждениях. Лица, совершающие мошенничества с использованием мобильных средств связи на территории исправительного учреждения, зачастую имеют преступный опыт, в курсе многих тактических приемов и комбинаций, которые применяются субъектами расследования при

---

[199] Российское информационное агентство. Официальный сайт. [Электронный ресурс]. -URL: http://ria.ru/society/20160321/1393862596.html (дата обращения 10.04.2017 г.)

[200] Официальный сайт Министерства внутренних дел Российской Федерации. – [Электронный ресурс]. – режим доступа: http://mvd.ru/presscenter/statistics/reports/item/804701.

[201] Официальный сайт ГУ МВД России по Свердловской области. – [Электронный ресурс]. − URL: https://66.мвд.рф.

производстве следственных действий, имеют возможность тщательно спланировать преступление, скрыть следы, заставить других лиц взять вину на себя. Так, при взаимодействии следственного подразделения и сотрудников ФКУ ИК-52 ГУФСИН России пос. Восточный Камышловского района в 2015 году раскрыты 2 преступления и направлено в суд уголовное дело № 1501268 по обвинению А. в совершении преступлений, предусмотренных ч.1 ст. 159, ч.2 ст. 159 УК РФ, который совершил преступления, находясь в местах лишения свободы. А., представляясь сотрудником сотовой компании, вводил потерпевших в заблуждении о предстоящей блокировке номера[202]. За 5 месяцев 2016 года в следственных подразделениях Свердловской области находилось в производстве 23 уголовных дела по преступлениям, совершенным неустановленными лицами, по которым получены детализации соединений абонентских номеров с привязкой к базовым станциям, расположенным в непосредственной близости к исправительным учреждениям в г. Сургут ХМАО, Новосибирской области, на территории Свердловской области[203].

Вышеперечисленное свидетельствует о тенденциях роста и расширению географии рассматриваемых преступлений, что подчеркивает необходимость совершенствования правоприменительной практики по предотвращению и эффективному расследованию данной категории уголовных дел. Основной задачей органов предварительного расследования по предупреждению мошенничеств с использованием средств сотовой связи является выявление причин и условий, способствующих совершению преступлений, принятию мер к их устранению, позитивное профилактическое воздействие на лиц с устойчивым антиобщественным поведением с целью недопущения с их стороны преступных деяний, а также предотвращение таких преступлений при строгом соблюдении законодательства РФ.

---

[202] Официальный сайт Министерства внутренних дел Российской Федерации. – [Электронный ресурс]. – режим доступа: http://mvd.ru/presscenter/statistics.

[203] Уголовное дело №1501268. Свердловский областной суд – [Электронный ресурс]. – www.ekboblsud.ru/doc/sudpr/pr_obzor_ug.doc.

Мошенничество, совершенное с использованием средств сотовой связи, характеризуется целым рядом специфических признаков (активное использование современных технических средств, изобретение новых способов криминальных действий, широкая география преступления и его последствий), объективно препятствующих процессу расследования. Рассматриваемые преступления в большинстве случаев носят латентный характер, так как многие граждане, став жертвой мошенников, и потеряв незначительную сумму денег, не обращаются с заявлением в полицию.

На сегодняшний день способы телефонных мошенничеств довольно разнообразны. Анализ материалов уголовных дел позволяет выделить наиболее распространенные формы таких преступлений:

1. Мошенник путем беспорядочного выбора различных абонентских номеров звонит или посылает SMS – сообщение потенциальному потерпевшему, представляется сотрудником банка, коммерческой организации, ведущим на радио и т.д., сообщает о выигрыше определенной денежной суммы, туристической поездки или бытовой техники. При этом мошенник отмечает необходимость соблюсти небольшую формальность − оплатить налог за «выигранный» приз (например, некоторую сумму денег за его доставку в адрес проживания «победителя») указывает абонентский номер мобильного телефона (либо номер банковской карты), на который необходимо перевести указанную сумму денежных средств. Так, Осужденный А., отбывая наказание в исправительной колонии УФСИН России по Московской области, приобрел сотовый телефон, в котором находилась SIM-карта с абонентским номером, зарегистрированным на другое лицо. 14 марта 2011 года в 14 часов 11 минут по данному сотовому телефону он позвонил на мобильный телефон с абонентским номером, зарегистрированным на гражданку К. Преступник, вводя в заблуждение и обманывая, сообщил потерпевшей, что он является диджеем радио и, что последняя выиграла в бесплатной лотерее автомобиль «БМВ» стоимостью 1 миллион рублей. Убедившись в том, что К. поверила о выигрыше автомобиля, пояснил, что ей срочно нужно перечислить налог в размере 10 тысяч рублей. для получения приза.

К. пояснила, что у нее нет такой суммы рублей, но имеется в наличии 3500 рублей, которые она может перечислить в счет уплаты налога.

Продолжая реализацию преступного умысла, осужденный А. сообщил К. номер лицевого счета, куда следует перечислить денежные средства. Потерпевшая перечислила имеющиеся у нее 3500 рублей на номер лицевого счета, названного осужденным Л.[204]

2. Мошенники при личном общении с потерпевшим просят совершить якобы очень срочный звонок. При этом аргументируют отсутствие собственного телефона тем, что он либо утерян, либо разрядился аккумулятор. В случае согласия жертвы, мошенник совершает звонки на платные номера, в результате чего денежные средства попадают на счет злоумышленников. Как правило, такие преступления носят латентный характер. Это обусловлено тем, что потерпевшему наносится незначительный ущерб, и жертвы мошенников не делают сообщений в правоохранительные органы. Если сообщения о таких преступлениях поступают, то установить злоумышленника практически невозможно, в силу того, что последние используют SIM-карты, оформленные на других лиц, краденные сотовые телефоны и по получению средств избавляются от того и другого.

3. Мошенник путем набора различных абонентских номеров звонит на мобильный телефон потерпевшего, представляясь сотрудником правоохранительных органов (инспектором ДПС, следователем, дознавателем, участковым и т.п.), сообщает заведомо ложные сведения о том, что кто-то из его родственников совершил наезд на пешехода, кражу, грабеж или разбой, нанес кому-то телесные повреждения. Пользуясь шоковым состоянием потерпевшего, указывая на срочность вопроса, мошенник предлагает решение проблемы. В большинстве случаев решение заключается в необходимости перевода некоторой денежной суммы на банковскую карту, счет, абонентский номер либо передача наличных через курьера (водитель такси или соучастник преступления) якобы для возмещения вреда «пострадавшему», чтобы тот не заявлял о случившемся в

[204] Уголовное дело № 1-16/2011. Звенигородской городской суд Московской области. – [Электронный ресурс]. – URL: http://zvenigorod.mo.sudrf.ru.

правоохранительные органы. Так, 22 марта 2010 года Н., приобрел сотовый телефон, в котором находилась SIM-карта с абонентским номером 8-920-***-**-**. Имея в пользовании сотовый телефон с абонентским номером 8-910-***-**-**, он позвонил своему знакомому И., находящемуся в г. Калуге, и предложил ему похищать денежные средства граждан, на что последний согласился. Распределив между собой преступные роли, согласно которым Н. должен будет по имеющемуся у него в пользовании сотовому телефону звонить на стационарные телефоны граждан, представляться их близким родственником, попавшим в дорожно-транспортное происшествие, и, вводя их в заблуждение, получать согласие на предоставление денежных средств для урегулирования своих проблем. И. должен будет приезжать к гражданам и забирать у них денежные средства. Участники сговора приступили к непосредственной реализации задуманного.

Н. 22.03.2010 в 13 часов 06 минут позвонил на стационарный телефон с абонентским номером 8-4842-***-***, зарегистрированный на гр. К., и сообщил, что он является ее зятем Б. и что он попал в ДТП. К. поверила, что разговаривает со своим зятем Б., Н. пояснил, что ему срочно нужны деньги в сумме 40000 рублей для возмещения ущерба по ДТП. Однако К.сказала, что у нее нет 40000 рублей, а имеется в наличии только 25000 рублей, которые она может ему передать для решения проблемы с ДТП. Н. сообщил, что сам за деньгами приехать не сможет, поэтому поручит это его знакомому.

Н. позвонил И. и сказал о том, что имел беседу с женщиной, представился ее зятем и договорился о том, что она передаст денежные средства в сумме 25000 рублей, которые И. должен будет у нее забрать. Сообщник пришел по указанному адресу, пояснив, что пришел к К. за деньгами по просьбе ее зятя Б. и получил от нее денежные средства в сумме 2500 рублей[205];

4. Мошенник совершает вызов потерпевшему, представляется сотрудником службы безопасности банка или сотовой компании, сообщает информацию о том,

---

[205] Уголовное дело № 1-128/2011. Архив Калужского районного суда Калужской области. [Электронный ресурс]. − URL: http://rospravosudie.com.

что «… с вашей карты (со счета мобильного телефона) в данный момент злоумышленники списывают денежные средства…» и предлагает провести определенный круг операций для блокировки карты, тем самым получая доступ к денежной сумме на балансе карты (счета) потерпевшего. Так, в январе 2015 года сотрудниками УМВД России по г. Челябинску совместно с коллегами из отдела «К» ГУ МВД России по Челябинской области было установлено, что на территории г. Челябинска совершен ряд мошенничеств с использованием средств мобильной связи, путем снятия денежных средств с банковских карт граждан, проживающих в Пермском крае. Установлено, что один из подозреваемых через сеть Интернет осуществлял рассылку SMS-сообщений на номера абонентов Пермского края. В них сообщалось о том, что с банковской карты абонента происходит снятие денежных средств и для его прекращения необходимо позвонить по указанному номеру. «SMS» приходило якобы с номера какого-либо банка, поэтому напуганные люди тут же перезванивали. На звонок отвечал второй из подозреваемых, который представлялся сотрудником банка и сообщал, что с банковской карты потерпевшего неизвестные в данный момент снимают деньги. Затем он просил сообщить номер банковской карты для ее блокировки. После того, как подозреваемые получали от граждан данные банковской карты и номер SMS-пароля, они осуществляли перевод денег на свой счет[206];

5. Мошенник отправляет SMS-сообщение с текстом: «У меня проблемы, позвони по … номеру, если номер не отвечает, положи на него … рублей и перезвони» или «Я в больнице, положи … рублей на этот номер».

Так, 24 апреля 2011 года осужденный М., отбывая наказание в исправительной колонии УФСИН России по Тульской области, приобрел сотовый телефон, в котором находилась SIM-карта с абонентским номером 8-910-***-**-**. С этого телефона он стал отправлять SMS-сообщения с текстом: «Мама, брось денег на этот номер, позже все объясню». В результате

[206] Официальный сайт Главного управления МВД России по Челябинской области [Электронный ресурс]. - URL: http://74.mvd.ru.

мошеннических действий М. завладел денежными средствами в размере 3650 руб[207].

Очевидно, что для выяснения обстоятельств мошеннических действий с использованием средств сотовой связи и для формирования доказательственной базы следователю необходимо использовать технические возможности оператора связи и оперативных подразделений правоохранительных органов. Для расследования могут задействоваться специалисты отдела «К» и УСТМ. Однако, одним из основных средств получения информации об абонентах и их соединениях являются следственные действия, направленные на собирание доказательств. К таким следственным действиям, результаты которых имеют важное доказательственное значение при расследовании мошенничеств, относятся получение информации о соединениях между абонентами и (или) абонентскими устройствами и контроль и запись переговоров. Однако в силу того, что преступники пользуются разными SIM-картами и телефонными аппаратами, тщательно конспирируются при совершении преступлений мошеннического характера, контроль и запись телефонных переговоров не всегда позволяет обеспечить должными доказательствами. Кроме того, с его помощью невозможно получить информацию об уже состоявшихся соединениях, что не скажешь о следственном действии, предусмотренном статьей 186.1 УПК РФ. В этом плане получение информации о соединениях между абонентами и (или) абонентскими устройствами в рамках тактических операции позволяет оперативно снабдить следователя необходимыми сведениями, которые в последующем могут использоваться не только в качестве криминалистически значимой, ориентирующей информацией, но и доказательственной базы уголовного дела.

Именно детализация вызовов и биллинговые данные послужили основным источником информации по уголовному делу № 141239119, направленному в суд СО МО МВД России «Верхнепышминский», где был осужден О. по 1 эпизоду о преступлении, предусмотренном ч.2 ст. 159 УК РФ.

---

[207] Уголовное дело № 1-264/2011. Архив Новомосковского городского суда Тульской области. [Электронный ресурс]. − URL: http://rospravosudie.com.

В ходе расследования уголовного дела установлено, что во время совершения преступления О. отбывал наказание в ФКУ ИК- 52 п. Восточный г. Камышлов Свердловской области. При помощи сотового телефона, подключенного к сети Интернет, осуществлял рассылку рекламных предложений о приобретении телекоммуникационного оборудования «Триколор ТВ». Ознакомившись с рекламным предложением, В. посредством электронной почты направил согласие О. на приобретение телекоммуникационного оборудования. О., используя незаконно находящийся у него аппарат сотовой связи, позвонил В. и путем обмана, представившись менеджером магазина «Сто антенн», похитил у В. денежные средства в сумме 26600 рублей, которые потерпевший 07.07.2014 перевел на лицевой счет банковской карты ОАО «Сбербанк России». Денежные средства получены через платежный терминал в г. Среднеуральске[208].

Не следует забывать, что преступники, совершают не одно преступление, а серию однотипных мошеннических действий. Следовательно, для оперативного реагирования, своевременного раскрытия и качественного расследования преступлений указанной категории необходима активная деятельность следственно-оперативной группы по «горячим следам», надлежащее взаимодействие между подразделениями и службами органов внутренних дел в ходе расследования, а также создание специализированных следственно-оперативных групп для расследования дел указанной категории. При поступлении сообщения о совершении мошенничеств с использованием средств сотовой связи особенно значимым представляется организация взаимодействия следователя и оперативных сотрудников их совместный алгоритм действий.

На первоначальном этапе расследования необходимо тщательно и подробно допросить потерпевшего, узнать как больше нюансов произошедшего. Сложности при допросе возникают в случае, когда жертвами преступников выступают люди пожилого возраста. В силу возраста им тяжело вспоминать приметы преступника, сам процесс и момент совершения преступных действий в отношении них. В ходе

[208] Материалы уголовного дела № 141239119 по обвинению О. [Электронный ресурс]. − URL: http://rospravosudie.com.

допроса выясняется: способ мошенничества, дата, время и продолжительность телефонного звонка, местонахождение потерпевшего во время разговора с мошенником, все детали разговора, особенности речи и голоса мошенника.

Как уже упоминалось, существенная роль при расследовании и раскрытии рассматриваемых преступлений принадлежит совместной тщательно спланированной работе следственных и оперативных подразделений. Одновременно со следователем оперативные сотрудники устанавливают свидетелей, соучастников преступления, например, курьеров, таксистов или иных содействующих преступникам лиц. Следователь, используя результаты получения информации об абонентах и (или) абонентских устройствах сопоставляет известные факты с детализацией вызовов потерпевшего. Путем анализа биллинговых данных предпринимаются попытки установления местонахождения преступника. Установив район и точное время вызова, необходимо установить наличие камер видеонаблюдения или возможных свидетелей. При содействии УСТМ МВД России проводиться сопоставление абонентских номеров и кодов IMEI устройств сотовой связи на предмет совпадения в контактах абонентов, чему способствуют программы, позволяющие проводить такое сопоставление в автоматическом режиме[209]. В основу доказательственной базы по рассматриваемым преступлениям могут лечь и результаты выемки (обыска) сотовых телефонов, которые должным образом осматриваются, а затем признаются вещественным доказательством и приобщается к материалам уголовного дела. Такое доказательство определенно играет существенную роль для подтверждения причастности лица к совершению преступления. Еще одним важным действием следователя является получение в отделениях Сбербанка России и иных банковских учреждениях сведения о номерах счетов, на которые потерпевшими осуществлялись денежные переводы, а также данные о лицах, их получивших.

---

[209] Проблемы расследования преступлений, связанных с мошенническими действия, совершенных с использованием средств сотовой телефонной связи / Т.В. Астишина, Е.В. Маркелова. Вестник Казанского Юридического института МВД России. Выпуск 2(16) 2014. С. 97.

Таким образом, даже если, удается задержать преступника «по горячим следам» еще не прибегая к производству следственного действия, предусмотренного статьей 186.1 УПК РФ, то его проведение необходимо на последующем этапе для подтверждения или опровержения показания подозреваемого, иных обстоятельств дела. Получение информации о соединениях между абонентами и (или) абонентскими устройствами является самым востребованным из следственных действий, проводимых при расследовании мошеннических действий с использованием средств сотовой связи, так как именно путем его производства следователь обеспечивается необходимыми неопровержимыми доказательствами.

Результаты следственного действия, предусмотренного статьей 186.1 УПК РФ, в совокупности с другими доказательствами, представляют важное значение не только для раскрытия и расследования преступлений указанной выше категории, но и других преступных посягательств. К примеру, рассматриваемое следственное действие будет неотъемлемой частью алгоритма действий следователя при расследовании хищений средств сотовой связи.

Постоянный рост потребительского спроса на услуги связи в Российской Федерации, а также достижения научно-технического прогресса привели к тому, что сотовая связь стала одной из наиболее динамично развивающихся отраслей инфраструктуры современного общества[210]. Так, если в 1997 г. было продано всего 200 тыс. сотовых телефонов[211], то за 2016. объем продаж достиг 26,4 млн. аппаратов, что на 4,4% больше 2015 года и на 1% больше 2014[212]. Как мы уже отметили, на сегодняшний день из преступлений, связанных с мобильными технологиями, наиболее распространенными являются телефонные мошенничества. Однако с момента начала популяризации средств сотовой связи было отмечено появление преступлений, связанных с их хищениями.

---

[210] Ударцев С.Ю. Раскрытие хищений средств сотовой связи подразделениями уголовного розыска: автореф. дис. … канд. юрид. наук. Омск, 2008. С. 3.

[211] Аналитический обзор рынка продаж мобильных телефонов. – [Электронный ресурс]. – URL: http://www.sostav.ru/news.

[212] Обзор цифровой трансформации, телекоммуникаций, вещания и ИТ. - [Электронный ресурс]. – URL: http://www.comnews.ru/node.

Несмотря на то, что с 2006 г. в стране зафиксировано снижение преступности (с 3 855,3 тыс. преступлений в 2006 г. до 2352,1 тыс. в 2015, 2160 тыс. в 2016 и 1551,6 тыс. за январь-сентябрь 2017 г.) почти половину всех общественно опасных деяний стабильно занимают хищения (46% в 2015 г., 43,3% в 2016г., 51,5% в январе-сентябре 2017 г.)[213]. Причем соразмерно темпам роста числа имеющихся в пользовании сотовых телефонов (смартфонов) увеличивалось и количество их хищений, что подтверждает и анализ указанных преступных деяний. В структуре всей преступности хищения мобильных телефонных аппаратов, как показал анализ данных уголовной статистики по ряду субъектов РФ, составляют от 9,8% до 20,5%, а в структуре хищений – от 22,6% до 30,5%7[214]. В то же время статистика фиксирует стабильное падение раскрываемости данного вида преступлений начиная с 2007 г. При этом в 2012 г. раскрываемость в РФ снизилась на 10,8%[215].

Именно данный вид преступлений, связанный с мобильными телефонами предшествовал мобильному мошенничеству в том виде, в котором оно распространено сейчас. Если сейчас мобильный телефон чаще выступает в качестве орудия или средства совершения корыстных преступлений, то около 5 лет назад сотовый телефон в первую очередь был предметом преступного посягательства. Тем не менее, статистика показывает, что хищения средств сотовой связи имеют место в структуре преступности и сейчас. Хотя и очевиден спад уровня хищений сотовых телефонов. в 2016 году половину всех зарегистрированных преступлений (43,3% %) составляют хищения чужого имущества: кражи — 996,5 тыс., грабежи — 71,1 тыс., разбои — 13,4 тыс. При этом из всего объема указанной категории преступлений, хищения мобильных телефонов составили 28%, из которых: кражи – 57%, грабежи – 27%, мошенничества – 11%, разбои – 3,5%. Например, наибольшее число таковых

---

[213] Официальный сайт Министерства внутренних дел Российской Федерации. – [Электронный ресурс]. – режим доступа: http://mvd.ru/presscenter/statistics/reports/item/show.
[214] Ковальчук Р.С. Хищение мобильных телефонных аппаратов // URL: http://www.nbpublish.com
[215] Официальный сайт Министерства внутренних дел Российской Федерации. – [Электронный ресурс]. – режим доступа: http://mvd.ru/presscenter/statistics/reports/item/show

фиксируется в Республике Татарстан (их доля составила 40%), в Свердловской области и Пермском крае – 30%, в городе Москве – 25%, в городе Санкт-Петербурге и Ленинградской области – 22%[216].

Снижению уровня указанных преступлений способствовало не только акцентирование работы правоохранительных органов в данном направлении, но и нововведения в законодательство Российской Федерации, в том числе и новая статья УПК РФ «Получение информации о соединениях между абонентами и (или) абонентскими устройствами». Возможности данного следственного действия во многом облегчили работу следователей по расследованию и раскрытию указанной категории преступлений и в положительную сторону повлияли на статистику преступности в России в части посягательств на мобильные телефоны граждан. Если до 2010 года до введения новой нормы количество преступлений, предметом преступного посягательства которых являлись сотовые телефоны в России, было в 2010 – 323 673, то после введения нового следственного действия в 2011 – 260 600, в 2012 – 224 703, а 2016 – менее 200 тысяч преступлений[217].

Отметим, что схожие возможности имеет такое оперативно-розыскное мероприятие как получение компьютерной информации, однако оно допустимо только при наличии информации о признаках подготавливаемого, совершаемого или совершения иного противоправного деяния, по которому предварительное следствие обязательно. Таким образом, получение компьютерной информации не производится по основным составам кражи, мошенничества и грабежа, подследственных дознанию. В данном случае оперативные сотрудники и сотрудники подразделений дознания имеют право работать только по поручениям уполномоченных лиц. В связи с этим, получить сведения об абонентах и их соединениях возможно следующими способами:

---

[216] Обзор состояния преступности в России за 2016 год [Электронный ресурс].-URL https://mvd.ru/folder/101762/item/7755683/(дата обращения 18.05.2017 г.).
[217] Там же. URL: https://mvd.ru/folder/101762/item/7755683.

1. Владелец телефона сам предоставляет выписку своих соединений, которую можно получить в личном кабинете абонента[218].

Как нами отмечалось, данный способ возможен только в бесконфликтной ситуации.

2. Выемка. Это следственное действие производится по судебному решению и только, если точно известно, где и у кого находится искомые предмете или документы.

3. Получение информации о соединениях между абонентами и (или) абонентскими устройствами. Процедуру данного следственного действия также осложняет необходимость получения судебного решения для его производства. Однако в отличие от двух предыдущих способов других ограничений в его возможностях нет. Поэтому оно производится следователями (дознавателями) в большинстве случаев, что подтверждается результатами анкетирования (94,6% проводят следственное действие, предусмотренное статьей 186.1 УПК РФ для получения биллинговой информации)[219].

Обозначенный выше вопрос о получении сведений об абонентах и (или) абонентских устройствах оперуполномоченными и сотрудниками дознания только по поручению по возбужденным уголовным делам, требует особого внимания, так как по своей сути ограничивает правомочия указанных лиц в средствах проверки сообщения о преступлений, связанных с хищениями сотовых телефонов, что нередко сказывается на оперативности и качестве их раскрытия. Но, так как изменений решающих данную проблему до сих пор внесено в действующее законодательство не было, мы рассмотрим некоторые особенности получения сведений об абонентах и их соединениях при расследовании хищений средств сотовой связи в современных условиях.

Проверка сообщения о хищении сотового телефона следующие действия следователя, дознавателя:

---

[218] Одна из услуг предоставляемых операторами сотовой связи

[219] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

- допрос (заявителя; свидетеля; задержанного; лиц, задержавших нарушителя; приобретателя похищенного сотового телефона);

- истребование документов (от потерпевшего - чеки, коробку, другие бумаги, содержащие идентификационные признаки похищенного устройства; от оператора связи – договор о предоставлении услуг);

- поручение органу дознания о проведении оперативно-розыскных мероприятий по установлению лица, совершившего преступление, очевидцев, местонахождения похищенного (наведение справок, опрос);

- осмотр места происшествия, предметов и документов, имеющих отношение к похищенному имуществу;

- освидетельствование (например, если было применено насилие при хищении, в частности, шнурком к которому прикреплен сотовый телефон для ношения его на шее);

- выемка (например, следов пальцев рук, документы на похищенный телефонный аппарат, видео, фото с камер видеонаблюдения и др.).

Сотрудники подразделений уголовного розыска в ходе доследственной проверки вправе передавать по информационному каналу оператору связи, который должен ввести данные об идентификационном номере мобильного средства связи, в программную базу данных. Программная база данных срабатывает на: 1) соединение мобильного средства связи с другими абонентами телефонной сети; 2) повторную регистрацию средства связи у оператора связи с установкой новой SIM-карты на мобильный телефон; 3) включение мобильного телефона с «чужой» SIM-картой и его идентификацию как похищенного.

При этом информацией о «срабатывании» системы на похищенное мобильное средство связи владеет лишь лицо, обслуживающее программу. Оператор связи обязан немедленно передать по каналу связи оперуполномоченному полученную информацию о выявлении похищенного мобильного средства связи. Причем полную информацию об абонентских соединениях и абоненте, пользующемся похищенным мобильным средством связи, оператор связи может передать только при наличии судебного решения в

рамках возбужденного уголовного дела[220]. Организация, оказывающая услуги по мобильной связи, на основании п. 3 ст. 46 и ст. 64 Закона о связи, предоставит инициатору запроса только исходящие абонентские номера (данные о модели и идентификационном номере) без предоставления данных об абоненте (ФИО, название предприятия, учреждения, организации, адреса). Кроме того, оперативные сотрудники принимают меры по проведению «биллинга» исходящих мобильных соединений с похищенного средства связи, установлению номера абонентов соединений, адреса, данные о личности (организации, предприятии и др.), а также проверяют указанных абонентов на причастность к преступлению.

При проверке сообщения о хищении средств сотовой связи, как правило, складываются следующие общие следственные ситуации:

- лицо, совершившее преступление не известно и нет информации о нем и очевидцах;

- лицо, совершившее преступление не известно, но есть очевидцы преступления;

- лицо, совершившее преступление задержано «по горячим следам».

Расследование хищений средств сотовой связи на первоначальном этапе напрямую зависит от сложившейся следственной ситуации (от времени, прошедшего с момента хищения, проведения осмотра места происшествия, обнаружения следов преступления, предмета посягательства, от поведения виновных, потерпевших, свидетелей и т.п.)[221].

Однако в любой из сложившейся следственной ситуации следователь включает в перечень необходимых следственных действий получение информации о соединениях между абонентами и (или) абонентскими устройствами. Различными будут цели данного следственного действия и его место в структуре проводимых следователем тактических операций. В одном

---

[220] Методические рекомендации по расследованию уголовных дел по преступлениям, связанным с различными формами хищения мобильных средств связи, находящихся в частной собственности граждан, предприятий, организаций, учреждений и др. Пермский областной суд // URL: http://perm.newsity.info/docs/sistemst.

[221] Белкин Р.С. Криминалистика: учебник. М., 2008. С. 727; Филиппов А.Г. Криминалистика: учебник. М., 2008. С. 527; Криминалистика: учебник / под ред. Е.П. Ищенко. М., 2000. С. 568.

случае, цель будет установление местонахождения похищенного имущества, подозреваемого или лица, владеющего в настоящий момент похищенным сотовым телефонов, в другом – установление обстоятельств дела, получение криминалистически значимой и доказательственной информации.

Ситуация 1. Лицо, совершившее хищение, задержано с поличным.

Основными задачами расследования в этой ситуации сводится к закреплению доказательств виновности лица. Соответственно все следственные действия и организационные мероприятия будут направлены на собирание доказательств вины подозреваемого.

Алгоритм следственных действий представляется нам следующим образом:

- осмотр места хищения;
- допрос потерпевшего и свидетелей-очевидцев;
- личный обыск подозреваемого;
- обыск по месту жительства подозреваемого;
- освидетельствование подозреваемого;
- осмотр одежды подозреваемого;
- осмотр изъятых у подозреваемого вещей и предметов (в частности похищенного сотового телефона);
- предъявление потерпевшему для опознания изъятых у подозреваемого вещей и предметов;
- проведение очной ставки – в частности, по карманным кражам (например, между подозреваемым и лицами, его задержавшими).

В данный алгоритм мы добавим подготовку и направление ходатайства в суд о получении информации о соединениях между абонентами и (или) абонентскими устройствами и соответственно само производство указанного следственного действия, так как в дальнейшем полученная детализация и биллинговые данные, будут представлять доказательства местонахождения лица в определенном месте, в определенный промежуток времени. С этой же целью органу дознания может быть поручено проверку интересующих абонентских номер из детализации

вызовов потерпевшего, проверка установленных лиц на причастность к совершению преступления.

Ситуация 2. Сведения о лице, совершившем хищение, имеются, но он не задержан.

Данная ситуация может сложиться, когда потерпевшие высказывают предположение о совершении хищения каким-либо лицом. Нередко, анализируя обстоятельства, предшествующие хищению, поведение своих знакомых, потерпевшие начинают кого-либо подозревать. Проверка указанных потерпевшими лиц способствует установлению виновного. Сведения о лице, совершившем хищение, могут быть получены при проверке по криминалистическим учетам и при проведении оперативно-розыскных мероприятий. После возбуждения уголовного дела, в перечень обязательных мероприятий добавляется получение информации о соединениях между абонентами и (или) абонентскими устройствами.

Основные задачи – задержание виновного и обнаружение похищенного имущества.

Организационные мероприятия:

- розыск лица, совершившего преступление (ориентировки в другие территориальные ОВД и т.п.);

- задержание «по горячим следам»;

- розыск похищенного имущества (перекрытие возможных мест сбыта, постановка номерных вещей на учет);

- установление свидетелей (из числа работников рынков, ломбардов и других мест, где сбывалось похищенное).

- установление IMEI кода устройства и других индентификационных признаков похищенного;

- выяснение сведений о SIM-карте, с которой устройство было похищено.

Если две последние задачи не были реализованы до возбуждения уголовного дела, то указанные обстоятельства получает следователь в ходе следственного действия, предусмотренного статьей 186.1 УПК РФ.

Ситуация 3. Сведения о лице, совершившем хищение, отсутствуют Основная задача – установление виновного и обнаружение похищенного.

Для этого проводятся организационные мероприятия:

- проверка учетов по способу совершения хищения;

- проверка по дактилоскопическому учету;

- установление свидетелей преступных действий (в частности, органом дознания по поручению следователя).

Для наиболее эффективного поиска преступника в рассматриваемой ситуации выдвигают версии о лице, совершившем хищение, которые основываются на первоначально собранном материале. Наиболее типичными являются следственные версии о том, что хищение совершили:

- ранее судимые за аналогичные преступления;

- несовершеннолетние;

- ранее совершавшие хищения аналогичным способом;

- не имеющие постоянного места жительства и работы;

- злоупотребляющие спиртными напитками и наркотиками;

- знакомые потерпевшего.

Для проверки данных версий проводятся мероприятия:

- информирование всего личного состава ОВД о совершении хищения и приметах похищенного средства мобильной связи;

- сведения о похищенных средствах мобильной связи ставятся на учет в Информационный центр ОВД по субъекту РФ, а также передаются в дежурную часть для обеспечения возможности проведения проверки предметов и вещей, находящихся у доставленных к ним за совершение преступлений или административных нарушений;

- принимаются меры к перекрытию возможных мест появления преступника и сбыта похищенного, для чего необходимо организовать наблюдение в местах возможного появления преступника, проверку возможных мест хранения и сбыта похищенного, в первую очередь, на вокзалах, рынках, киосках, специализированных ремонтных мастерских, ломбардах и др.

Планирование на первоначальном этапе расследования хищений средств мобильной связи имеет две важные задачи: тактическую и стратегическую[222].

Главная тактическая задача состоит в установлении личности преступника и его розыске (если виновное лицо известно). Стратегическая задача заключается в создании исходной базы для всего дальнейшего расследования, в обеспечении его доказательственным и поисковым материалом, то есть в исследовании всех обстоятельств, подлежащих доказыванию по уголовному делу.

Решение двух задач – установления лица и доказывания его виновности – должно происходить одновременно на всех этапах деятельности по раскрытию и расследованию преступлений. Анализ уголовных дел свидетельствует, что на практике между следователями и оперативными работниками происходит временное разделение решения перечисленных задач. В первую очередь это относится к преступлениям совершенным в условиях неочевидности, и наиболее характерно для первоначального этапа их расследования. Подавляющее число следственных действий и оперативно-розыскных мероприятий, проводимых следователями и оперативными работниками, направлено на установление лиц, причастных к преступлению. На первоначальном этапе расследования планирование должно обеспечиваться, с одной стороны, быстротой проведения каждого следственного действия, с другой – соблюдением качества, полноты и объективности в расследовании[223]. В этих условиях следователю необходимо предусмотреть использование при производстве следственных действий (начиная с осмотра места происшествия) возможностей других участников следственно - оперативной группы и в первую очередь – оперативных работников, участкового уполномоченного полиции.

Чем меньше времени пройдет с момента совершения преступления до момента начала расследования, тем больше реальных возможностей его раскрыть и изобличить преступника. Однако, несмотря на очевидность этого положения, на

---

[222] Лавров В.П. Расследование преступлений по горячим следам: учебно-практическое пособие / В.П. Лавров. – Москва, 1989. С. 44-45.

[223] Мозяков В.В. Руководство для следователей / под ред. В.В. Мозякова. – Москва, 2005. С. 166–170.

практике оно реализуется редко. В результате имеет место возбуждение уголовных дел по фактам хищений не сразу, как только они становятся известными правоохранительным органам, а спустя длительное время. В связи с этим, утрачивается возможность установления преступника «по горячим следам» и соответственно усложняется поиск похищенного. Оперативные сотрудники на данный момент действуют уже по поручению следователя и не могут самостоятельно с помощью оперативно-розыскных мероприятий получить сведения об абонентах и абонентских устройствах. Данная информация предоставляется в ходе производства следственного действия, предусмотренного статьей 186.1 УПК РФ, для установления местонахождения похищенного средства связи, в целях проверки абонентской активности похищенного сотового телефона с другими SIM-картами. Данное следственное действие также позволяет отследить последние местонахождение устройства перед его отключением. Географическое положение позволяет нам установить возможных очевидцев, наличие видеонаблюдения на участке местности, что сужает границы поиска как лица совершившего похищение средства связи, так и предмета посягательства.

При расследовании таких преступлений, как хищения сотовых телефонов, у следователей возникают затруднения, обусловленные необходимостью вторжения в сферу охраняемых законом прав – тайну связи.

Способы получения информации о месте нахождения похищенного мобильного телефона:

1) получение от потерпевшего детализации входящих и исходящих соединений с указанием входящих и исходящих звонков с SIM-карты похищенного мобильного телефона.

При этом способе не нарушается тайна связи, поскольку указанная информация должна быть предоставлена оператором пользователю услугами связи (ч. 4 ст. 63 Федерального Закона «О Связи»)[224]. Однако у потерпевшего не всегда есть возможность выполнить такое требование (командировка, отпуск и

[224] О связи: федеральный закон от 07.07.2003 № 126-ФЗ. (действующая редакция). – [Электронный ресурс]. − URL: http:// www.consultant.ru.

пр.). Кроме того, нередко потерпевший и собственник телефона – разные люди (например, при купле-продаже мобильного телефона без надлежащего оформления). В этом случае он не имеет права на получение информации у оператора связи;

2) получение необходимой информации у оператора связи органами, осуществляющими оперативно-розыскную деятельность (ч.ч. 1 и 2 ст. 64 Федерального закона «О связи»)[225];

3) истребование по решению суда документов, содержащих информацию о входящих и исходящих звонках с похищенного мобильного телефона.

Документом в данном случае в соответствии с ч. 2 ст. 84 УПК РФ могут быть как бумажные, так и иные носители информации, содержащие сведения о входящих и исходящих звонках с похищенного мобильного телефона. Особенностью истребования таких документов является также вторжение в охраняемую законом сферу – тайну связи, поэтому по аналогии с выемкой документов, содержащих информацию о государственной и иной охраняемой законом связи.

В системе GSM идентификационные номера хранятся в специально созданной базе данных – Регистре идентификации оборудования EIR. Ресурсы этой базы используются для подтверждения подлинности используемого идентификационного номера мобильного телефона.

Нами уже упоминались программные комплексы, позволяющие устанавливать информацию об абонентах, абонентских устройствах и их местоположении, однако рассмотрим этот вопрос подробнее применительно к расследованию хищений средств сотовой связи.

Анализ концепций и условий построения сетей мобильной связи, а также аппаратно-программных комплексов, обеспечивающих их функционирование, позволяет сделать вывод об их очевидной значимости при использовании в криминалистических целях, в частности для определения местоположения лица,

---

[225] О связи: федеральный закон от 07.07.2003 № 126-ФЗ. (действующая редакция). – [Электронный ресурс]. − URL: http:// www.consultant.ru.

представляющего оперативный интерес. В частности, к одной из разновидностей электронного оперативного наблюдения можно отнести позиционирование абонентов сотовой связи с помощью стандартных или специализированных программно – аппаратных комплексов систем сотовой связи – «системы позиционирования мобильных абонентов».

Под системами позиционирования мобильных абонентов понимается совокупность средств радиомониторинга (оператора мобильной связи, специализированных подразделений правоохранительных органов и т.д.) пространственного положения, координат и характеристик динамики движения излучающего объекта в пределах зоны покрытия мобильной связи, с целью идентификации мобильного телефона на местности, определения его местонахождения и миграции и зоны миграции.

В целях позиционирования абонентов используются как стандартные средства мобильной связи, так и специализированные программно-аппаратные комплексы. Использование стандартного оборудования мобильной связи – базовых станций и мобильных терминалов с целью определения соты, в которой абонент находится, основывается на так называемом однозоновом методе (Cell Geographic Identification, CGI). В нем используется уникальный идентификатор соты – Cell ID и географические координаты ее центра (базовой станции), радиус соты, которые точно известны. Значение Cell ID постоянно находится в памяти мобильного телефона. При переходе из соты в соту это значение обновляется. В крупных городах размер соты минимальный, и точность метода может быть порядка 150 м. В пригородных и сельских районах плотность установки базовых станций ниже, поэтому и точность метода значительно меньше (до 35 км). Тем самым погрешность нахождения места таким способом может доходить до 30–35 км. Специализированные системы, определяющие местоположение абонента, построены на основе методов классической пеленгации (дальномерный, угломерный и разностно-дальномерный) и триангуляции, использующих как

сигналы мобильных сетей, так и спутниковой системы GPS[226]. При использовании сигналов системы GPS точность определения местоположения составляет 10–15 м, а в ряде случаев достигается точность 2–5 м. Однако общеизвестны и недостатки этого метода. Во-первых, высокая точность измерения возможна только на открытых пространствах: GPS-приемник должен «видеть» как минимум 3–4 спутника. В городах с высотной застройкой, а тем более в зданиях система GPS неработоспособна. Во-вторых, терминалы с GPS-приемником дорогие. Кроме того, наличие GPS-приемника ухудшает массогабаритные и энергетические показатели мобильных терминалов[227].

Рассматривая вопрос о криминалистическом и доказательственном значении сведений, получаемых с помощью следственного действия, предусмотренного статьей 186.1 УПК РФ, мы приходим к выводу о том, что повсеместное использование средств сотовой связи[228] позволяет применять его при расследовании любой категории уголовных дел[229]. Это обуславливает необходимость рассмотрения криминалистического и доказательственного значения результатов данного следственного действия не только для раскрытия и расследования хищений средств сотовой связи и мошеннических действий, связанных с использованием сотовых телефонов, но и других преступлений.

Представляется интересным, насколько информативными являются сведения, получаемые в ходе производства следственного действия, предусмотренного статьей 186.1 УПК РФ, при расследовании преступлений, связанных с незаконным оборотом наркотических средств.

Получение информации о соединениях, происходивших на момент совершения преступления, позволяет установить примерный круг лиц,

---

[226] Семенов Г.В. Расследование преступлений в сфере мобильных телекоммуникаций. М., 2008. С. 230–232.

[227] Сравнительное описание методов определения местоположения мобильных терминалов. URL: http://www.mobilecomm.ru.

[228] Исходя из данных федеральной службы государственной статистики, из 1000 человек населения в 2015 году 1938 являются абонентами сотовых мобильных телефонных сетей. Это значит, что практический каждый человек имеет либо две и более SIM-карты либо два и более абонентских устройства.

[229] См.: Обзор данных о результатах анкетирования практических сотрудников (Приложение 1).

причастных к совершению преступления, установить точное время и место отдельных юридически значимых действий, составляющих объективную сторону состава преступления. Так, например, по делам о незаконном обороте наркотических средств приобретатель наркотиков, как правило, договаривается посредством сотовой связи о встрече в определенное время со сбытчиком наркотиков. Информация о соединениях между покупателем и сбытчиком наряду с другими доказательствами позволяет ограничить определенными рамками событие преступления. Очевидно, что процесс передачи наркотического средства проходит после телефонного разговора, а данные геопозиционирования указанных лиц в момент соединения, с учетом привязки используемых преступниками телефонов, свидетельствуют о точном месте совершения преступления. В результате у следователя появляется возможность существенно конкретизировать формулировку обвинения. Так, по уголовному делу в отношении организованного преступного сообщества под руководством А. установлено, что лицо таджикской национальности С. по указанию лидера (зафиксировано ОРМ «Прослушивание телефонных переговоров», подтверждается данными детализации вызовов) осуществляло закладку в тайники наркотического средства – героина по 200 грамм для неизвестных ему соучастников русской национальности, которые в свою очередь в последующем оставляли данные закладки по 5 грамм для покупателей, сообщая место руководителю преступного сообщества по телефону (зафиксировано ОРМ «Прослушивание телефонных переговоров», подтверждается данными детализации вызовов. В ходе проверки показаний на месте С. указал место получения и передачи наркотиков, которое совпало с местами, указанными другими соучастниками. Данные доказательства субъективного характера подтвердились доказательствами объективного характера, зафиксированными детализациями телефонных соединений с совпадением адресов расположения базовых станций сотовых телефонов, изъятых у обвиняемых[230]. Таким образом, установлено место и время передачи наркотика

[230] Уголовное дело № 20131602. Соликамский городской суд Пермского края. – [Электронный ресурс]. – URL: http://solikam.perm.sudrf.ru/

одного соучастника преступной группы другому, а, соответственно, участие конкретных лиц в совершении преступления.

В другом случае требуется доказать связь обвиняемого и других участников, связанных с совершением преступления. Такая необходимость возникает, когда обвиняемый отрицает существование этой связи. Возникают такие ситуации, например, при проведении оперативно-розыскных мероприятий, направленных на выявление лиц, занимающихся сбытом наркотических средств (к примеру, при проверочной закупке). Оперативные сотрудники используя, в целях реализации информации о причастности того или иного лица к преступлению, предлагают ему продать запрещенные предметы или вещества. Переговоры, как правило, ведутся длительное время посредством сотовой связи, обсуждаются условия сделки, назначается дата и время. Установление фактов абонентских соединений, времени и продолжительности переговоров позволяют доказать важные обстоятельства дела. Приведем пример, Кобляков М.А. с целью последующего незаконного сбыта незаконно хранил при себе наркотическое средство. Добровольно участвующий в оперативно-розыскном мероприятии «Проверочная закупка» под псевдонимом Н., заведомо зная, что у Коблякова М.А. можно незаконно приобрести наркотическое средство - героин, в ходе телефонного разговора с Кобляковым М.А. попросил продать наркотическое средств. Согласно договоренности Н. встретился с Кобляковым М.А., и передал последнему деньги в сумме 3000 рублей. Кобляков М.А. в свою очередь Н. передал три свёртка героином. После чего подозреваемый был задержан. Одним из доказательств по делу являлась детализация, которая подтверждала сеансы связи с подозреваемого с Н., и отражала точное время телефонных звонков Коблякова[231].

По другому уголовному делу Устюгов С.М. занимался незаконной продажей наркотических средств. А., с целью приобретения наркотических средств созвонился посредством сотовой связи с Устюговым и договорился о приобретении у него наркотического средства, на сумму 1400 рублей. После чего,

[231] Уголовное дело № 20144352. Соликамский городской суд Пермского края. – [Электронный ресурс]. – URL: http://solikam.perm.sudrf.ru/

в этот же день А. через платежный терминал, перечислил, посредством услуги «Мобильный кошелек», на указанный Устюговым номер платежной карты личные денежные средства в сумме 1400 рублей, предназначенные для приобретения наркотических средств. После чего Устюгов, удостоверившись в поступлении денежных средств, посредством сотовой связи, сообщил А. местонахождение заранее обусловленного тайника – «закладки» с наркотическим средством. Будучи задержанным сотрудниками оперативных подразделений А. пояснил, что договорился о сделке со сбытчиком за несколько дней, с ним не знаком и никогда его не видел, связывался по сотовому телефону, а забирал «товар» в условленном месте[232]. Доказывание вины Устюгова было затруднительным, поскольку его действий приобретатели не видели. В связи с этим, важным доказательством послужили детализация позволившая установить зарегистрированные на Устюгова SIM-карты, а также иные сведения об абонентских соединениях с лицами, которым он сбывал наркотики. Справедливо заметить, что вариант с успешным установлением сбытчика возможен только при обстоятельстве, что абонентский номер, зарегистрирован именно на него. В ином случае установить лицо, осуществляющего дистанционную продажу, наркотиков редко представляется возможным.

Результаты получения информации о соединениях между абонентами и (или) абонентскими устройствами выступают важным доказательством и источником ориентирующей информации, когда преступление совершенно группой лиц, соучастники которой на протяжении длительного времени осуществляют подготовку и планирование преступления, в том числе посредством общения по сотовым телефонам. Информация о фактах переговоров таких лиц позволяет полнее установить состав соучастников, их местонахождение и даже занимаемую роль в преступной группе. Аналогично, при совершении обвиняемым длящегося преступления, когда деяния преступника растянуты во времени. Также с помощью информации о соединениях между абонентами можно установить

[232]Приговор Октябрьского районного суд г.Уфа Республики Башкортостан по уголовному делу 1-204/2015.

факт нахождения лица, пользующегося абонентским устройством на определенной ограниченной территории. Например, по находившемуся в производстве следственной части ГУ МВД России по УрФО по уголовному делу по обвинению ряда лиц в совершении налоговых преступлений, обвиняемые утверждали, что никогда не были в городах Курганской области, где подавались налоговые декларации с искаженными сведениями. Вместе с тем в ходе следствия были установлены многочисленные случаи, когда зарегистрированные на обвиняемых абонентские устройства обслуживались базовыми станциями в соответствующих населенных пунктах Курганской области. Данное обстоятельство в совокупности с тем фактом, что, судя по зафиксированным вызовам и иным материалам уголовного дела, переговоры по указанным абонентским устройствам в период совершения преступлений велись именно обвиняемыми, послужило доказательством причастности данных лиц к совершению преступлений[233]. По другому уголовному делу Л. обвинялся в фальсификации доказательств по гражданскому делу (протокола внеочередного общего собрания участников акционерного общества, отчета об итогах голосования), которые представил в органы федеральной налоговой службы и арбитражный суд, с целью незаконного захвата управления в акционерном обществе. Л. свою вину в предъявленном обвинении не признал, пояснив, что не находился в зданиях, где изготавливались поддельные документы. Однако, анализ соединений абонентского номера Л. позволил по привязкам к базовым станция опровергнуть показания обвиняемого[234]. Как отмечено в юридической литературе, информация о соединениях между абонентами часто запрашивается по делам о ДТП, для проверки факта нахождения тех или иных лиц на месте происшествия[235]. Так, сведения об абонентах и местоположении абонентских устройств являются основополагающими в доказательстве причастности и вины водителя,

---

[233] Уголовное дело № 121034003. 2011 год // Архив СЧ ГУ МВД России по Уральскому Федеральному округу.

[234] Дело №1-9/2013. Приговор Кировского районного суда г. Уфы от 8 февраля 2013 г. // Архив Кировского районного суда г. Уфы.

[235] Куприянов А.А. Суд свяжет следствию «провода» // Уголовный процесс. 2010. № 6. С. 10.

нарушившего правила дорожного движения, причинив тем самым смерть или иные тяжкие последствия потерпевшему, а затем скрывшегося с места происшествия. По уголовным делам о террористических актах и криминальных взрывах сведения об абонентах, обслуживавшихся в момент совершения преступления находящейся в его районе базовой станцией, позволяет значительно сузить круг причастных к преступному деянию лиц.

По некоторым делам детализация соединений необходима для выдвижения версий о самом событии преступления, его участниках и лицах, которым могут быть известны обстоятельства происшедшего. Так, по получившему широкий резонанс уголовному делу о безвестном исчезновении самолета АН-2 после вылета с аэродрома города Серова Свердловской области детализация соединений лиц, бывших на борту самолета, была запрошена для установления свидетелей, с которыми переговаривались участники полета и которым последние могли сообщить цель и другие обстоятельства вылета[236].

Обобщение следственной и судебной практики, позволяет выделить перечень следственных ситуации и соответствующих им направлений использования информации о соединениях между абонентами и (или) абонентскими устройствами. Как верно отмечает В.Ю. Стельмах, перечень таких направлений не является исчерпывающим и характеризует главные, существующие на сегодня, пути применения сведений, полученных в результате исследуемого следственного действия[237].

По нашему мнению, информация о соединениях между абонентскими устройствами, полученная в ходе производства следственного действия, предусмотренного статьей 186.1 УПК РФ, чаще выступает в качестве косвенных доказательств. Это обусловлено в первую очередь тем, что полученные сведения не отражают содержание самих переговоров, а фиксируют только факт соединения. В связи с этим, возможно установить круг абонентов и используемых

---

[236] Колесник А. Деревья скрыли следы// Российская газета. 2012. № 164 (5837).

[237] Стельмах В.Ю. Следственные действия, ограничивающие тайну связи: монография / Ю.В. Стельмах. – Москва: Юрлитинформ. 2016. С. 303.

абонентских устройств, но не более того. Иную информацию необходимо получать путем производства иных следственных действий или мероприятий. Второй момент заключается в том, что абонент, с которым заключен договор оператора о предоставлении услуг связи, не всегда является лицом, использующим этот абонентский номер или абонентское устройство. Мобильные телефоны могут свободно передаваться от одного человека другому, что невозможно отследить. В отношении стационарных телефонов и компьютеров можно отследить их местонахождение, но установление конкретного пользователя требует дополнительных доказательств.

Ю.Н. Соколов справедливо утверждает, что «отсутствие в настоящее время реальных методик определения подлинности и авторства цифровых сообщений является основной проблемой преобразования в доказательства соответствующих данных»[238]. Данная проблема вытекает из самой природы электросвязи. Поэтому параллельно с получением и анализом детализации следователю необходимо устанавливать факты использования абонентских устройств конкретными лицами. Прежде всего, это делается в ходе допросов соответствующих участников судопроизводства. При этом надо отдавать отчет в том, что указанные факты заинтересованными лицами, скорее всего, будут скрываться. Поэтому устанавливать данные обстоятельства в ходе допросов нужно без акцентирования на этом особого внимания, например в контексте выяснения данных о личности самого допрашиваемого или лица, о котором даются показания. Вместе с тем из показаний должно четко следовать, что в момент соответствующих действий абонентским устройством пользовалось определенное лицо. Если производится допрос владельца указанного устройства, в ходе данного следственного действия требуется в обязательном порядке зафиксировать, что он не передавал мобильное абонентское устройство другим лицам, либо посторонние не имели доступа к стационарному абонентскому устройству. На допросах других лиц необходимо выяснить, как они поняли, что переговоры ведутся с конкретным лицом

---

[238] Соколов Ю.Н. Электронное наблюдение в уголовном судопроизводстве и оперативно-розыскной деятельности. Екатеринбург: Оптима Проф, 2006. С. 130.

(например, указать, что допрашиваемый достаточно хорошо знал собеседника и определял его по голосу либо они использовали какие-либо условные фразы, понятные только им, и т.п.).

Сказанное означает, что сам по себе факт соединения абонентского устройства, взятый изолированно от других добытых по делу сведений, не может свидетельствовать практически ни о каких обстоятельствах дела. Однако при его рассмотрении в совокупности с другими собранными по делу данными он может иметь важнейшее доказательственное значение.

Изложенное свидетельствует о следующих обстоятельствах, характеризующих криминалистическое и доказательственное значение результатов информации о соединениях между абонентами и (или) абонентскими устройствами.

1. Результаты получения о соединениях между абонентами и (или) абонентскими устройствами в настоящее время используются в процессе доказывания по уголовным делам практически всех категорий для установления самых разнообразных фактов, в качестве криминалистически значимой (ориентирующей) или доказательственной информации.

2. Данные сведения чаще представляют косвенные доказательства, поэтому они всегда должны анализироваться в совокупности с собранными в ходе расследования фактическими данными, а также всей информацией, получаемой от оператора сотовой связи (время соединений, место, длительность переговоров, последовательность звонков, биллинговые данные).

ЗАКЛЮЧЕНИЕ

Результаты исследования позволяют сделать следующие выводы, касающиеся процессуальных и организационно – тактических аспектов производства получения информации о соединениях между абонентскими устройствами, а также использования результатов указанного следственного действия при расследовании преступлений:

1. Учитывая положения нормативно-правовых актов, регулирующих работу организаций (компаний) сотовой связи, проведен анализ технических возможностей абонентских устройств связи, оборудования и базы данных оператора сотовой связи, как источников криминалистических значимых сведений.

2. Получение информации о соединениях между абонентами и (или) абонентскими устройствами – сравнительно новое для науки следственное действие и представляет закрепленное законодательно, процессуальное средство получения от оператора сотовой связи в установленном порядке биллинговой информации, представляемой следователю на электронном носителе и закрепляемой в качестве вещественного доказательства. Данное следственное действие обособлено, уникально и, безусловно, занимает важное место в системе следственных действий.

3. Обязательными участниками следственного действия, предусмотренного статьей 186.1 УПК РФ, без которых его производство невозможно являются суд, следователь и оператор сотовой связи. В качестве дополнительных могут привлекаться специалист (сотрудник компании сотовой связи), понятые.

4. В рамках получения информации о соединениях между абонентами и (или) абонентскими устройствами от оператора сотовой связи могут быть получены следующие сведения:

- сведения об абоненте (фамилия, имя, отчество, адрес проживания, паспортные данные), пользующегося услугами связи оператора сотовой связи;

- сведения об IMEI-номере абонентского устройства связи, устанавливаемые по абонентскому номеру, а также информация об абонентах, его использующих;

- сведения о номере абонента по информации об абоненте или по IMEI-номеру абонентского устройства;

- сведения о соединениях между абонентами по абонентскому номеру за определенный период (дата и время соединения, продолжительность разговора, номера абонентов, стоимость услуг связи, сведения о номерах и месте расположения приемопередающих базовых станций и т.д.);

- сведения о соединениях между абонентами по IMEI-номеру абонентского устройства за определенный период;

- сведения о соединениях между абонентами прошедшие через конкретную базовую станцию за определенный период;

- сведения о местонахождении абонента или абонентского устройства с указанием направления передвижения в определенный период в зоне покрытия приемопередающих базовых станций.

Вышеуказанные сведения предоставляются субъектам расследования в виде документа, именуемого детализацией, закрепленного на бумажном или электронном носителе информации. И в том и в другом случае документ представленный документ подлежит осмотру по правилам осмотра документа, о чем составляется соответствующий протокол.

5. Автономизация получения информации о соединениях между абонентами и (или) абонентскими устройствами в системе следственных действий в качестве самостоятельного позволила решить проблему законности вторжения в область гарантированных конституционных прав граждан. Поэтому совершенно справедливо производство указанного следственного действия по судебному решению, так как это является гарантией защиты конституционного права гражданина на тайну телефонных переговоров и иных сообщений.

6. Выбор следственного действия зависит от конкретных обстоятельств, сложившейся следственной ситуации. Исходя из конкретной следственной ситуации, обусловленной наличием объективных факторов, перед субъектом

расследования стоит выбор о производстве получения информации о соединениях между абонентами и (или) абонентскими устройствами.

7. Анализ следственных ситуаций, при которых необходимо получение информации о соединениях между абонентами и (или) абонентскими устройствами, позволил определить программу действий следователя, в части касающейся подготовки, проведения, оценки данного следственного действия, сопутствующих мероприятий и иных процессуальных действий.

8. Рассмотрение получения информации о соединениях между абонентами и (или) абонентскими устройствами в структуре тактических операции позволило установить, что данное следственное действие может играть ключевую роль в тактической операции и выступать в качестве центрального мероприятия, а также иметь вспомогательное значение. Автором также учтены особенности использования данного следственного действия в тактических операциях по установлению лиц, причастных к совершению преступления, а также по изобличению подозреваемых, обвиняемых, проверке алиби лица, по проверке признательных показаний подозреваемого, обвиняемого и других лиц.

9. Тактика любого следственного действия призвана обеспечить его максимальную результативность при безусловном соблюдении требований законности и представлена в виде подготовительно, основного (рабочего) и заключительных этапов. Но, структура тактики получения информации о соединениях между абонентами и (или) абонентскими устройствами отличается. В связи с этим, на подготовительном и основном этапах автор выделил по две стадии, с соответствующим набором действий. Такая структура обусловлена комплексным характером следственного действия, предусмотренного статьей 186.1 УПК РФ.

10. Результаты получения информации о соединениях между абонентами и (или) абонентскими устройствами предопределяют решение субъекта расследования о рациональности дальнейших следственных действий, их последовательность, а также конкретных тактических приемов, реализуемых при их проведении.

11. Сведения, получаемые в ходе производства рассматриваемого следственного действия, имеют доказательственное значение и могут выступать в качестве прямых и косвенных доказательств по уголовному делу. Такие сведения также имеют криминалистическое значение в наличии ориентирующей информации для организации дальнейшего планирования расследования преступления.

Вышесказанное свидетельствует о том, что поставленные для достижения цели диссертационного исследования, задачи решены. Однако объем и требования, предъявляемые к такому виду работ, не позволяют охватить весь перечень возможных проблем, которые необходимо разрешить и исследовать. Видится, что отдельные вопросы, касающиеся производства и технических возможностей получения информации о соединениях между абонентами и (или) абонентскими устройствами должны быть рассмотрены в рамках отдельного исследования. Так, перспективы развития телекоммуникационных технологий предполагают расширение перечня информации, которая может иметь доказательственное и криминалистическое значение. Обилие современных мобильных приложений только «на руку» для современного преступника. В свою очередь, сотрудники органов внутренних дел нуждаются в новейших технических средствах, позволяющих решать поставленные задачи в кратчайшие сроки, не нарушая при этом конституционные права граждан. Также, в качестве дальнейшего направления для исследования по данной тематике могут быть рассмотрены вопросы, связанные с правовым значением и особенностями получения биллинговой информации, судебного контроля за целесообразностью ее истребования со стороны правоохранительных органов, изучения электронных носителей информации, которые содержат сведения с ограниченным видом доступа (тайна личной жизни, персональные данные и иные виды служебной тайны). Особое внимание следует обратить на действующее законодательство в сфере сотовой связи и информационных технологий, оно должно не только соответствовать положениям Конституции РФ, но реалиям современного общества, которое справедливо считается информационным.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. Аналитический обзор рынка продаж мобильных телефонов. – [Электронный ресурс]. – URL: http://www.sostav.ru/news.

2. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации о получении информации о входящих и исходящих сигналах соединений телефонов при расследовании уголовных дел на основании судебного решения): паспорт проекта федерального закона № 7176-5. – [Электронный ресурс]. – режим доступа: http://www.lawmix.ru/lawprojects/234443.

3. О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: федеральный закон от 6 июля 2016 г. №374-ФЗ. – Российская газета – Федеральный выпуск №7017 (149).

4. О внесении изменений в Федеральный закон «О связи» и статьи 333.33 и 333.34 части второй Налогового кодекса Российской Федерации»: федеральный закон от 25.12.2012 № 253-ФЗ. – [Электронный ресурс]. − URL: http:/www.consultant.ru.

5. О персональных данных: федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства РФ. 2006. № 31 (1 ч.).

6. О порядке оказания услуг телефонной связи: постановление правительства Российской Федерации от 9 декабря 2014 г. № 1342 г. Москва. – [Электронный ресурс]. − URL: http:// www.consultant.ru.

7. О связи: федеральный закон от 07.07.2003 № 126-ФЗ. (действующая редакция). – [Электронный ресурс]. − URL: http:// www.consultant.ru.

8. О Федеральном законе «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации» (проект № 7176-5): постановление

Государственной Думы Федерального Собрания РФ пятого созыва от 11 июня 2010 г. № 3766-5 ГД // Собрание законодательства РФ. 2010. № 25. Ст. 3081.

9. О Федеральном законе «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации»: Постановление Совета Федерации Федерального Собрания РФ от 23 июня 2010 г. № 258-СФ // Собрание законодательства РФ. 2010. № 26. Ст. 3282.

10. Об отказе в принятии к рассмотрению жалобы гражданина Новосельцева Александра Викторовича на нарушение его конституционных прав статьями 4, 74, 88, 165, 186 и 406 уголовно-процессуального кодекса российской федерации: Определение Конституционного суда РФ от 16 декабря 2010 г. N 1712-О-О [Электронный ресурс]. – URL: https://rospravosudie.com. (дата обращения 05.03.2018 г.).

11. Об отказе в принятии к рассмотрению жалобы гражданина Власова Валерия Александровича на нарушение его конституционных прав положениями статей 115 и 165 Уголовно-процессуального кодекса Российской Федерации: Определение Конституционного Суда Российской Федерации от 25 марта 2004 года № 124-О [Электронный ресурс]. – URL: https://rospravosudie.com. (дата обращения 05.03.2018 г.).

12. Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 г. «О связи: определение Конституционного Суда РФ от 2 октября 2003 г. № 345-0 // Вестник Конституционного Суда РФ. 2004. № 1. С. 50—52.

13. Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность: постановление правительства Российской Федерации от 27 августа 2005 г. № 538 (ред. от 10.04.2013) // Собрание законодательства Российской Федерации. 2005. – № 36 ст. 3704.

14. Об утверждении Правил оказания телематических услуг связи: постановление правительства Российской Федерации от 10 сентября 2007 г. № 575

г. Москва // Российская газета - № 622 (0). – [Электронный ресурс]. –https://rg.ru/2007/09/25/svyaz-pravila-dok.html.

15. Об утверждении Правил оказания услуг подвижной связи: постановление правительства Российской Федерации от 25 мая 2005 г. № 328. – [Электронный ресурс]. − URL: http:// www.consultant.ru.

16. Обзор применения криминалистической техники Главным управлением Следственного комитета Республики Крым. – [Электронный ресурс]. − URL: http:/ http://crim.sledcom.ru/Kabinet_kriminalistiki (дата обращения 5.04.2016 г.).

17. Обзор состояния преступности в России за 2016 год. – [Электронный ресурс].-URL https://mvd.ru/folder/101762/item/7755683/(дата обращения 18.05.2017 г.).

18. Обзор судебной практики, утвержденный Президиумом Верховного Суда Российской Федерации 27 июня 2012 г. // Бюллетень Верховного Суда РФ. – 2012. – № 10. –С. 47.

19. Обзор цифровой трансформации, телекоммуникаций, вещания и ИТ. - [Электронный ресурс]. – URL: http://www.comnews.ru/node.

20. Официальный сайт ГУ МВД России по Свердловской области. – [Электронный ресурс]. − URL: https://66.мвд.рф.

21. Официальный сайт Главного управления МВД России по Челябинской области. – [Электронный ресурс]. - URL: http://74.mvd.ru.

22. Официальный сайт Министерства внутренних дел Российской Федерации. – [Электронный ресурс]. – режим доступа: http://mvd.ru/presscenter/statistics/reports/item/804701.

23. Пакет антитеррористических поправок И. Яровой. – [Электронный ресурс]. – режим доступа: https://rg.ru/2017/07/04/v-paket-antiterroristicheskih-popravok-iriny-iarovoj-dobaviat-utochneniia.html

24. Постановление Кировский районный суд г. Волгограда от 04 июня 2015 года. по делу №1-107/2015. – [Электронный ресурс]. – URL: https://rospravosudie.com. (дата обращения 22.03.2016 г.).

25. Российское информационное агентство. Официальный сайт. – [Электронный ресурс]. – URL: http://ria.ru/society/20160321/1393862596.html.

26. Собрание законодательства РФ. 2010. № 27. Ст. 3427.

27. Справка по результатам обобщения практики судебных обращений по применению положений ст.ст. 186, 186.1 Уголовно-процессуального кодекса Российской Федерации. – [Электронный ресурс]. – www.ekboblsud.ru/doc/sudpr/pr_obzor_ug.doc.

28. Сравнительное описание методов определения местоположения мобильных терминалов. – [Электронный ресурс]. – URL: http://www.mobilecomm.ru.

29. Статистические данные 2015-2016 // URL: http://www.amobile.ru/info (дата обращения 21.11.2017 г).

30. Статистический сборник (Росстат). Федеральная служба государственной статистики.– [Электронный ресурс]. − URL: http:/ www.gks.ru/.

31. Уголовно-процессуальный кодекс Российской Федерации (действующая редакция). – [Электронный ресурс]. − URL: http:/www.consultant.ru.

Монографии, учебники, учебные пособия

32. 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: монография / В.В. Агафонов, С.А Вазюлин, В.Ф. Васюков. – Москва: Юрлитинформ. – 2015. – 182 с.

33. Андрианов В.И. Средства мобильной связи / В.И. Андрианов, А.В. Соколов. – СПб: ВНУ – Санкт-Петербург, 1998. – 256 с.

34. Баев О.Я. Основы криминалистики: курс лекций. 2-е издание перераб. и дополненное / О.Я. Баев. – Москва: Экзамен. – 2003. – 282 с.

35. Баев О.Я. Следователь (основы теории и практики деятельности). Научно-практическое издание / О.Я. Баев. – Москва: Прометей. – 2017. – 480 с.

36. Батоев В.Б., Бычков В.В. Раскрытие и расследование хищений средств мобильной связи: монография / В.Б. Батоев, В.В. Бычков. – Москва: Юрлитинформ, 2013. – 177 с.

37. Безлепкин, Б.Т. Краткое пособие для следователя и дознавателя / Б.Т. Безлепкин.– Москва. – 2011. – 288 с.

38. Белкин Р.С. Курс криминалистики: учебное пособие для вузов. – 3 изд., дополненное / Р.С. Белкин. – Москва. – 2001. – 790 с.

39. Белкин Р.С. Курс советской криминалистики / Р.С. Белкин. – Москва: Академия МВД СССР. – 1979. – 407 с.

40. Белкин Р.С. Тактика следственного действия // Криминалистика. учебник для вузов / Б.А. Викторов и Р.С. Белкин. – Москва. – 1976. – 532 с.

41. Волчецкая Т.С. Криминалистическая ситуалогия: монография / Т.С. Волчецкая; под ред. Н.П. Яблокова. – Москва; Калининград: Калининградский униерситет, 1997. – 248 с.

42. Гавло В.К. О следственной ситуации и методике расследования хищений, совершаемых с участием должностных лиц. Вопросы криминалистической методологии, тактики и методики расследования. – Москва. – 1973. – С. 90.

43. Гавло В.К. Судебно-следственные ситуации: психолого-криминалистические аспекты: монография / В.К. Гавло, В.Е. Клочко, Д.В. Ким. под редакцией профессора В.К. Гавло. – Барнаул: Алтайский университет. –2006. – 226 с.

44. Гаврилин Ю. В., Дубоносов Е. С. Использование контроля и записи телефонных и иных переговоров в раскрытии и расследовании преступлений: учебное пособие / Ю.В. Гаврилин, Е.С. Дубоносов. – Москва. – 2003. – 70 с.

45. Гармаев Ю.П. Раскрытие и расследование должностных преступлений, совершенных работниками таможенных органов: методическое пособие / Ю.П. Гармаев. –Иркутск: Иркутский государственный университет. – 1998. – 124 с.

46. Герасимов И.Ф. Некоторые проблемы раскрытия преступлений / И.Ф. Герасимов. – Свердловск: Среднеуральское книжное издательство – 1975. – 178 с.

47. Герасимов И.Ф. Принципы построения методики раскрытия преступлений: в книге: Вопросы криминалистической методологии, тактики и методики расследования / И.Ф. Герасимов. – Москва. –1973. С. 82.

48. Давлетов А.А. Основы уголовно-процессуального познания: монография / А.А. Давлетов. – Екатеринбург, 1997. – 191 с.

49. Доля Е.А. Использование в доказывании результатов оперативно-розыскной деятельности / Е.А. Доля. – Москва., 1996.

50. Драпкин Л.Я. Понятие и иллюстрация следственных ситуаций. «Следственные ситуации и раскрытие преступлений». – Свердловск, 1975.

51. Драпкин Л.Я. Следственные ситуации: роль и значение в раскрытии и расследовании преступлений: учебное пособие / Л.Я. Драпкин, Д.Л. Кокорин, И.Г. Пяткова. – Екатеринбург: Уральский юридический институт МВД России, 2017. – 80 с.

52. Драпкин Л.Я. Тактика следственных действий: учебное пособие / Л.Я. Драпкин. – Екатеринбург: Уральский юридический институт МВД России. 2014. – 110 с.

53. Драпкин Л.Я., Долинин В.Н. Тактика следственных действий: учебно-практическое пособие. – Екатеринбург: издательский дом Уральского государственного университета, 2015. – 136 с.

54. Железняк А.С. Криминалистика: тактико-методические основы уголовного судопроизводства (досудебная стадия): учебное пособие / А.С. Железняк. – Москва: МГИУ, 2007. – 126 с.

55. Информационные технологии в юридической деятельности: учебник для академического бакалавриата / П.У. Кузнецов [и др.]. – Москва: Издательство Юрайт, 2017. – 325 с.

56. Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи: монография / В.А. Козинкин. – Москва: Юрлитинформ, 2010. – 192 с

57. Комаров И.М. Основы частной теории криминалистических операций досудебного производства: монография / И.М. Комаров. – Москва: Юрлитинформ, 2010. – 160 с.

58. Коротков А.П., Токарева М.Е. Контроль и запись переговоров при осуществлении оперативно-розыскных мероприятий и следственных действий: методические рекомендации / А.П. Коротков, М.Е. Токарева. – Москва, 2005. – 20 с.

59. Криминалистика: учебник / А.Г. Филиппов. Москва. – 2008. – 687 с.

60. Криминалистика: учебник / Д.Н. Балашов, Н.М. Маликов. – Москва. – 2005. 503 с.

61. Криминалистика: учебник / Л.Я. Драпкин, В.Н. Карагодин. 2-е изд., перераб. и доп. – Москва, 2011. – 768 с.

62. Криминалистика: учебник / под ред. Е.П. Ищенко. Москва. – 2000. – 784 с.

63. Криминалистика: учебник / Р.С. Белкин. Москва: НОРМА – ИНФРА, 1999. 990 с.

64. Криминалистика: учебник / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Россинская. – 3-е изд., перераб. и доп. – Москва: Норма, 2008. С. 599-600.

65. Криминалистика: учебник для бакалавров / под ред. Л.Я. Драпкин. – М.: Издательство Юрайт, 2013. – 831 с.

66. Криминалистика: учебник для вузов / Т.В. Аверьянова, Е.Р. Россинская, Р.С. Белкин, Ю.Г. Корухов. – 3-е изд., перераб. и доп. – Москва: НОРМА, 2008. – 944 с.

67. Курс криминалистики: Общая теория криминалистики: в 3 т. / Р.С. Белкин. – Москва: Юристъ, 1997. – Т. 1. – 408 с.

68. Курс криминалистики: Частные криминалистические теории : в 3 т. / Р.С. Белкин. – Москва: Юристъ, 1997. – Т. 2 – 464 с.

69. Курс криминалистики: Криминалистические средства приемы и рекомендации: в 3 т. / Р.С. Белкин. – Москва: Юристъ, 1997. – Т. 3. – 480 с.

70. Лавров В.П. Расследование преступлений по горячим следам: учебно-практическое пособие / В.П. Лавров. – Москва, 1989 – 87 с.

71. Лапин Е.С. Тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами: монография / Е.С. Лапин – Юрлитинформ, 2014. – 191 с.

72. Лузгин И.М. Моделирование в расследовании преступлений. М., 1981. С.94.

73. Маркин В.И.Самые громкие преступления XXI века в России / Владимир Маркин. – Москва: Издательство «Э», 2016. – 352 с. – (Тайны Следственного комитета с Владимиром Маркиным).

74. Методические рекомендации по расследованию уголовных дел по преступлениям, связанным с различными формами хищения мобильных средств связи, находящихся в частной собственности граждан, предприятий, организаций, учреждений и др. Пермский областной суд // URL: http://perm.newsity.info/docs/sistemst.

75. Михальчук А.Е. Тактические комбинации при производстве следственных действий: монография / А.Е. Михальчук. – Саратов: Издательство Саратовского университета, 1991. – 183 с.

76. Мозяков В.В. Руководство для следователей / под ред. В.В. Мозякова. –Москва, 2005. – 912 с.

77. Невдяев Л.М. Телекоммуникационные технологии. Англо-русский толковый словарь-справочник / Ю.М. Горностаев. – Серия изданий «Связь и бизнес». – Москва, 2002. – 592 с.

78. Ожегов С.И. Толковый словарь русского языка / С.И. Ожегов, Н.Ю. Шведова. – URL: http://slovarozhegova.ru/word.php?wordid=31378.

79. Россинский С.Б. Уголовный процесс России: курс лекций / С.Б. Россинский.– Москва: Эксмо, 2008. – 571 с.

80. Селиванов Н.А. Советская криминалистика. Система понятий / Н.А. Селиванов. – Москва, 1982. – 172 с.

81. Семенов Г.В. Расследование преступлений в сфере мобильных телекоммуникаций / Г.В. Семенов. – Москва: Юрлитинформ, 2006. – 336 с.

82. Соколов Ю.Н. Электронное наблюдение в уголовном судопроизводстве и оперативно-розыскной деятельности / Ю.Н. Соколов. – Екатеринбург: Оптима Проф, 2006. – 164 с.

83. Соколов Ю.Н. Использование биллинговой информации в уголовном процессе: учебное пособие. Екатеринбург, 2012. – 135 с.

84. Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: монография / В.Ю. Стельмах. – Екатеринбург: Уральский юридический институт МВД России, 2014. – 209 с.

85. Стельмах В.Ю. Следственные действия, ограничивающие тайну связи: монография / Ю.В. Стельмах. – Москва: Юрлитинформ. – 2016. – 424 с.

86. Уголовно-процессуальное право РФ: учебник / отв. ред. П.А. Лупинская. – 2-е изд., перераб. и доп. – Москва: Норма, 2009. – 1072 с.

87. Усманов Р.А. Теория и практика использования криминалистической информации в процессе раскрытия и расследования преступлений : монография / Р.А. Усманов. – Челябинск: Челябинский юридический институт МВД России, 2006. – 232 с.

88. Федотов Н.Н. Форензика – компьютерная криминалистика / Н.Н. Федотов. - Москва: Юридический Мир, 2007. – 360 с.

89. Шейфер, С.А Следственные действия. Основания,процессуальный порядок и доказательственное значение / С.А. Шейфер. – Москва: Юрлитинформ, 2004. – 183 с.

90. Шурухнов, Н.Г. Криминалистика: определения, схемы, таблицы, диаграммы, рекомендации : учебное пособие / Н.Г. Шурухнов. - М. : Эксмо, 2008. - 352 с.

91. Яблоков Н. П. Криминалистика: учебник / Н. П. Яблоков. – Москва, 2005. – 781 с.

Научные статьи

92. Алексанов И.В. Типичные следственные ситуации и оптимальные системы следственных действий в расследовании налоговых преступлений / И.В. Алексанов // Правоведение. – 2002. – № 6. – С. 182.

93. Астафьев Ю.В., Винокурова Т.В. Проблема получения сведений о телефонных соединениях при производстве ОРД [Электронный ресурс]. URL: http://www.consultant.ru.

94. Баев О.Я. О возможностях использования особенностей мобильной сотовой связи для раскрытия и расследования преступлений / О.Я. Баев, В.А. Мещеряков // Воронежские криминалистические чтения. - Выпуск 7 / Редколлегия: О.Я. Баев, Т.Э. Кукарникова, В.А. Мещеряков. – Воронеж: Издательство Воронежского университета, 2006. – С. 35-45.

95. Богдановский А. Может ли ошибаться Конституционный Суд? / А. Богдановский // Законность. – 2006. – № 8. – С. 34 – 39.

96. Брусницын Л. УПК РФ: соответствует ли он рекомендациям ООН и Совета Европы по обеспечению безопасности свидетелей / Л. Брусницын // Уголовное право. – 2010. – № 6. – С. 65–66.

97. Бурцева Е.В., Рогова И.А. Проблемы получения информации, содержащейся в электронных мобильных устройствах, с применением универсального устройства извлечения судебной информации (UFED) / Materialy X mezinarodni vedecko-prakticka konf.: Efektivni nastroje modernich ved. – 2014 (27.04.2014-05.05.2014). Dil 11. Pravni vedy Administrativa. - Praha. Publishing House «Education and Scietnce» s.r.o. – С. 53 – 57.

98. Быков В.М., Сазонова Т.П. Истребование сведений о телефонных контактах как процессуальное действие по собиранию доказательств // Уголовный процесс. 2008. №9. С. 54–56.

99. Вайпан В.А. Базы данных об абонентах операторов связи / В.А. Вайпан // Право и экономика. – 2006. – №9. – С. 21-24.

100. Вазюлин С.А., Васюков В.Ф. Получение информации о соединениях между абонентами: специфика процедуры / С.А. Вазюлин, В.Ф. Васюков // Уголовный процесс. – 2014. –№ 1. – С. 10–20.

101. Варпаховская Е., Вяткин А. Расследование хищений мобильных телефонов / Е. Варпаховская, А. Вяткин // Законность. – 2005. – № 3. – С. 23.

102. Васюков В.Ф. Процессуальные особенности истребования информации об абонентских соединениях и абонентских устройствах при расследовании преступлений против личности. /В. Ф. Васюков // Наука и практика. – 2012. – № 3. – С.15-17.

103. Васюков В.Ф. Сведения об абонентах связи как криминалистически значимая информация при раскрытии и расследовании грабежей и разбоев, совершаемых на открытой местности / В.Ф. Васюков // Правовые вопросы связи. – 2008. – № 2. – С. 15.

104. Веденин А.В. Понятие результатов оперативно-розыскной деятельности / А.В. Веденин // Вестник Владимирского юридического института. 2008. – № 2 (7). – С. 114.

105. Вехов В.Б. Аспекты расследования преступлений в сфере предоставления услуг сотовой электросвязи / В.Б. Вехов // Труды Тамбовского филиала юридического института МВД России за первое полугодие 2001 г. – Вып. 4. –Тамбов : Тамбовский филиал ЮИ МВД России, 2001. – С. 102-108.

106. Винокурова Т.В., Астафьев Ю.В. Проблема получения сведений о телефонных соединениях при производстве ОРД / Т.В. Винокурова, Ю.В. Астафьев // Российская юстиция. – 2008. – № 1. – С. 55.

107. Гавло В.К. Методика расследования как особая теоретикометодическая модель - информационный аналог расследования криминальных событий / В.К. Гавло // Проблемы теории и практики борьбы с преступностью. - Томск, 1984. С. 162-174.

108. Гаврилов М. Следственный осмотр при расследовании преступлений в сфере компьютерной информации / М. Гаврилов, А. Иванов // Законность. – 2001. – №9. – С. 11-16.

109. Герасимов И.Ф. Тактическая операция как форма взаимодействия органов предварительного расследования / И.Ф. Герасимов // Тактические операции и эффективность расследования. Свердловск, 1986.

110. Драпкин Л.Я. Общая характеристика следственных ситуаций / Л.Я. Драпкин // Следственная ситуация: сборник научных трудов. – Москва, 1984. – С. 18.

111. Драпкин Л.Я. Особенности информационного поиска в процессе расследования и тактика следствия / Л.Я. Драпкин // Проблемы повышения эффективности предварительного следствия: тезисы научной конференции. 1976. С. 54.

112. Дулов А.В. О разработке тактических операций при расследовании преступлений / А.В. Дулов // 50 лет советской прокуратуры и проблемы совершенствования предварительного следствия. Москва, 1973.

113. Дулов А.В. Тактические операции при расследовании преступлений / А.В. Дулов. – Минск: Издательство БГУ, 1979. – С. 89–91.

114. Иванов А. Использование в доказывании информации, полученной у операторов связи / А. Иванов, О. Корниенко // Уголовное право. – 2006. – № 1. – С. 111.

115. Иванов А.Н. Проблемы получения при расследовании преступлений информации у операторов связи / А.Н. Иванов // Криминалистика в системе правоприменения: материалы конференции (27–28 октября 2008 г., Москва, МГУ им. М.В. Ломоносова). – Москва. – С. 135.

116. Ионова Е.В. Понятие, значение и тактика получения информации о соединениях между абонентами и (или) абонентскими устройствами (ст. 186.1 УПК РФ) / Е.В. Ионова// Вестник криминалистики. − 2011. − Вып. 1 (37). − С. 35.

117. Ищенко Е.П. Получение и использование новых видов доказательств – актуальная задача российской криминалистики / Е.П. Ищенко // Криминалистика в системе правоприменения. Материалы конференции, 27–28 октября 2008 г., Москва, МГУ им. М.В. Ломоносова. – Москва. – 2008. – С. 143.

118. Кальницкий В.В. Вопросы правовой регламентации следственных действий на современном этапе / В.В. Кальницкий // Законы России: опыт, анализ, практика. – 2015. – № 2. – С. 34.

119. Ковальчук Р.С. Хищение мобильных телефонных аппаратов / Р.С. Ковальчук // Российский следователь. – 2010. –№ 5 – С. 12-13.

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

121. Колесник А. Деревья скрыли следы / А. Колесник // Российская газета. – 2012. – № 164 –(5837). – С. 21.

122. Краснова Л.Б. Электронные носители информации как вещественные доказательства / Л.Б. Краснова // Известия Тульского государственного университета. Вып. 4. Ч. II. Юридические науки. Тула. – 2013. – С. 258.

123. Куприянов А.А. Суд свяжет следствию «провода» / А.А. Куприянов // Уголовный процесс. 2010. – № 6. – С. 10.

124. Лапин Е.С. Технология получения информации о соединениях между абонентами и (или) абонентскими устройствами при расследовании преступлений против интеллектуальной собственности / Е.С. Лапин // Российский следователь. – 2011. – №3. – С. 2-5.

125. Макаров А.В., Фирсов О.В. Особенности использования результатов оперативно-розыскной деятельности в процессе доказывания по уголовным делам / А.В. Макаров, О.В. Фирсов // Российский следователь. 2012. – № 8. – С. 43.

126. Миролюбов С. Л. Генезис правовой основы использования результатов ОРД в доказывании по уголовным делам: актуальные проблемы / С.Л. Миролюбов // Вестник Владимирского юридического института. – 2009. – № 1 (10). – С. 115.

127. Образцов В. А., Танасевич В. Г. Понятие и криминалистическое значение следственной ситуации / В.А. Образцов, В.Г. Танасевич // Советское государство и право. – 1979. – № 8. – С. 113.

128. Подойницын Р. Прикладная экономика сетей беспроводного доступа / Р. Подойницын // ИнформКурьерСвязь. –2009. – №6. – С. 15-18.

129. Подшибякин А.С. Преодоление противодействия расследованию в ходе допроса / А.С. Подшибякин // Организационное противодействие раскрытию и расследованию преступлений и меры его нейтрализации. –Москва, 1997. – С. 114-117.

130. Проблемы расследования преступлений, связанных с мошенническими действиями, совершенных с использованием средств сотовой телефонной связи / Т.В. Астишина, Е.В. Маркелова // Вестник Казанского Юридического института МВД России. – 2014. – Выпуск 2(16). – С. 97.

131. Скобелин С.Ю. Юридическая основа и процессуальное оформление извлечения и анализа данных из мобильных устройств / С.Ю. Скобелин // Расследование преступлений: проблемы и пути их решения: сборник трудов. – вып. 1. – Москва: Буки Веди, 2013. – С. 183.

132. Соколов Ю.Н. Использование информации о соединениях между абонентами и (или) абонентскими устройствами в ходе предварительного расследования преступлений / Ю.Н. Соколов // Российский следователь. – 2011. – №11. – С. 18–21.

133. Стрельцов И.А. Технико-криминалистическое обеспечение предварительного следствия как функция Главного управления криминалистики Следственного комитета Российской Федерации / И.А. Стрельцов // Российский следователь. – 2014. – № 20. – С. 15 – 18.

134. Фалалеев М. Не верь, не слушай, не звони. МВД составило базу данных на телефонных мошенников / М. Фалалеев // Российская газета. – 2010.

135. Фомин М.А. Допустимость материалов ОРМ в качестве доказательств по делам о получении взятки / М.А. Фомин // Уголовный процесс. – 2011. – № 2 (62). – С. 20.

136. Фролова Т.А. Закрепление результатов ОРД и передача их следственным органам и суду / Т.А. Фролова // Уголовный процесс. – 2008. – № 3 (39). – С. 30.

137. Фролова Т.А. Использование в доказывании результатов оперативно-розыскной деятельности / Т.А. Фролова // Уголовный процесс. – 2008. –№ 9 (45) – С. 10.

138. Центров Е.Е. Особенности использования положений следственной тактики в правоприменительной деятельности / Е.Е. Центров // Криминалистика в системе правоприменения: материалы конференции, 27–28 октября 2008 г., Москва, МГУ им. М.В. Ломоносова. – Москва, 2008. – С. 25–26.

139. Чечетин А.Е. Ограничение тайны связи / А.Е. Чечетин // Законность. – 2005. – № 7. – С. 40.

140. Шебалин А.В. Правовая регламентация получения сведений о соединениях абонентов как важное условие успешного расследования хищений средств сотовой связи / А.В. Шебалин // Вестник Барнаульского юридического института МВД России. – 2009. – № 2 (17). – С. 77.

141. Шергин Г. Н. Использование результатов ОРД в уголовно-процессуальном судопроизводстве / Г.Н. Шергин // Российский следователь. – 2011. – № 11. – С. 24–26.

142. Шиканов В.И. Разработка теории тактических операций – важнейшее условие совершенствование методики расследования преступлений / В.И. Шиканов // Методика расследования преступлений (общие положения): материалы научно-практической конференции. – Москва, 1976. – С. 156-157.

143. Яблоков, Н.П. Совершенствование методических основ расследования преступлений / Н.П. Яблоков // Советское государство и право. – 1976. – №2. – С. 68–69.

Диссертации и авторефераты

144. Архипова Н.А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной связи: автореф. дис. … канд. юрид. наук / Н.А. Архипова. – СПб.: Санкт-Петербургский университет МВД России, 2011. – 25 с.

145. Архипова Н.А. Организационно-тактические аспекты раскрытия и расследования преступлений в ситуациях использования средств мобильной

связи: дис. … канд.юрид. наук/ Н.А. Архипова. – СПб.: Санкт-Петербургский университет МВД России, 2011. – 203 с.

146. Васюков В.Ф. Особенности раскрытия и расследования грабежей и разбоев, совершаемых на открытой местности: дис. …канд. юрид. наук / В.Ф. Васюков. – Орел, 2009. – 237 с.

147. Васюков В.Ф. Особенности раскрытия и расследования грабежей и разбоев, совершенных на открытой местности: автореф. дис. … канд. юрид. наук / В.Ф. Васюков. – Орел: Орловский юридический институт МВД России, 2009. – 33 с.

148. Горячев Э.К. Тактико-криминалистическое обеспечение раскрытия и расследования преступлений : дис. ... канд. юрид. наук / Э.К. Горячев. - Москва, 2004. – 200 с.

149. Драпкин Л.Я. Основы криминалистической теории следственных ситуаций. дис. … д-ра. юрид. наук / Л.Я. Драпкин. – Свердловск, 1987. – 440 с.

150. Ивченко Л.И. Тактика контроля и записи переговоров и использование результатов этого следственного действия в расследовании преступлений: дис. … канд. юрид. наук / Л.И. Ивченко. – Москва, 2004. – 210 с.

151. Козинкин В.А. Использование в расследовании преступлений информации, обнаруживаемой в средствах сотовых систем подвижной связи: дисс. …канд. юрид. наук. / В.А. Козинкин. – Ижевск, 1998. – 252 с.

152. Комаров И.М. Проблемы теории и практики криминалистических операций в досудебном производстве: дис. ... д-ра юрид. наук / И.М. Комаров. – Барнаул, 2003. – 437 с.

153. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: дис. ... д-ра юрид. наук / В.А. Мещеряков. – Воронеж, 2001. – 418 с.

154. Нуждин А.А. Расследование мошенничества, совершенного осужденными в учреждениях УИС с использованием средств сотовых систем подвижной связи: дисс. …канд. юрид. наук. / А.А. Нуждин. – Рязань, 2013. – 232 с.

155. Перекрестов В. Н. Уголовно-процессуальное значение признания вины в России: автореф. … дис. канд. юр. наук. Саратов, 2013. – 28 с.

156. Пигорев О.И. Развитие института следственных действий в российском уголовно-процессуальном праве: автореф. дис. … канд. юрид. наук / О.И. Пигорев. – Москва. – 2010. – 29 с.

157. Пономаренко Н.Ю. Тактические операции и оперативно-тактические комбинации как средства расследования преступлений: дисс. …канд. юрид. наук. / Н.Ю.Пономаренко. – Белгород, 2017. – 255 с.

158. Прыткова Е.В. Обеспечение безопасности подозреваемого (обвиняемого), заключившего досудебное соглашение о сотрудничестве, на стадии предварительного расследования: тактические аспекты: дис. канд. юрид. наук / Е.В. Прыткова. – Барнаул, 2015. – 219 с.

159. Савельева М.В. Теория и практика использование фактора внезапности в уголовном судопроизводстве: дис. .. канд. юрид. наук / М.В. Савельева. – Саратов, 2003. – 227 с.

160. Семенов Г.В. Расследование преступлений в сфере мобильных телекоммуникаций: дис. … канд.юрид. наук / Г.В. Семенов. – Воронеж, 2003. – 242 с.

161. Смушкин А.Б. Задержание в структуре тактической операции при расследовании преступлений: дис. ... канд. юрид. наук / А.Б. Смушкин. – Саратов, 2005. – 243 с.

162. Стельмах В.Ю. Получение информации о соединениях между абонентами и (или) абонентскими устройствами как следственное действие: дис. ... канд. юрид. наук / В.Ю. Стельмах. – Екатеринбург, 2013. – 240 с.

163. Сухов В.А. Повышение точности определения местоположения мобильных абонентских устройств в сетях IEEE 802.11G путем применения оптимальных алгоритмов обработки сигналов: дис. … канд. технич. наук. СПб.: Санкт-Петербургский государственный политехнический университет, 2012. – 140 с.

164. Ударцев С.Ю. Раскрытие хищений средств сотовой связи подразделениями уголовного розыска: автореф. дис. … канд. юрид. наук / С.Ю. Ударцев. – Омск, 2008. – 37 с.

165. Фомина А.С. Основные тактические операции при расследовании серийных убийств: автореф. дис. ... канд. юрид. наук. Воронеж, 2003. - 32 с.

166. Цыкора А.А. Тактико-криминалистические особенности производства следственных действий, связанных с получением и исследованием информации, передаваемой по техническим каналам связи: дис. … канд. юрид. наук / А.А. Цыкора. – Ростов-на-Дону. 2013. – 221 с.

167. Черенков А. В. Использование контроля и записи переговоров в раскрытии и расследовании преступлений: автореф. дис. … канд. юрид. наук / А.В. Черенков Москва, 2005. – 30 с.

168. Чернышев М.А. Осмотр места происшествия как базовая тактическая операция: дис. … канд. юрид. наук / М.А. Чернышев. – Курск, 2008. – 182 с.

169. Шиканов В.И. Теоретические основы тактической операции в расследовании преступлений: дис. … канд. юрид. наук / В.И. Шиканов. – Иркутск, 1983. – 200 с.

170. Ширев Д. А. Контроль и запись телефонных и иных переговоров и их доказательственное значение в уголовном судопроизводстве России: дис. … канд. юрид. наук / Д.А. Ширев. – Москва, 2009. – 219 с.

171. Юрина Л.Г. Процессуальные и криминалистические проблемы контроля и записи переговоров: дис ... канд. юрид. наук / Л.Г. Юрина. – Саратов, 2001. – 214 с.

ПРИЛОЖЕНИЯ

Приложение 1

Анкета
для следователей (дознавателей) по изучению мнения об особенностях производства следственного действия, предусмотренного статьей 186.1 УПК РФ Получение информации о соединениях между абонентами и (или) абонентскими устройствами

Уважаемый коллега!
Вашему вниманию предлагается анкета, посвященная исследованию процессуальных и тактико-криминалистических особенностей производства получения информации о соединениях между абонентами и (или) абонентскими устройствами. Заполняя пункты данной анкеты, помните, что для ее разработчиков ценно Ваше мнение, профессиональная позиция, связанная с производством данного следственного действия. Разработчики анкеты ни в коей мере не преследовали цель осуществить те или иные формы профессиональной аттестации. Поэтому в данном случае не существует так называемых «неправильных» ответов, даже если их содержание расходится с действующей законодательной редакцией определенных положений. Ряд вопросов содержит варианты ответа, некоторые потребуют прописать свой ответ. Поскольку Ваши ответы ценны, прежде всего, для разработки рекомендаций по совершенствованию производства следственного действия, предусмотренного статьей 186.1 УПК РФ то, пожалуйста, при выборе данного пункта не стесняйтесь выразить свое мнение, пусть, даже если оно не вполне совпадает с официальной позицией.

1. Ваша должность, подразделение, стаж работы в сфере расследования преступлений (следователем, старшим следователем, руководителем следственного органа; дознавателем, старшим дознавателем, начальником подразделения дознания)	Общее количество анкетируемых	%
Следователь (Старший следователь)	79	
Дознаватель (Старший дознаватель)	39	
Руководитель СО	7	
Руководитель ОД	4	
Всего	129	
2. Проводите ли Вы следственное действие получение информации о соединениях между абонентами и (или) абонентскими устройствами?		
А) Да, регулярно, каждое второе уголовное дело;	54	41,9
Б) Иногда, каждое 5,6 уголовное дело;	35	27,1
В) Редко, одно из 10 уголовных дел;	9	7,0
Г) Не назначаю никогда;	2	1,6

Д) Иное (укажите, как часто вы назначает данное следственное действие).		
3. Если не назначаете, то по какой причине?		
А) Недостаток знаний по тактике производства получения информации о соединениях между абонентами и (или) абонентскими устройствами;	4	3,1
Б) Отсутствие в непосредственной близости компании (организации) связи, предоставляющей интересующие сведения;		
В) Наличие письменных, устных и (или) неофициальных распоряжений локального характера о не назначении данного следственного действия и проведении аналогичного оперативно-розыскного мероприятия;	9	7,0
Г) Получаю информацию об абонентах в рамках других следственных действий (выемка, контроль и запись переговоров) или оперативно-розыскных мероприятий (прослушивание телефонных переговоров, наведение справок, получение компьютерной информации);	20	15,5
Д) Исходя из обстоятельств, подлежащих доказыванию, по уголовному делу, нет необходимости в проведении данного следственного действия.	96	74,4
4. Учитываете ли Вы, что средства сотовой связи могут представлять интерес для следствия и содержать криминалистически значимую информацию?		0,0
А) Да, средства сотовой связи представляют интерес для следствия, поэтому им уделяю особое внимание и принимаю меры к использованию потенциальной информации;	107	82,9
Б) Уделяю внимание только в том случае, если об этом стало заранее известно;	22	17,1
В) Никогда об этом не задумывался;	1	0,8
Г) Не обращаю внимания на средства сотовой связи, так как они не являются источником криминалистически значимой информации.		
5. Насколько эффективно производство получения информации соединениях между абонентами и (или) абонентскими устройствами при расследовании преступлений?		0,0
А) Результаты носят только справочный характер;	3	2,3
Б) Результаты позволяют определить дальнейший ход расследования;	29	22,5
В) Результаты являются предпосылкой для дальнейших следственных действий;	49	38,0
Г) Результаты носят ориентирующий характер;	39	30,2
Д) Результаты имеют доказательственное значение.	57	44,2

6. По каким видам преступлений чаще всего применяется получение информации соединениях между абонентами и (или) абонентскими устройствами?		0,0
А) Мошенничества;	83	64,3
Б) Вымогательства	51	39,5
В) Убийства;	48	37,2
Г) Корыстно-насильственные преступления;	75	58,1
Д) Преступления в сфере компьютерной информации;	54	41,9
Е) Иной вид преступлений (НОН, ДТП, кражи автомобилей)	66	51,2
7. С какой целью Вы планируете и проводите получение информации о соединениях между абонентами и (или) абонентскими устройствами?		
А) С целью получения доказательственной базы по уголовному делу;	112	86,8
Б) С целью собирания ориентирующей и криминалистически значимой информации;	98	76,0
В) Иная цель.	1	0,8
8. На Ваш взгляд, какие следственные (процессуальные) действия, необходимо проводить для сбора информации об использовании средств сотовой связи в расследовании уголовного дела?		
А) Осмотр места происшествия;	35	27,1
Б) Допросы;	103	79,8
В) Обыск;	92	71,3
Г) Выемка распечатки телефонных соединений у владельца средства мобильной связи;	88	68,2
Д) Выемка предметов и документов, содержащих IMEI- номер и другие технические характеристики средств мобильной связи;	115	89,1
Е) Осмотр предметов и документов;	84	65,1
Ж) Получение от оператора связи по судебному решению распечатки телефонных соединений абонентов;	121	93,8
З) Получение от оператора связи по судебному решению содержания SMS-, EMS-, MMS-сообщений;	31	24,0
И) Получение от оператора связи информации о пользователе мобильного телефона по IMEI-номеру;	109	84,5
К) Выемка мобильного телефона;	78	60,5

Л) Выемка SIM-карты.	69	53,5
9. Какие объекты, непосредственно содержащие информацию об абонентах и абонентских устройствах, либо позволяющие получить данную информацию, Вами изымались?		
А) Сотовый телефон;	124	96,1
Б) Компьютер, ноутбук, нетбук, планшеты и т.п. устройства, в которых функция телефонных переговоров существует как дополнительная;	99	76,7
В) SIM-карта, флеш-карта, компакт диск, иной съемный носитель информации;	115	89,1
Г) Распечатка детализации телекоммуникационных контактов определенного абонента (абонентского устройства);	108	83,7
Д) Упаковка для сотовых телефонов, SIM-карта, иных предметов, другие аксессуары;	82	63,6
Е) Иное цифровое устройство, оснащенное функцией устных или письменных телекоммуникационных переговоров (указать, какое). (Переносной жесткий диск)	3	2,3
10. Какие характеристики (данные) средств сотовой связи Вы учитываете при расследовании уголовных дел?		
А) Идентификационный номер IMEI оборудования;	123	95,3
Б) Абонентский номер SIM-карты;	126	97,7
В) Хранение текстовой информации, звуковой, фото-, видеозаписей, сведений о телефонных номерах, содержание SMS-, EMS-, MMS-сообщениях.	104	80,6
11. Если Вами собиралась информация об использовании средств мобильной связи в ходе раскрытия и расследования преступлений, то каким образом?		0,0
А) Получение от оператора связи распечатки телефонных соединений на бумажном носителе (ст. 186.1 УПК РФ);	119	92,2
Б) Получение от оператора связи распечатки телефонных соединений на электронных носителях (ст. 186.1 УПК РФ);	125	96,9
В) Контроль и запись телефонных переговоров (ст. 186 УПК РФ);	31	24,0
Г) Выемка документов, содержащих технические характеристики средств мобильной связи;	20	15,5
Д) Изъятие средств мобильного телефона в ходе проведения следственных действий (осмотра места происшествия, обыска, выемки).	68	52,7

12. В случае обнаружения на месте происшествия абонентского устройства связи (мобильного телефона, смартфона, части мобильного устройства с сохранившимся кодами IMEI, номером телефона), SIM-карты, какие дальнейшие действия Вы производили или укажите последовательность производства действий?		
А) Осмотр предмета;	124	96,1
Б) Изъятие;	118	91,5
В) Получение информации о соединениях между абонентами и (или) абонентскими устройствами;	125	96,9
Г) Назначение компьютерно-технической экспертизы;	77	59,7
Д) Иное (указать действие или последовательность производимых действий).		
13. При обнаружении сотового телефона осматривалась и изымалась ли Вами содержащаяся в нем информация?		0,0
А) Осматривался только внешний вид обнаруженного сотового телефона	21	16,3
Б) При осмотре, информация с экрана мобильного телефона, записывалась в протокол следственного действия;	66	51,2
В) При осмотре, информация с экрана мобильного телефона, фотографировалась при помощи фотоаппарата;	84	65,1
Г) Во время осмотра информация, содержащаяся в мобильном телефоне, осматривалась и изымалась на электронный носитель информации;	35	27,1
Д) Во время осмотра информация, содержащаяся в мобильном телефоне, осматривалась и изымалась на бумажный носитель информации.	71	55,0
14. Проводя получение информации о соединениях между абонентами и (или) абонентскими устройствами, какие сведения представляют наибольший интерес для следствия?		
А) Персональные данные абонента;	42	32,6
Б) Местоположение абонента или абонентского устройства в определенный период времени;	119	92,2
В) Данные об абонентском устройстве (абонентской активности);	76	58,9
Г) Детализация вызовов, перечень входящих/исходящих сообщений;	89	69,0
Д) Все вышеперечисленное в совокупности;	125	96,9
Е) Иные сведения (указать какие).		

15. Каким способом Вы получали от операторов связи информацию об использовании средств сотовой связи?		
А) Получение распечатки телефонных соединений путем проведения следственного действия (ст. 186.1 УПК РФ);	122	94,6
Б) Запрос следователя оператору связи;	69	53,5
В) Направление поручения о производстве ОРМ в ОУР;	44	34,1
Г) Направление поручения о производстве ОРМ в БСТМ;	42	32,6
Д) Получение распечатки телефонных соединений у владельца SIM-карты.	86	66,7
16. В результате каких еще следственных действий (помимо получения информации о соединениях между абонентами и (или) абонентскими устройствами) Вы получаете в распоряжение объект, содержащий информацию о телекоммуникационных контактах?		
А) Обыск помещения, жилища;	62	48,1
Б) Личный обыск;	45	34,9
В) Выемка в помещении, в жилище;	33	25,6
Г) Выемка информации, содержащей охраняемую законом тайну;	15	11,6
Д) Осмотр места происшествия;	74	57,4
Ж) Осмотр предметов и документов;	77	59,7
З) Следственный эксперимент;	12	9,3
И) Иные (указать).		0,0
17. Считаете ли Вы, что следственное действие, предусмотренное статьей 186.1 УПК РФ, является комплексным, т.е. предусматривает в себе ряд других самостоятельных действий (работа специалистов организации связи, осмотр документов, детализации следователем, приобщение полученных сведений в качестве вещественных доказательств)?		
А) Да, я согласен с позицией о том, что данное следственное действие носит сложный, комплексный характер, так как состоит из нескольких действий;	112	86,8
Б) Нет, не согласен, оно одномоментное и представляет единое действие, предполагающее определенный результат;	6	4,7
В) Данное следственное действие является технически сложным, но не носит комплексный характер;	11	8,5
В) Укажите свой ответ, аргументируйте.		0,0
18. На каком из этапов предварительного расследования преступлений Вы используете возможности следственного действия Получение		0,0

информации о соединениях между абонентами и (или) абонентскими устройствами?		
А) Первоначальный этап предварительного расследования (с момента возбуждения уголовного дела до предъявления подозреваемому обвинения);	118	91,5
Б) Последующий этап предварительного расследования (с момента предъявления обвинения).	23	17,8
19. Укажите, с какой следственной ситуацией Вы сталкивались в процессе расследования преступлений?		
А) Ситуации, когда преступные действия направлены на хищение средств сотовой связи;	71	55,0
Б) Ситуации, когда сотовый телефон используются как непосредственное средство совершения преступления;	105	81,4
В) Ситуации, когда мобильные телефоны используются в качестве средства организации подготовки, совершения, сокрытия преступных действий между участниками преступной группы и иными лицами;	79	61,2
Г) Ситуации, когда использование мобильного телефона напрямую не связано с совершением преступлений, а носит случайный, ситуационный характер.	36	27,9
20. В каких следственных ситуациях чаще всего следователь принимает решение о получении информации о соединениях между абонентами и (или) абонентскими устройствами?		
А) Следствие располагает информацией, что перед преступлением имелись телефонные переговоры (сговор) между соучастниками - членами организованной группы или группы лиц по предварительному сговору;	117	90,7
Б) Имеются данные о том, что разыскиваемый выходит или предполагается, что будет выходить на связь со своими близкими родственниками, близкими лицами, знакомыми или соучастниками преступления;	106	82,2
В) Имеется информация о том, что подозреваемый будет звонить потерпевшему, его родным, близким или знакомым лицам после совершения деяния или что он им звонил до того, как преступление совершить;	92	71,3
Г) Сделано заявление подозреваемым (обвиняемым) об алиби, которое связано с его телефонными соединениями;	33	25,6
Д) Необходимо определить круг знакомых лица;	31	24,0
Е) Следствию неизвестно кто совершил преступление, но есть информация о телефонных соединениях потерпевшего с предполагаемыми преступниками.	108	83,7

21. Для решения каких тактических задач использовались данные, полученные в ходе получения информации о соединениях между абонентами и (или) абонентскими устройствами?		
А) Получения информации о лице, совершившем преступление;	68	52,7
Б) Установления личности других участников преступления и свидетелей;	109	84,5
В) Выявления организованной преступной группы;	82	63,6
Г) Розыска лиц, причастных к совершению преступлений;	97	75,2
Д) Установления местопребывания и задержания подозреваемого;	113	87,6
Е) Выявления мест хранения похищенного имущества, орудий и средств преступления;	41	31,8
Ж) Выявления средств и способов сокрытия следов преступления;	13	10,1
З) Выявления неблагоприятных обстоятельств для расследования (характера противодействия расследованию и др.);	36	27,9
И) Проверки алиби;	75	58,1
К) Выявления признаков инсценировки;	22	17,1
Л) Выдвижения версий и планирования расследования;	78	60,5
М) Иное (укажите свой вариант ответа).		0,0
22. Как часто в процессе расследования преступлений Вы используете возможности производства тактической операции «Получение информации о соединениях между абонентами и (или) абонентскими устройствами»?		
А) Проводили тактическую операцию;	103	79,8
Б) Не проводили тактическую операцию.	26	20,2
23. Каким элементом тактической операции чаще всего выступает следственное действие, предусмотренное статьей. 186.1 УПК РФ?		0,0
А) Имеет центральное значение;	52	40,3
Б) Носит вспомогательный характер;	75	58,1
В) Не включается в тактические операции.	2	1,6
24. Используете ли Вы консультации со специалистами перед планированием и организацией получения информации о соединениях между абонентами и (или) абонентскими устройствами?		
А) Да, обязательно использую;	66	51,2

Б) Нет, не использую;	60	46,5
В) Затрудняюсь ответить.	3	2,3
25. Какие действия проводятся на подготовительном этапе указанного следственного действия?		
А) Выяснение абонентского номера и номера пользовательского оборудования;	107	82,9
Б) Установление идентификационного номера абонентского устройства (пользовательского оборудования) и абонентского номера;	98	76,0
В) Определение периода времени, за который необходимо получить информацию;	102	79,1
Г) Получение данных о принадлежности пользовательского оборудования;	76	58,9
Д) Выяснить у какого оператора связи или нескольких операторов связи запрашивать интересующие сведения;	89	69,0
Е) Вынесение и согласование следователем с руководителем следственного органа постановления о возбуждении перед судом ходатайства о производстве следственного действия;	116	89,9
Ж) Укажите, какие еще мероприятия необходимо провести в рамках подготовительного этапа.		
26. Какие действия следователь осуществляет на основном (рабочем) этапе указанного следственного действия?		
А) Направляет оператору сотовой связи разрешение суда о производстве получения информации о соединениях между абонентами и (или) абонентскими устройствами;	123	95,3
Б) Осматривает полученную детализацию и составляет протокол осмотра документа;	122	94,6
В) Непосредственно участвует при осуществлении конкретным сотрудником оператора сотовой связи технических действий по выборке и записи интересующей информации;	16	12,4
Г) Иные действия (укажите).		0,0
27. Каким образом проявляется взаимодействие следователя и оператора сотовой связи на основном (рабочем) этапе получения информации о соединениях между абонентами и (или) абонентскими устройствами?		
А) Взаимодействия не происходит;	31	24,0
Б) Только при передаче судебного решения;	120	93,0

В) Следователь лично присутствует при процедуре получения сведений оператором сотовой связи;	17	13,2
Г) Иное (укажите формы взаимодействия). (Устная консультация)	7	5,4
28. В какие сроки операторами связи предоставляют запрашиваемую информацию о соединениях между абонентами и (или) абонентскими устройствами?		
А) Операторы связи предоставляют запрашиваемую информацию в течение 7 рабочих дней;	25	19,4
Б) Операторы связи предоставляют запрашиваемую информацию в течение 10 дней;	20	15,5
В) Операторы связи предоставляют запрашиваемую информацию в течение 1 –го месяца;	34	26,4
Г) Обычно операторы связи предоставляют запрашиваемую информацию по каждому уголовному делу в течение 2-х месяцев;	17	13,2
Д) Операторы связи предоставляют запрашиваемую информацию не по каждому уголовному делу;	7	5,4
Е) Операторы связи предоставляют запрашиваемую информацию редко и с большими запозданиями;	17	13,2
Ж) Операторы связи предоставляют запрашиваемую информацию немедленно.	9	7,0
29. Если следователь принял решение о личном присутствии на техническом этапе получения информации об абонентах и (или) абонентских устройствах, то чем это обусловлено?		
А) Разъяснить работникам оператора связи цель и задачи данного получения информации о соединениях между абонентами и (или) абонентскими устройствами;	23	17,8
Б) Ускорить ознакомление с искомыми данными биллинга с целью оперативного решения задач предварительного расследования (то есть ознакомиться с этими данными до того, как осуществляющая услуги связи организация оформит надлежащим образом, упакует, опечатает документы с соответствующими данными биллинга, напишет к ним сопроводительное письмо и отправит все это следователю);	103	79,8
В) Укажите иные цели.	3	2,3

30. В каком виде оператор сотовой связи чаще всего предоставляет интересующую следователя информацию?		
А) На электронном носителе (диск, флеш-накопитель);	19	14,7
Б) В распечатанном виде;	17	13,2
В) В ином виде (укажите в каком).	1	0,8
31. С какими трудностями сталкивается следователь при осуществлении фиксации в протоколе осмотра документа полученной от оператора сотовой связи информации?		0,0
А) Необходимо выбирать имеющую значение для уголовного дела информацию из большого объема данных;	89	69,0
Б) Нехватка знаний в пользовании компьютерной техники при осмотре информации, представленной от оператора сотовой связи на электронном носителе;	8	6,2
В) Нет трудностей при осуществлении фиксации в протоколе осмотра документа полученной от оператора сотовой связи информации;	32	24,8
Г) Укажите, с какими трудностями Вы сталкивались при осуществлении осмотра и фиксации полученной от оператора сотовой связи информации.		
32. Каким образом фиксируются сведения, полученные от оператора сотовой связи в протоколе осмотра документа?		
А) Выбираются и фиксируются только имеющие значение для уголовного дела данные;	115	89,1
Б) Фиксируется весь объем предоставленной информации	14	10,9
В) Иное (укажите свой вариант).		
33. Привлекаете ли Вы специалиста после получения детализации или биллинговых данных? Если да, то какую помощь он оказывает?		
А) Помощь специалиста не требуется;	43	33,3
Б) Требуется помощь по работе с компьютером;	11	8,5
В) Требуется помощь специалиста (сотрудника компании сотовой связи) для консультации по представленной информации;	36	27,9
Г) Необходим специалист для фиксации хода следственного действия.	39	30,2
34. Всегда ли присутствуют понятые при составлении протокола осмотра документа?		

А) Да, всегда;	45	34,9
Б) Нет;	61	47,3
В) На усмотрение следователя.	23	17,8
35. Как часто происходит ознакомление обвиняемого с приобщенным в качестве вещественного доказательства электронным или бумажным носителем информации, полученной от оператора сотовой связи?		
А) Всегда;	73	56,6
Б) Никогда;		0,0
В) Редко, по желанию обвиняемого;	54	41,9
Г) Иное.	2	1,6
36. Используете ли Вы сведения, предоставленные оператором сотовой связи при производстве иных следственных действий?		0,0
А) Да	86	66,7
Б) Не использую, они, как правило, бесполезны	4	3,1
В) Использую только при допросе	39	30,2
Г) Укажите свой ответ.		
37. При проведении каких следственных и иных действий использовались результаты получения информации о соединениях между абонентами и (или) абонентскими устройствами?		
А) Допрос подозреваемого	115	89,1
Б) Допрос обвиняемого	120	93,0
В) Допрос свидетеля	104	80,6
Г) Допрос потерпевшего	96	74,4
Д) Очная ставка	48	37,2
Е) Укажите иные варианты ответа. (ОМП, проверка показаний на месте)	71	55,0
38. Для установления каких обстоятельств, подлежащих доказыванию, использовались сведения, полученные в результате получения информации о соединениях между абонентами и (или) абонентскими устройствами?		
А) События преступления	53	41,1
Б) Времени совершения преступления	86	66,7
В) Места преступления	109	84,5

Г) Состава и характеристики преступной группы	79	61,2
Д) Ролевых функций соучастников	57	44,2
Е) Виновности лица в совершенном преступлении	78	60,5
Ж) Наличия умысла	16	12,4
З) Характера и размера вреда, причиненного преступлением	0	0
И) Иное.	1	0,8
39. Каким образом влияет информация о соединениях между абонентами и (или) абонентскими устройствами на производство и ход допроса?		
А) никак не влияет;	3	2,3
Б) позволяет преодолеть противодействие;	61	47,3
В) используется в качестве подтверждения имеющихся сведений;	118	91,5
Г) предоставляется допрашиваемому для того, чтобы он вспомнил некоторые детали происшедшего;	42	32,6
Д) Укажите свой вариант ответа.		
40. Имела ли информация о соединениях между абонентами и (или) абонентскими устройствами существенное значение для раскрытия и расследования преступлений и доказывания обстоятельств, указанных в ст. 73 УПК РФ?		
А) Данная информация способствовала раскрытию и расследованию преступлений, а также доказыванию обстоятельств, указанных в ст. 73 УПК РФ;	106	82,2
Б) Данная информация носит второстепенный характер;	20	15,5
В) Данная информация для раскрытия, расследования и доказывания по уголовным делам не представляет никакого интереса.	3	2,3
41. С какими проблемами Вы сталкиваетесь при производстве следственного действия, предусмотренного статьей 186.1 УПК РФ?		0,0
А) Проблемы, связанные с получением судебного решения;	25	19,4
Б) Теряется много времени, что влияет на раскрытие преступления по горячим следам;	101	78,3
В) Оператор связи несвоевременно представляет запрашиваемую информацию	114	88,4
Г) Большой объем, представляемых сведений;	63	48,8
Д) Постоянно необходима помощь специалиста;	3	2,3

Е) Недостаточная законодательная регламентация статьи 186.1 УПК РФ, отсутствие рекомендаций по производству данного следственного действия;	13	10,1
Ж) Нет никаких трудностей в производстве рассматриваемого следственного действия;	2	1,6
З) Отсутствие в распоряжении следователя специальных аппаратно-программных комплексов (средств) предназначенных для осмотра и получения информации из мобильного телефона.	46	35,7
42. Как вы считаете, целесообразно ли расширять возможности данного следственного действия? Если да, то в каком направлении (например, возможность отражения содержательной части SMS-сообщении или контроль переписки и звонков, совершенных с помощью приложений на мобильном устройстве: Viber, Whatsapp и т.п.).		
А) Да;	126	97,7
Б) Нет.	3	2,3

Приложение 2

Результаты изучения уголовных дел, связанных с использованием средств сотовой связи, в процессе раскрытия и расследования преступлений

В ходе исследования были изучены 174 уголовных дела, расследовавшихся в период с 2011 по 2017 г.г., при расследовании которых применялось следственное действие, предусмотренное статьей 186.1 УПК РФ, либо использовалась информация об абонентах или их соединениях

№	Вопрос	Количество уголовных дел	%
1.	**Общее число изученных уголовных дел**	174	100%
2.	**Наименование органа, возбудившего уголовное дело**		
	Следователь ОВД РФ	86	49,4%
	Следователь СК РФ	19	10,9%
	Орган дознания	69	39,7%
3.	**Наименование преступления и статья УК РФ, по которой возбуждено уголовное дело**		
	Мошенничество (ст. 159 УК РФ)	29	16,7%
	Вымогательство (ст. 163 УК РФ)	11	6,3%
	Кража (ст. 158 УК РФ)	26	14,9%
	Убийство (ст. 105 УК РФ)	21	12,1%
	Грабеж (ст. 161 УК РФ)	16	9,2%
	Разбой (ст. 162 УК РФ)	10	5,7%
	Похищение человека (ст. 126 УК РФ)	4	2,3%
	Нарушение авторских и смежных прав (ст. 146 УК РФ)	2	1,1%
	Бандитизм (ст. 209 УК РФ)	17	9,8%

	Преступления, связанные с незаконным оборотом наркотических средств (ст. 228, 228.1, 228.1, 228.3, 228.4 УК РФ)	33	19%
	Взяточничество (ст. 290, 291, 291.1 УК РФ)	3	1,7%
	Заведомо ложное сообщение об акте терроризма	2	1,1%
4.	**В ходе производства каких следственных действий была получена информация об использовании средств сотовой связи?**		
	Получение информации о соединениях между абонентами и (или) абонентскими устройствами	121	69,5%
	Выемка распечатки телефонных соединений у потерпевшего (свидетеля)	16	9,2%
	Выемка SIM-карты, мобильного телефона, предметов и документов, содержащих IMEI- номер и другие технические характеристики средств мобильной связи	51	29,3%
	Допрос потерпевшего (свидетеля) или подозреваемого (обвиняемого)	88	50,6%
	Осмотр места происшествия	35	20,1%
	Обыск	28	16,1%
	Осмотр предмета (абонентского устройства, SIM-карты, коробки от устройства связи)	34	19,5%
	Контроль и запись переговоров	23	13,2%
5.	**Какие объекты, непосредственно содержащие информацию об абонентах и абонентских устройствах, изымались в ходе расследования уголовного дела?**		
	Сотовый телефон	56	32,2%

	Компьютер, ноутбук, нетбук, планшеты и т.п. устройства, в которых функция телефонных переговоров существует как дополнительная	19	10,9%
	SIM-карта, флеш-карта, компакт диск, иной съемный носитель информации	66	37,9%
	Распечатка детализации телекоммуникационных контактов определенного абонента (абонентского устройства)	16	9,2%
	Упаковка для сотовых телефонов, SIM-карта, иных предметов, другие аксессуары	51	29,3%
6.	**В отношении каких участников расследования запрашивали информации о соединениях между абонентами и (или) абонентскими устройствами у оператора сотовой связи**		
	Потерпевший	117	67,2%
	Свидетель	38	21,8%
	Подозреваемый (обвиняемый)	163	93,7%
	Иное лицо	9	5,2%
7.	**Проводилась ли компьютерно-техническая экспертиза абонентского устройства связи**		
	Да	11	6,3%
	Нет	163	93,7%
8.	**Для решения каких тактических задач использовалась информация о соединениях между абонентами и (или) абонентскими устройствами в процессе расследования по уголовному делу**		

	Получения информации о лице, совершившем преступление	159	91,4%
	Установления личности других участников преступления и свидетелей	123	70,7%
	Выявления организованной преступной группы	41	23,6%
	Розыска лиц, причастных к совершению преступлений	97	55,7%
	Установления местопребывания и задержания подозреваемого	76	43,7%
	Выявления мест хранения похищенного имущества, орудий и средств преступления	82	47,1%
	Выявления средств и способов сокрытия следов преступления	59	33,9%
	Проверки алиби	98	56,3%
	Выявления признаков инсценировки	17	9,8%
9.	**Ситуации, использования средства сотовой связи**		
	Сотовый телефон использовался как средство совершения преступления	64	36,8%
	Сотовый телефон использовался для связи между преступниками	112	64,4%
	Сотовый телефон выступает предметом посягательства	52	29,9%
	Использование средства связи не связано с совершением преступления	4	2,3%
10.	**Для установления, каких обстоятельств, подлежащих доказыванию, использовались сведения, полученные в результате получения информации о соединениях между абонентами и (или) абонентскими устройствами?**		
	События преступления	63	36,2%

	Времени совершения преступления	114	65,5%
	Места преступления	36	20,7%
	Состава преступной группы	71	40,8%
	Ролевых функций соучастников	17	9,8%
	Виновности лица в совершенном преступлении	109	62,6%
	Способ совершения преступления	64	36,8%

Приложение 3

ГУ МВД России по Пермскому краю
Межмуниципальный отдел
Министерства внутренних дел
Российской Федерации
« Соликамский»
(реализующий задачи и функции органов внутренних дел на территории Соликамского городского округа и Соликамского муниципального района)
(Межмуниципальный отдел
МВД России «Соликамский»)
ул. Соликамское шоссе, 2а Соликамск, 618540
тел. (34253) 5-41-00

_____ № _____
на № _____ от _____

Директору Пермского филиала
ООО «Т2-Мобайл»
г. Пермь ул. Шоссе Космонавтов, 111 корп. 43

В Следственном отделе Межмуниципального отдела МВД России «Соликамский» находится уголовное дело № 11701570005000877 возбужденное по факту незаконного сбыта наркотического средства, а именно: в неустановленное время до 17.06.2017 года неустановленное лицо в неустановленном месте незаконно сбыло Иванову И.И. наркотическое средство - производное N-метилэфедрона общей массой 0,195 граммов.

В ходе следствия было установлено, что неустановленное лицо пользовалось абонентским номером 89025595132.

Следствию необходимо установить владельца SIM-карты с абонентским номером 89025595132 за период с 01.06.2017 по настоящее время, и есть ли возможность предоставления информации о детализации входящих и исходящих соединений за период с 01.06.2017 до настоящего времени по указанному абонентскому номеру.

На основании части 5 ст. 64 Федерального закона от 07.07.2003 года № 126-ФЗ «О связи», части 4 ст. 21 УПК РФ прошу Вас сообщить на кого был зарегистрирован абонентским номер 89025595132 за период с 01.06.2017 по настоящее время.

Начальник СО МО МВД России «Соликамский»
подполковник юстиции Самойлов А.А.

исп. Петров А.В.
р.т. 8(34253) 6-23-15

Приложение 4

« СОГЛАСЕН »
Начальник СО МО
МВД России «Соликамский»
полковник юстиции
Б.Н. Уваров
«20» февраля 2016 г.

П О С Т А Н О В Л Е Н И Е
о возбуждении перед судом ходатайства о производстве получения информации о соединениях между абонентами и (или) абонентскими устройствами

г. Соликамск «20» февраля 2016 г.

Ст. следователь СО МО МВД России «Соликамский» Жданова А.Б., рассмотрев материалы уголовного дела № 532,

У С Т А Н О В И Л:

23.07.2015 года неизвестный путем производства закладки у здания ВКУ СИЗО-2 ГУФСИН России по Пермскому краю по ул. 20 лет Победы, 15 г. Соликамска, незаконно сбыл Сидрову С.С. наркотическое средство – N- метилэфедрон массой 0,782 граммов, в значительном размере.

В ходе следствия установлено, что Сидоров С.С. для приобретения наркотического средства использовал сотовый телефон с абонентским номером 89025595132.

Следствию необходимо установить владельцев сим-карты абонентский номер 89025595132, которые пользовались данным номером, а также географическое положение, исходящие и входящие звонки данного абонента в период с 10.07.2015 года по 31.07.2015 года.

На основании изложенного, руководствуясь ст. 183 ч. 3, 186.1 УПК РФ,

П О С Т А Н О В И Л:

1. Ходатайствовать перед Соликамским городским судом о получении информации о владельцах сим-карты с абонентским номером 89025595132, владельцах сим-карты с абонентским номером 89822551268, а также географического положения, исходящих и входящих звонков данных абонентов в период с 10.07.2015 года по 31.07.2015 года.

2. Техническое осуществление получения информации о соединениях между абонентами и (или) абонентскими устройствами поручить:

- ПАО «МТС»

3. Оператору связи ПАО «МТС» предоставить истребуемую информацию в течении 10 суток с момента поступления постановления суда.

Ст. следователь
СО МО МВД России
«Соликамский» Жданова А.В.

Приложение 5

ПРОТОКОЛ

осмотра предметов (документов)

город Соликамск “ 11 ” июля 2017 г.
(место составления)

Осмотр начат в ____ ч ____ мин
Осмотр окончен в ____ ч ____ мин

Следователь СО МО МВД России «Соликамский»
старший лейтенант юстиции Петров И.И.

в присутствии понятых:

1. В соответствии с ч.1.1 ст.170 УПК РФ осмотр проводился без понятых
(фамилия, имя, отчество
проводилась фотосьемка
и место жительства понятого)
2. В соответствии с ч.1.1 ст.170 УПК РФ осмотр проводился без понятых
(фамилия, имя, отчество
проводилась фотосьемка
и место жительства понятого)

с участием* _____

в соответствии со ст.164, частью первой ст.176, частями первой-четвертой и шестой ст.177 УПК РФ произвел осмотр в каб. 100 МО МВД России «Соликамский» детализации звонков абонента № 89025595132, сотового телефона «Iphone» черного цвета
(где и чего именно)

Перед началом осмотра участвующим лицам разъяснены их права, обязанности и ответственность, а также порядок производства осмотра предметов (документов).

Понятым, кроме того, до начала осмотра разъяснены их права, обязанности и ответственность, предусмотренные ст.60 УПК РФ.

_____
(подпись понятого)

_____
(подпись понятого)

Специалисту (эксперту) не привлекался
(фамилия, имя, отчество)
разъяснены его права, обязанности и ответственность, предусмотренные ст.58 (57) УПК РФ.

_____
(подпись специалиста (эксперта)

Участвующим лицам также объявлено о применении технических средств _____
персональный компьютер, принтер, фотоаппарат
(каких именно, кем именно)

Осмотр производился в условиях искусственного освещения _____

(освещенность)

Осмотром установлено:

1)Детализация входящих и исходящих соединений абонента № 89124994831 выполнена на 5 листах формата А4 за период с 15.05.2017 по 20.05.2017 года. Детализация имеет графы «дата и время; сервис; Номер телефона; продолжительность; «стоимость».

Имеются соединения с абонентским номером **79194511135 (номер Смолова**), а именно: **15.05.2017** года в 21:39:55, 21:49:00 - телефонные звонки; **16.05.2017 года** в 16:27:31, 16:28:15, 17:57:32, 18:05:05, 18:09:44, 21:58:34 - телефонные звонки; **17.05.2017 года** в 14:11:08, 21:24:36, 21:36:18- телефонные звонки; **18.05.2017 года** в 19:54:23, 19:55:02, 23:05:19, 23:12:40- телефонные звонки; **19.05.2017 года** в 12:35:42, 17:34:34, 17:39:03, 17:41:23- телефонные звонки.

Имеются соединения с абонентским номером **79519295649 (номер Ляхова),** а именно: **16.05.2017 года** в 09:10:05 – телефонный звонок; **17.05.2017 года** в 20:39:38 – телефонный звонок; **18.05.2017 года** в 20:30:59 – телефонный звонок; **19.05.2017** года в 9:03:19, 12:37:06 – телефонные звонки; **20.05.2017 года** в 22:55:14, 23:03:30 – телефонные звонки.

Другие соединения с другими абонентскими номерами не имеют значения по уголовному делу.

2) сотовый телефон «Iphone» в корпусе черного цвета, телефон имеет 1 SIM-карту, IMEI: 355668079952052. При включении данного телефона, на экране появляется клавиатура с просьбой ввести код для разблокировки телефона, при введении кода «025766» телефон разблокировался и открывается рабочий стол телефона с мобильными приложениями, при открытии мобильного приложения «В контакте». В папке сообщения переписка с контактом «Denis Sokolovskii» пуста. При открытии и просмотре контактов сотового телефона установлено, что имеются контакты: «Дэн»-89519295649, и «Смал»- 89194511135; другие контакты не имею значение для уголовного дела.

Другой информации имеющей значение для уголовного дела в телефоне не имеется.

В ходе осмотра проводилась фотосъемка

К протоколу осмотра фототаблица прилагаются

(фототаблицы и т.п.)

Перед началом, в ходе либо по окончании осмотра от участвующих лиц

заявления не поступили Содержание заявлений:

(поступили, не поступили)

Протокол прочитан лично

(лично или вслух следователем (дознавателем)

Замечания к протоколу нет

(содержание замечаний либо

Настоящий протокол составлен в соответствии со ст.166 и 167 УПК РФ.

Следователь

(подпись)

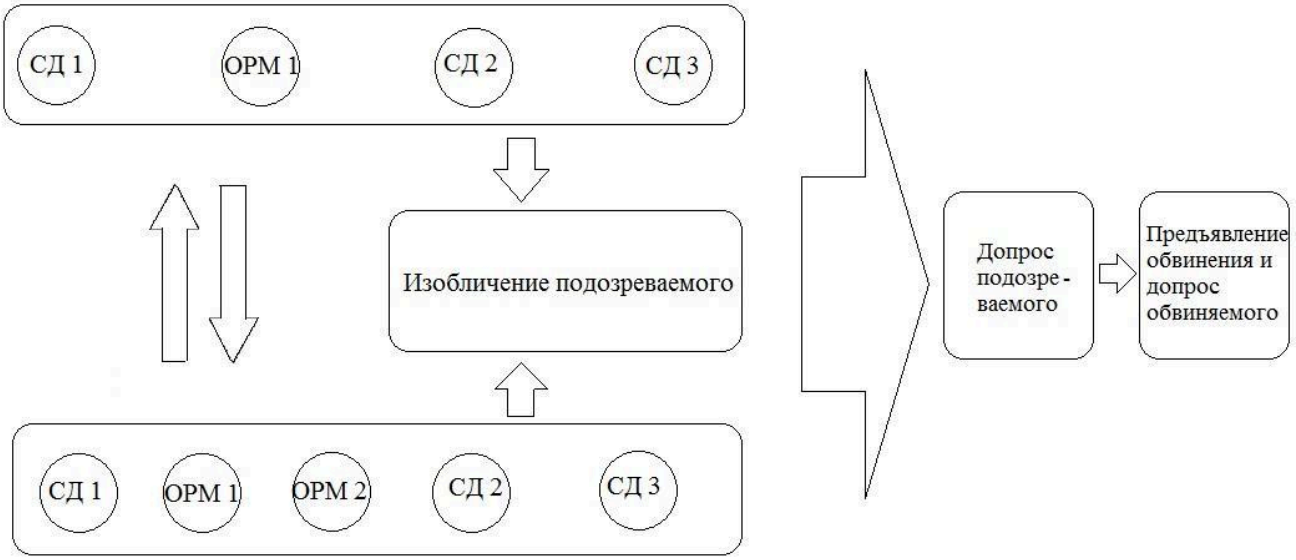
Приложение 6

Схема тактической операции по установлению лиц, причастных к совершению преступления



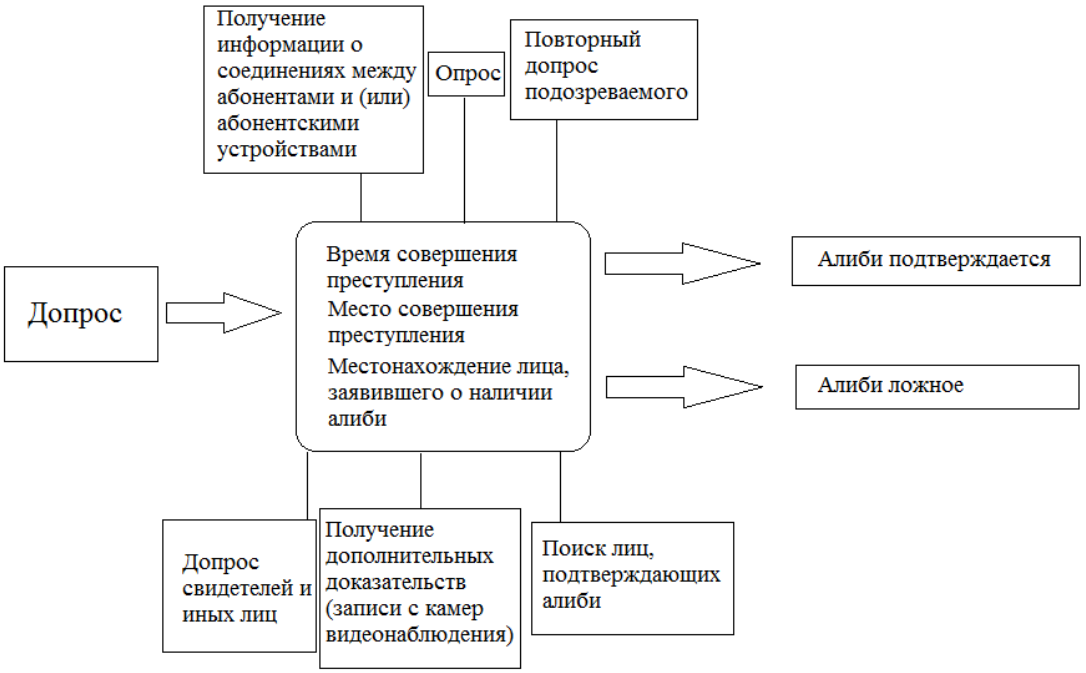
Приложение 7

Схема тактической операции по изобличению подозреваемых (обвиняемых)



Приложение 8

Схема тактической операции по проверке алиби лица



Приложение 9

Схема тактической операции по проверке признательных показаний подозреваемого (обвиняемого) и других лиц



Приложение 10

ФОТОТАБЛИЦА

к протоколу осмотра вещей и предметов по уголовному делу № 1345 от 02.10.2016 года по факту открытого хищения имущества гр. Рамель Н.Г.

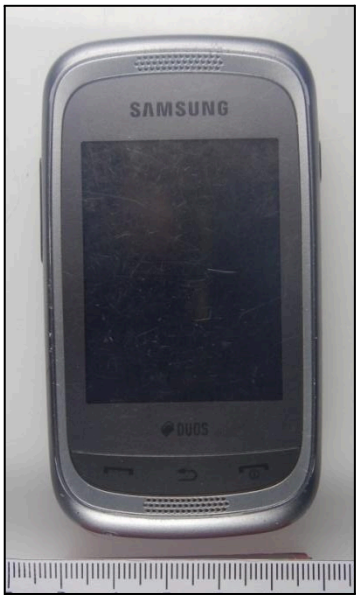


Фото 1. Лицевая сторона сотового телефона «Самсунг».



Фото 2. Оборотная сторона сотового телефона «Самсунг».

Специалист Петрова О.Т.



Фото 3. Общий вид крышки, аккумуляторной батареи и оборотной стороны телефона.



Фото 4. Номера «IMEI» телефона.

Специалист Петрова О.Т.



Фото 5. Банковские карты с лицевой стороны.



Фото 6. Банковские карты с оборотной стороны.

Специалист Петрова О.Т.