

ООО «ОПТИМА ПРОФ»

Ю. Н. Соколов

ЭЛЕКТРОННОЕ НАБЛЮДЕНИЕ
В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ
И ОПЕРАТИВНО-РОЗЫСКНОЙ
ДЕЯТЕЛЬНОСТИ

Екатеринбург
ООО «Оптим Проф»
2006

УДК 343.2
ББК Х881
С594

Научный редактор С. Д. М и л и ц и н, кандидат юридических наук,
доцент (Уральская государственная юридическая академия)

Рецензенты:

В. К. Г а л о, заслуженный юрист РФ, доктор юридических наук,
профессор (Алтайский государственный университет); В. Н. Б у т о в, док-
тор юридических наук, профессор (Уральский государственный экономи-
ческий университет)

Соколов Ю. Н.

С594 Электронное наблюдение в уголовном судопроизводстве и опе-
ративно-розыскной деятельности / Ю. Н. Соколов. — Екатеринбург:
ООО «Оптима Проф», 2006. — 164 с.

ISBN 5-902-968-03-8

Рассматриваются основные направления развития правовой основы при-
менения электронного наблюдения в информационной сфере обращения,
хранения, производства, передачи и потребления информации как в уго-
ловном производстве, так и в оперативно-розыскной деятельности.

Книга предназначена для студентов, аспирантов и преподавателей юри-
дических специальностей вузов, а также юристов-практиков и сотрудни-
ков правоприменительных органов.

УДК 343.2
ББК Х881

ОГЛАВЛЕНИЕ

Введение	4
Глава 1. Основные особенности электронного наблюдения	
§ 1. Понятие электронного наблюдения	8
§ 2. Нормативно-правовая основа электронного наблюдения	23
§ 3. Виды электронного наблюдения	29
Глава 2. Электронное наблюдение в оперативно-розыскной деятельности	
§ 1. Информация и электронное наблюдение	36
§ 2. Электронное наблюдение как комплексное оперативно-розыскное мероприятие	42
§ 3. Использование оперативно-розыскной информации, полученной в ходе проведения электронного наблюдения, в доказывании по уголовным делам	62
Глава 3. Электронное наблюдение в уголовном судопроизводстве	
§ 1. Электронное наблюдение как следственное действие	101
§ 2. Использование результатов электронного наблюдения в процессе доказывания по уголовным делам	124
Заключение	138
<i>Приложения</i>	145
Список литературы	153

ВВЕДЕНИЕ

Современный этап развития Российской Федерации характеризуется не только глубокими политическими, социальными, экономическими, но также и правовыми изменениями. Криминологические прогнозы последних лет не вселяют в сердца россиян оптимизма: криминальность общества из правоприменительной проблемы может превратиться в насущную социальную, а следовательно, и политическую проблему.

Сегодня уже никто не станет отрицать, что наличие в нашей стране групп профессиональных преступников, террористов, незаконных вооруженных формирований, организованной преступности становится реальной угрозой безопасности общества.

Установление фактических обстоятельств совершенного преступления является ретроспективным, т. е. обращено в прошлое, и картина происшедшего, как правило, восстанавливается по следам, оставленным преступлением в памяти людей и на предметах материального мира. Но когда опытные преступники (нередко с помощью квалифицированных специалистов) заранее принимают меры к тому, чтобы таких следов не оставить, а оставленные — уничтожить, надежд на раскрытие преступлений только процессуальными средствами остается мало.

Жизнь наглядно показывает, что такие преступления, как терроризм, захват заложников, убийство по найму, взяточничество или вымогательство, незаконное изготовление, приобретение, хранение, перевозка, пересылка либо сбыт наркотических средств или психотропных веществ, незаконное приобретение, передача, сбыт, хранение, перевозка или ношение оружия, его основных частей, боеприпасов, взрывчатых веществ и взрывных устройств, чисто следственным путем раскрыть зачастую не удается. Практика по-

следних лет свидетельствует, что успех борьбы с такого рода преступлениями обеспечивается только применением наряду с процессуальными средствами методов оперативно-розыскной деятельности. Использование таких методов позволяет не ограничиваться тем, чтобы только идти по следам преступников, реагируя на заявления и иные сообщения о совершенном преступлении, и уже после этого отыскивать источники фактической информации, а с помощью различных оперативно-розыскных мероприятий дает возможность выявлять и пресекать преступления на самом раннем этапе их совершения, а если предотвратить преступное деяние не удалось, — задерживать виновных в максимально короткие сроки.

Проблема доказывания в уголовном судопроизводстве относится к числу, так сказать, вечных. Доказывание (выявление, фиксация/закрепление, проверка и оценка доказательств) — важнейший элемент, сердцевина уголовного процесса. Тема доказательств и доказывания предполагает постоянное развитие. Сегодня многие из традиционных способов раскрытия, расследования преступлений и разбирательства уголовных дел судом оказываются недостаточными, часто не срабатывают.

Между тем в правоприменительной практике материалы электронного наблюдения все чаще используются в доказывании по уголовным делам. Ряд ученых регулярно высказывают пожелания о возможности такого применения результатов оперативно-розыскной деятельности в названных целях, что и является одной из актуальных проблем в современном уголовном судопроизводстве¹.

¹ См., например: *Мингалин Н. Н.* Контроль и запись переговоров в системе следственных действий // *Следователь.* 2003. № 12; *Громов Н. А.* Доказательства, доказывание и использование результатов оперативно-розыскной деятельности / *Громов Н. А., Пономаренков В. А., Гущин А. Н.* и др. М., 2001; *Громов Н. А.* Доказательства, доказывание и использование результатов оперативно-розыскной деятельности / *Громов Н. А., Гущин А. Н., Луговец Н. В.* и др. М., 2006; *Поляков М. П.* Уголовно-процессуальное использование результатов оперативно-розыскной деятельности / *Поляков М. П., Попов А. П., Попов Н. М.* Пятигорск, 1998; *Доля Е. А.* Использование в доказывании результатов оперативно-розыскной деятельности. М., 1996; *Зажицкий В. И.* Связь оперативно-розыскной деятельности и уголовного процесса // *Государство и право.* 1995. № 6; *Бедняков Д. И.* О реализации оперативно-розыскной информации в процессе доказывания и особенности ее оценки // *Проблемы надежности доказывания в советском уголовном процессе.* М., 1984; и др.

Кроме того, в последние годы в результате принятия Конституции Российской Федерации (далее — Конституция РФ)², Федерального закона РФ от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности» (далее — Федеральный закон «Об оперативно-розыскной деятельности»)³, Уголовно-процессуального кодекса Российской Федерации (далее — УПК РФ)⁴, а также использования новейших технологий по обработке, хранению и передаче информации в различных сферах человеческой деятельности проявился ряд других проблемных моментов, на которые ни теория, ни практика пока должным образом не ответили. К ним, в частности, относятся следующие:

- недостаточность нормативного регулирования на законодательном уровне, «сухость» и нечеткость правовых норм в регламентации порядка проведения оперативно-розыскных мероприятий на современных телекоммуникационных системах и средствах связи, а также введения полученных результатов в уголовный процесс;

- несовершенство перечня оперативно-розыскных мероприятий, приведенного в ст. 6 Федерального закона «Об оперативно-розыскной деятельности», который морально устарел и не учитывает специфику новых методов передачи информации; содержание оперативно-розыскных мероприятий не раскрыто, что становится особенно актуальным при ограничении конституционных прав граждан, затрагивающих неприкосновенность их частной жизни;

- конкуренция норм Федерального закона «Об оперативно-розыскной деятельности» и Федерального закона РФ от 7 июля 2003 года № 126-ФЗ «О связи» (далее — Федеральный закон «О связи»)⁵. Если ранее ст. 14 Федерального закона РФ от 16 февраля 1995 года № 15-ФЗ «О связи»⁶ прямо предписывала операторам связи оказывать помощь субъектам оперативно-розыскной деятельности в проведении оперативно-розыскных мероприятий на сетях связи общего пользования, то в п. 4 ст. 64 новой редакции названного закона такого указания не содержится. Законодатель использует

бланкетную норму, переводя порядок взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, на подзаконный уровень;

- недостаточная регламентация в УПК РФ правоотношений, возникающих между уполномоченными государственными органами и операторами связи при оказании содействия первым в проведении следственных действий на сетях электросвязи России.

Таким образом, имеющиеся пробелы в уголовно-процессуальном законе, неопределенность в вопросах, связанных с ограничением конституционных прав граждан при проведении оперативно-розыскных мероприятий и следственных действий с помощью современных телекоммуникационных систем и средств связи, не способствуют единообразному применению действующих норм права.

В книге предпринята попытка обозначить основные направления развития правовой основы применения электронного наблюдения в информационной сфере обращения, хранения, производства, передачи и потребления информации как в уголовном судопроизводстве, так и в оперативно-розыскной деятельности.

² Российская газета (Рос. газ.). 1993. 25 дек.

³ Там же. 1995. 18 авг.

⁴ Собр. законодательства РФ. 2001. № 52. Ст. 4921.

⁵ Рос. газ. 2003. 10 июля. (Закон вступил в силу 1 января 2004 года.)

⁶ Там же. 1995. 22 февр. (Закон утратил силу.)

ГЛАВА 1

ОСНОВНЫЕ ОСОБЕННОСТИ ЭЛЕКТРОННОГО НАБЛЮДЕНИЯ

§ 1. Понятие электронного наблюдения

Предпосылкой возникновения электронного наблюдения можно считать подслушивание разговоров — один из наиболее древних методов добывания информации. Первоначально контроль речевой информации осуществлялся непосредственным способом, т. е. путем использования слухового аппарата человека. Существенным недостатком данного способа являлось то, что он позволял улавливать речевые сигналы человека на небольшом расстоянии.

Важной вехой в развитии контроля переговоров между людьми стала разработка устройств, позволяющих людям разговаривать друг с другом на расстоянии, что связано с появлением в XIX веке проводной телефонной связи. Первый телефонный разговор состоялся 10 марта 1876 года, а в 1883 году была открыта телефонная связь между Бостоном и Нью-Йорком¹.

Одновременно с появлением нового вида связи возникла идея использования технических средств для тайного прослушивания телефонных переговоров, особенно в сфере политики, дипломатии и военного дела. Несмотря на отсутствие специальных технических средств, позволяющих реализовать эту идею, данный вопрос небезуспешно решался и в России. Тогда к каждой телефонной станции был прикреплен человек, в чьи обязанности входило время

¹ См.: Гаврилин Ю. В., Дубонос Е. С. Использование контроля и записи телефонных и иных переговоров в раскрытии и расследовании преступлений: Учеб. пособие. М., 2003. С. 5.

от времени поднимать параллельно подключенную телефонную трубку и слушать разговоры².

После Октябрьского переворота новое правительство особое значение придавало контролю за телефонной и телеграфной связью. В апреле 1918 года В. И. Ленин отмечал: «Социализм без почты, телеграфа, машин — пустейшая фраза»³. В декабре 1918 года было утверждено Положение о военной цензуре, которое ввело контроль над всей печатной продукцией, радио, телеграфом и телефоном, и особенно за международными телефонными переговорами⁴.

В дальнейшем система тотального сбора информации непрерывно расширялась. В связи с этим в приказе Народного комиссариата внутренних дел СССР от 29 декабря 1939 года отмечалось: «Все без исключения международные телефонные переговоры, как сотрудников иностранных посольств, так и инкорреспондентов брать на контроль путем звукозаписи и стенографирования»⁵.

В конце 30-х годов XX века прослушивание телефонных переговоров получило широкое распространение и в Германии. Немецкая система прослушивания считалась одной из лучших в мире (не отставали в этом плане и США с Великобританией). Приход к власти нацистов превратил практику контроля переговоров в особую индустрию. Для совершенствования данного направления деятельности была создана специальная организация, получившая название Научно-исследовательского института Германа Геринга. Институт контролировал телефонные и телеграфные сети, а также радиосвязь⁶.

² См. об этом: Панченко М., Колтакиди А. Уши Лубянки // Версия. 2001. 22—28 мая. С. 11.

³ Ленин В. И. Заключительное слово по докладу об очередных задачах Советской власти // Полн. собр. соч.: В 42 т. 4-е изд. Т. 36. С. 272.

⁴ Положение о военной цензуре (Прил.: Перечень сведений, подлежащих предварительному просмотру военной цензурой; Перечень сведений, не подлежащих распространению путем почтово-телеграфных сообщений; Штаты военно-цензурных отделений. Утверждено приказом Российской Военной Социалистической Республики от 23 дек. 1918 г. № 346. [Электрон. ресурс]. Режим доступа: <http://www.vif2/ru/users/offtopic/vio/VIO/IST16.htm>.

⁵ Цит. по: Гаврилин Ю. В., Дубонос Е. С. Использование контроля и записи... С. 6.

⁶ См.: Деларю Ж. История гестапо / Пер. с фр. Ю. А. Немешаева и др. Смоленск, 1998. С. 133.

Развитие системы контроля и записи переговоров в СССР в последние десятилетия его существования связано с отнесением в 1973 году данного мероприятия исключительно к компетенции Комитета государственной безопасности. Вопрос о санкционировании прослушивания переговоров граждан, как правило, решался лично руководителями органов безопасности⁷ и, надо думать, совместно с партийными структурами КПСС.

Первую попытку процессуальной регламентации контроля (прослушивания) и записи переговоров законодатель предпринял 12 июня 1990 года, когда Основы уголовного судопроизводства Союза ССР и союзных республик дополнили ст. 35-1, в которой перечислялись основания и предусматривался общий порядок проведения рассматриваемых действий⁸. Тогда же союзные республики обязали внести соответствующие дополнения в республиканский УПК. Однако в УПК РСФСР этого не было сделано, что породило дискуссию о правовой природе нового доказательственного средства и допустимости использования его результатов в доказывании.

Закон РФ «Об оперативно-розыскной деятельности» от 13 марта 1992 года № 2506-1⁹ создал прочную правовую основу прослушивания телефонных и иных переговоров, но только для оперативно-розыскных органов, что позволяло им получать изобличающую информацию, способствующую предупреждению и раскрытию преступлений, розыску преступников, возмещению материального ущерба. Изменился порядок санкционирования рассматриваемого оперативно-розыскного мероприятия. Если Закон РФ «Об оперативно-розыскной деятельности» допускал прослушивание телефонных переговоров только с санкции прокурора, то с принятием Конституции РФ и новой редакции Федерального закона «Об оперативно-розыскной деятельности» от 12 августа 1995 года № 144-ФЗ — на основании постановления суда.

⁷ См. об этом материалы сайта «Московские новости»: <http://www.mn.ru>.

⁸ См.: Закон СССР от 12 июня 1990 года «О внесении изменений и дополнений в Основы уголовного судопроизводства Союза ССР и союзных республик» // Бюл. Глав. следств. упр. МВД СССР. 1990. № 4. С. 91.

⁹ Рос. газ. 1992. 29 апр.

Так, за шесть месяцев 1995 года федеральными судьями было рассмотрено 9106 ходатайств субъектов оперативно-розыскной деятельности о прослушивании телефонных переговоров¹⁰.

Проведение контроля телефонных переговоров в интересах следственных органов могло осуществляться только после возбуждения уголовного дела, применялось крайне редко и исключительно путем дачи органам дознания обязательного для исполнения поручения о проведении оперативно-розыскных и следственных действий в соответствии со ст. 119 УПК РСФСР.

Законодательная интерпретация контроля и записи переговоров исключительно как оперативно-розыскного мероприятия существенно сужала сферу его применения. Изменения такого положения наступили после внесения дополнения в УПК РСФСР (ст. 174-1 «Контроль и запись переговоров»)¹¹. Контроль и запись телефонных и иных переговоров допускались по уголовным делам о тяжких и особо тяжких преступлениях на основании судебного решения в отношении обвиняемого, подозреваемого и других лиц, которые могли располагать сведениями о преступлении либо иными сведениями, имеющими значение для уголовного дела. Теперь уже следователь мог самостоятельно выполнять указанное следственное действие либо поручить его производству органу дознания. Таким образом, получение информации, передаваемой по телефону или иному переговорному устройству, с целью раскрытия и расследования преступлений стало возможно оперативно-розыскным и уголовно-процессуальным путем.

Дополнение к УПК РСФСР просуществовало недолго, современное закрепление на законодательном уровне контроля и записи переговоров как следственного действия произошло в ст. 186 УПК РФ.

¹⁰ См.: Диденко В. И. Использование следователем фактических данных, полученных в результате применения в оперативно-розыскной деятельности аудио- и видеозаписи, фото- и киносъемки: Автореф. дис. ... канд. юрид. наук. М., 1996. С. 22.

¹¹ Федеральный закон РФ от 20.03.2001 г. № 26-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты РФ в связи с ратификацией Конвенции о защите прав человека и основных свобод» // Рос. газ. 2001. 23 марта.

Однако ни Федеральный закон «Об оперативно-розыскной деятельности», ни УПК РФ не учитывают специфики современных телекоммуникационных средств связи при проведении вышеназванных оперативно-розыскных мероприятий и следственного действия.

В чем же эта специфика? В первую очередь необходимо обратить внимание на следующие моменты. Современные технологии связи не ограничиваются телефонными и иными переговорами. Информация производится, транслируется, хранится и потребляется в самой разнообразной форме. Большая ее часть передается в электронном виде или с использованием цифровых средств связи. То, что ранее понималось под устным сообщением (телефонный разговор), сегодня таковым не является. Человеческий голос проходит многочисленные изменения и весьма далек от своего оригинала. Контроль и запись переговоров по своему объему не охватывают тех сообщений, которые не могут быть восприняты органами слуха человека, а именно информация, передаваемая по документальным сетям электросвязи, пейджинговые сообщения, иные переговоры с использованием цифровых технологий. Информация, которая может быть получена при проведении такого оперативно-розыскного мероприятия, как снятие информации с технических каналов связи, в рассматриваемое следственное действие не входит, что существенно ограничивает возможности следователя.

Если бы в Федеральном законе «Об оперативно-розыскной деятельности» вышеназванная специфика передачи информации была учтена, то следователь, как и раньше, мог бы дать поручение правоприменительным органам на проведение тех или иных оперативно-розыскных мероприятий, а представленные материалы в случае необходимости приобщить к уголовному делу в соответствии с действующим УПК РФ. Однако предусмотренные названным федеральным законом оперативно-розыскные мероприятия, такие как прослушивание телефонных переговоров и снятие информации с технических каналов связи, также не охватывают современные формы передачи информации. Как быть с сообщением, в котором присутствует, например, голосовая и визуальная информация? К какому виду оперативно-технического мероприятия отнести контроль информации, передаваемой по сетям документальной связи или радиосвязи? Контроль сообщений, передаваемых посредством элект-

ронной почты и содержащих вложенные видео- и звуковые файлы? Что это за оперативно-техническое мероприятие? Контроль почтовых отправок, телеграфных и иных сообщений, прослушивание телефонных переговоров, снятие информации с технических каналов связи, а может быть, наблюдение в электронной его составляющей? Однозначно не ответишь. Как правило, присутствуют признаки всех названных видов оперативно-розыскных мероприятий. На все поставленные вопросы постараемся ответить в ходе дальнейшего изложения.

За последнее десятилетие телекоммуникационные технологии прочно вошли в жизнь россиян. Миллионы граждан Российской Федерации ежедневно часами просиживают перед компьютерами, получая и отправляя электронную почту, пополняя базы данных различной направленности и участвуя в других бесчисленных операциях по передаче самой разнообразной информации.

К сожалению, тот, кто совершает преступление, не остается в стороне от информационной революции. Все большее число преступников для совершения противоправной деятельности используют современные средства связи. Например, Интернет используется далеко не в информационных целях. Здесь и хакерские атаки на уязвимые компьютерные сети физических и/или юридических лиц, шантаж, мошенничество, распространение компьютерных вирусов, передача изображений порнографической направленности и т. д.¹²

¹² Распространение порнографических материалов, в т. ч. и детской порнографии, через Интернет приобретает поистине катастрофический характер. Операторы связи, оказывающие услуги по доступу во Всемирную паутину на территории России, даже не пытаются осуществить настройку экранов-препятствий для выхода на порносайты. Сегодня достаточно набрать в строке поиска информации слова «детская порнография» или просто «ДП», как любая поисковая машина выдает список электронных адресов на нескольких десятках страниц.

Во всем цивилизованном мире подобные деяния уголовно наказуемы. В США и Италии действуют специальные подразделения полиции, основным видом деятельности которых является выявление и изобличение лиц, занимающихся распространением и/или хранением детской порнографии. Наказание, применяемое к виновным, является очень суровым (как правило, это лишение свободы на 10 и более лет). В Китае, например, за подобные деяния предусмотрена смертная казнь. В России ответственность наступает только за распространение и изготовление подобной «продукции».

Представляется, что со временем в сфере компьютерных сетей, в том числе глобальных, с большой вероятностью можно ожидать увеличения числа правонарушений. И если уже сейчас не начать самым активным образом бороться с криминализацией Интернета, то в недалеком будущем нам придется пожинать горькие плоды собственной беспечности.

Чтобы оценить криминогенный потенциал Всемирной паутины, В. В. Голубев предлагает обратиться к УК РФ. По его мнению, посредством эксплуатации возможностей сети могут совершаться самые разнообразные преступления. Он утверждает, что постепенно компьютеризируются многие процессы жизнеобеспечения людей. Сегодня нельзя исключить даже совершения убийства посредством компьютерной техники (преступник может, к примеру, ввести искажения в программу изготовления лекарственных препаратов и в результате добиться смерти пациента медицинского учреждения). Реально осуществление и многих других деяний, признаваемых преступными. Некоторые хакеры утверждают, что им под силу все, кроме изнасилования¹³.

Самое поверхностное знакомство с Интернетом позволяет с полной уверенностью предположить, что помимо выявляемых уголовно наказуемых деяний посредством сети уже сейчас совершается немало других преступлений, признаки состава которых при желании могут быть обнаружены в Интернете. В частности, предусмотренные УК РФ: клевета (ст. 129), оскорбление (ст. 130), нарушение неприкосновенности частной жизни (ст. 137), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138), нарушение авторских и смежных прав (ст. 146), нарушение изобретательских и патентных прав (ст. 147), незаконное предпринимательство (ст. 171), незаконное распространение порнографических материалов или предметов (ст. 242), возбуждение национальной, расовой или религиозной вражды (ст. 282) и др.

Наконец, вероятно использование злоумышленниками всемирной компьютерной сети для незаконного получения и разглашения

¹³ Подробнее об этом см.: Голубев В. В. Интернет и оперативно-розыскная деятельность // Законодательство. 1999. № 11. С. 71—78.

сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ). Кроме того, Интернет служит инструментом для шпионажа (ст. 276 УК РФ) и других преступлений против государственной власти.

Системы передвижной радиосвязи, персонального вызова общего пользования, спутниковой связи, документальной электросвязи давно перестали быть экзотикой в силу их редкости и дороговизны. Сегодня эти средства связи типичны для нашей повседневной жизни и являются общедоступными.

Человеческий фактор в получении оперативно-значимой информации меркнет в сиянии новейших технологий прослушивания. Инициатором здесь выступал альянс западных спецслужб. Технологии, применяемые ранее только в разведывательных целях, сегодня прочно вошли в арсенал правоприменительных и полицейских служб.

Например, в тесном сотрудничестве с секретной американской службой NSA¹⁴ служба Пуллахера в течение ряда лет ведет массовое прослушивание телефонных переговоров «восток — запад». Осуществляется это с помощью гигантских станций контроля передаваемой информации в Везермюндунге, Франкфурте, Аугсбурге, Цвайбрюккене, Дармштадте и других городах¹⁵.

«Ручную работу» принимают на себя компьютеры: по заданию NSA американская компания IBM разработала компьютер для прослушивания «Харвист» («Урожай»), который уже с 1974 года с помощью спутниковой техники «проверяет» около 75 млн ведущихся во всем мире телефонных переговоров и 1,8 млн из них выбирает для анализа специалистами. Робот-«слухач» реагирует на «крамольные» слова и цифровые комбинации (набираемый номер, электронный адрес). Применительно к ФРГ (ежегодно около 217 млн переговоров с границей общей продолжительностью 15,2 млн часов по состоянию на 1979 год) это означает, что для контроля над всеми переговорами с зарубежными странами вполне достаточно было бы установки трех компьютеров «Харвист».

¹⁴ NSA — National Security Agency.

¹⁵ См.: Гесснер Р., Херцог У. За фасадом права: Методы новой тайной полиции. М., 1990. С. 166.

Для контроля всех внутренних переговоров, разумеется, потребовалось бы во много раз больше подобных компьютеров, однако это вполне реально¹⁶.

Если подобные технологии применялись в 1979 году, то, надо думать, в современной ФРГ электронное наблюдение стало стандартной полицейской функцией для борьбы с уголовными преступлениями.

В США электронное наблюдение часто используется при проведении криминальных расследований. В ходе дознания по компьютерным преступлениям сотрудники правоприменительных органов вправе проводить мониторинг за хакером в то время, когда он взламывает компьютерную систему жертвы или вправе установить клонированный (зеркальный) E-mail-ящик для того, чтобы контролировать отправку и получение подозреваемым материалов детской порнографии по Интернету. В более традиционном контексте названные сотрудники могут контролировать телефон подозреваемого или получить трафик его соединений¹⁷.

В США проведение электронного наблюдения в реальном режиме времени регламентируют два федеральных статута. Первый, и самый важный, — это статут по снятию информации с проводной связи¹⁸, впервые принятый как раздел сводного закона «О контроле над преступностью и обеспечении безопасности на улицах 1968 года»¹⁹. Второй статут — это глава из Свода законов США о приборах, регистрирующих исходящую и входящую информацию²⁰.

В названных статутах была предпринята попытка сбалансировать потребности правоприменительных органов в борьбе с преступностью и защиту граждан от необоснованного вторжения государства в их частную жизнь. Кроме того, был введен ряд ограничений, не предусмотренный ранее в решениях Верховного суда

¹⁶ См.: Гесснер Р., Херцог У. За фасадом права... С. 167.

¹⁷ См.: Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations / Criminal Division United States Department of Justice, July 2002 [Electronic resource]. [Http://www.cybercrime.gov](http://www.cybercrime.gov).

¹⁸ См.: Свод законов США. Разд. 18, параграфы 2510—2522.

¹⁹ Названный Закон более известен как «Титул III».

²⁰ См.: Свод Законов США. Разд. 18, параграфы 3121—3127.

США. Прежде всего был четко ограничен круг преступлений (правда, весьма широкий), при расследовании которых могло применяться прослушивание. Законы запретили всякое прослушивание с помощью любых устройств без соответствующего судебного ордера. При этом правила прослушивания различались в отношении устных переговоров (*oral communication*) и переговоров с помощью проводных средств связи (*write communication*). Первые могли прослушиваться на основании ордера лишь в тех местах, которые конституционно охраняются от государственного вторжения (квартира, место работы, номер в отеле и т. д.). Для прослушивания в иных местах, например в тюрьме, ордер не требовался. Во втором случае прослушивание без ордера вообще запрещалось. Нарушение этих правил признавалось фелонией, за совершение которой предусматривалось наказание в виде лишения свободы на срок до 5 лет и/или штраф до 10 тыс. долларов США. Доказательства, добытые с нарушением установленных правил, автоматически исключались из любого судебного разбирательства. Потерпевшим от незаконных действий возмещались все понесенные расходы (например, на адвоката) и убытки²¹.

В Российской Федерации широкое распространение электронное наблюдение получило в начале 90-х годов прошлого века, когда в массовом порядке стали эксплуатироваться современные телефонные станции²².

Начинается постепенная плановая замена морально устаревших автоматических телефонных станций на электронные (цифровые) станции нового поколения, в связи с чем в корне изменяются технологии передачи информации. Появляются системы передвижной радиосвязи и персонального радиовызова общего пользования. На российском рынке достойное место занимают сети документальной электросвязи. Оперативно-розыскная деятельность закономерно входит в названные сферы передачи информации.

²¹ См. об этом: Searching and Seizing...

²² Приказ Минсвязи России № 226 от 24 июня 1992 года «Об использовании средств связи для обеспечения оперативно-розыскных мероприятий Министерства безопасности РФ» [Электрон. ресурс]. Режим доступа: http://www.svcons.ru/normdok/Prikaz_Minsviasi_ot24.06.92_No_226.shtml.

Так, п. 4 приказа Минсвязи России «Об использовании средств связи для обеспечения оперативно-розыскных мероприятий Министерства безопасности РФ» гласит:

...Согласовать в месячный срок представленные Министерством безопасности РФ эксплуатационно-технические требования к аппаратным и программным средствам, системам коммутации сетей электросвязи по обеспечению проведения оперативно-розыскных мероприятий.

При постановке научно-исследовательских и опытно-конструкторских работ по созданию новых систем коммутации включить разработанные в соответствии с п. 4.1 требования в технические задания.

При выдаче сертификатов на оборудование, при закупке импортных систем коммутации и при организации их выпуска отечественной промышленностью по лицензиям в контракты включать поставки аппаратных и программных средств, реализующие возможность осуществления оперативно-розыскных мероприятий.

На подзаконном уровне появляется новое понятие в оперативно-розыскной деятельности — система технических средств по обеспечению оперативно-розыскных мероприятий. Однако до сих пор названная система не получила своего закрепления ни на уровне федерального закона, ни в Федеральном законе «Об оперативно-розыскной деятельности», ни в новой редакции Федерального закона «О связи». Сформулируем определение этого понятия.

Под системой технических средств по обеспечению оперативно-розыскных мероприятий следует понимать комплекс организационных и технических мероприятий, включающий в себя установку различных системных блоков и специальных технических средств непосредственно в современных средствах связи (независимо от их специфики и ведомственной принадлежности) и позволяющий на программном уровне получить всю необходимую информацию о том или ином абоненте.

Объем информации может колебаться от идентификации абонента по его электронному адресу до записи и документирования всей переданной пользователем информации.

В настоящее время система технических средств по обеспечению оперативно-розыскных мероприятий разделилась на пять больших и относительно самостоятельных направлений:

1. Система технических средств по обеспечению оперативно-розыскных мероприятий на электронных автоматических телефонных станциях (независимо от фирмы производителя и ведомственной принадлежности телефонной станции).

2. Система технических средств по обеспечению оперативно-розыскных мероприятий на сетях подвижной радиотелефонной связи, включающая в себя операторов сотовых, транкинговых, радиотелефонных компаний.

3. Система технических средств по обеспечению оперативно-розыскных мероприятий на сетях персонального радиовызова общего пользования.

4. Система технических средств по обеспечению оперативно-розыскных мероприятий на сетях документальной электросвязи²³.

5. Система технических средств по обеспечению оперативно-розыскных мероприятий на сетях спутниковой (космической) связи.

Сегодня создано правовое поле для развития еще одного направления — и н ф о р м а ц и о н н о г о.

С 1 января 2006 года вступили в силу Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, которые были утверждены постановлением Правительства РФ от 27 августа 2005 года № 538²⁴. Правила определяют порядок взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими в соответствии с Федеральным законом «Об оперативно-розыскной деятельности» № 144-ФЗ указанную деятельность с использованием технических средств в сетях операторов связи, при предоставлении операторами связи уполномоченным органам информации об абонентах и оказании им услуг, а также иной информации, необходимой для выполнения возложенных на уполномоченные органы задач в порядке и случаях, установленных иными федеральными законами²⁵.

Согласно Правилам, операторы связи обязаны создать или привести в соответствие с этими Правилами базы данных, содержащих информацию об абонентах оператора связи: фамилия, имя,

²³ Включает в себя услуги по передаче данных.

²⁴ См.: Рос. газ. 2005. 2 сент.

²⁵ См.: Там же. 1995. 18 авг.

отчество, место жительства и реквизиты основного документа, удостоверяющего личность, предъявленные лично владельцем (для абонента, являющегося физическим лицом); для юридического лица — его местонахождение, а также список лиц, использующих оконечное оборудование юридического лица, заверенный уполномоченным представителем юридического лица, в котором указаны их фамилия, имя, отчество, место жительства и реквизиты основного документа, удостоверяющего личность.

Понятие «электронное наблюдение» по своему содержанию является намного шире, чем понятие системы технических средств по обеспечению оперативно-розыскных мероприятий или отдельно взятые виды оперативно-розыскных мероприятий (прослушивание телефонных переговоров и снятия информации с технических каналов связи — ч. 1 ст. 6 Федерального закона «Об оперативно-розыскной деятельности»), контроля и записи переговоров (ст. 186 УПК РФ) как следственного действия. Понятие «электронное наблюдение» объединяет, консолидирует, учитывает все нюансы и особенности этих мероприятий на основе единой категории — информации.

На сегодня сложилась парадоксальная ситуация. В УПК РФ говорится только о контроле и записи переговоров. Что под этим подразумевается? Это телефонные и иные переговоры подозреваемого, обвиняемого и других лиц, содержащие сведения, имеющие значения для уголовного дела (ч. 1 ст. 186 УПК РФ), а также прослушивание и запись переговоров путем использования любых средств коммуникации, осмотр и прослушивание фонограмм (п. 14.1 ст. 5 УПК РФ). А как же быть с информацией, передаваемой в электронном виде, ведь сообщения, передаваемые по электронной почте, техническим каналам связи, не являются аналоговыми сигналами, как мы к этому привыкли? Осуществить запись рассматриваемых сообщений следователю, может быть, и удастся, но вот понять их смысл без определенных технических преобразований — нет. Кроме того, упомянутые сообщения по большому счету не являются переговорами, а следовательно, при формальном подходе к рассматриваемому следственному действию не могут быть отнесены. Излишне говорить, что это существенно сужает рамки данного следственного действия.

В Федеральном законе «Об оперативно-розыскной деятельности» присутствует два вида оперативно-розыскных мероприятий: 1) прослушивание телефонных переговоров и 2) снятие информации с технических каналов связи — и, как уже говорилось, не упоминается о системе технических средств по обеспечению этих мероприятий. Вышеназванные оперативно-розыскные мероприятия не охватывают всех тех возможностей, которые имеются в названной системе. Конечно, можно расширенно трактовать эти два вида оперативно-розыскных мероприятий, включая сюда и функции системы технических средств по обеспечению этих мероприятий. Но столь вольная трактовка оперативно-розыскных мероприятий, существенно ограничивающих конституционные права граждан на неприкосновенность частной жизни и тайну телефонных переговоров, которые допустимы только на основании судебного решения, на наш взгляд, неправильна. Таким образом, система технических средств по обеспечению оперативно-розыскных мероприятий, как бы «выпадает» из перечня оперативно-розыскных мероприятий, закрепленных в Федеральном законе «Об оперативно-розыскной деятельности». Поэтому можно утверждать, что проведение оперативно-розыскной деятельности на современных средствах связи урегулировано только на подзаконном уровне.

Как выйти из данной ситуации? На наш взгляд, было бы логичным учесть все имеющиеся особенности, присущие уже рассмотренным оперативно-розыскным мероприятиям, с учетом специфики систем технических средств по обеспечению оперативно-розыскных мероприятий и специфики следственного действия, в понятии «электронное наблюдение». Итак, что мы понимаем под электронным наблюдением?

Электронное наблюдение — это совокупность последовательно осуществляемых действий, выполняемых уполномоченным государственным органом в пределах своей компетенции на проведение следственных действий и/или оперативно-розыскной деятельности и на основании судебного решения, по снятию информации, передаваемой в форме любого излучения, передаче или приему знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам.

Введение подобного понятия в УПК РФ существенно расширило бы возможности следователя или органа дознания на получение информации, имеющей значение для уголовного дела как на первоначальной, так и на последующих стадиях расследования.

В Федеральном законе «Об оперативно-розыскной деятельности» данное определение реально отражало бы ту совокупность оперативно-розыскных мероприятий, которые охватываются в первую очередь системой технических средств по обеспечению оперативно-розыскных мероприятий, а также прослушиванием телефонных переговоров и снятием информации с технических каналов связи, а кроме того, создало бы правовую базу упомянутой системы на уровне федерального закона, исключив ведомственное нормотворчество.

А главное, это способствовало бы дальнейшему укреплению законности и обоснованности при ограничении конституционных прав граждан на неприкосновенность их частной жизни и тайну телефонных переговоров и иных сообщений.

Электронное наблюдение используется в самых различных областях²⁶ :

- в сфере уголовного судопроизводства — это новое следственное действие, осуществляемое органами предварительного расследования после возбуждения уголовного дела, по которому производство предварительного следствия обязательно, в целях обнаружения и фиксации следов преступления, а также формирования доказательств, имеющих значение для уголовного дела;

- в области оперативно-розыскной деятельности — новое оперативно-розыскное мероприятие, проводимое субъектами оперативно-розыскной деятельности в пределах своей компетенции, для подготовки и осуществления процессуальных действий, выявления, предупреждения, пресечения и раскрытия преступлений, выявления и установления лиц, их подготавливающих, совершающих или совершивших, а также для розыска лиц, скрывшихся от органов дознания, следствия и суда, уклоняющихся от исполнения наказания и без вести пропавших;

²⁶ На наш взгляд, использование одного понятия для различных областей применения не должно вызывать недоумения, т. к. цели, задачи, субъекты, условия и т. п. при его проведении различны.

- в повседневной жизни — использование заинтересованными лицами общедоступных технических средств для обеспечения собственной безопасности или безопасности окружающих от преступных посягательств третьих лиц.

Нами уже неоднократно подчеркивалось, что рассматриваемые оперативно-розыскные мероприятия и следственное действие, контроль и запись переговоров существенно ограничивают конституционные права граждан. В связи с чем хотелось бы кратко остановиться на имеющейся нормативной базе, регулирующей общественные отношения в области электронного наблюдения.

§ 2. Нормативно-правовая основа электронного наблюдения

Формирующееся оперативно-розыскное законодательство есть комплексная отрасль российского права, выделяемая пока только теоретически²⁷. Совокупность нормативно-правовых актов, регулирующих общественные отношения между лицом и государством в процессе защиты человека, общества и государства от преступных посягательств в ходе проведения электронного наблюдения, — часть правового института оперативно-розыскных мероприятий. Кроме того, электронное наблюдение регулируется международными нормами права и нормами права из смежных отраслей российского законодательства.

Можно выделить следующие группы источников современного правового регулирования электронного наблюдения, систематизировав их в зависимости от юридической силы и значимости.

- К первой группе относится Конституция РФ и федеральные конституционные законы. Это базовые источники правового регулирования электронного наблюдения.

²⁷ См., например: Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» / Д. В. Ривман. СПб., 2003. С. 28; Комментарий оперативно-розыскного законодательства РФ и зарубежных стран: Учеб. пособие / М. П. Смирнов. М., 2003. С. 78; Комментарий к Федеральному закону «Об оперативно-розыскной деятельности»: С постановленным приложением нормативных актов и документов / А. Ю. Шумилов. М., 2003. С. 30; и др.

В главе второй Конституции РФ (ст. 17—64) определяются основные права и свободы человека и гражданина, составляющие основу правового статуса личности. Так, согласно ст. 23 (ч. 2) каждый имеет право на тайну переписки²⁸, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения. А в соответствии со ст. 55 (ч. 3) права и свободы человека и гражданина могут быть ограничены федеральным законом только в той мере, в какой это необходимо в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Необходимо отметить Федеральный конституционный закон от 23 июня 1999 года № 1-ФКЗ «О военных судах РФ»²⁹. В нем установлено, что военные суды в пределах своих полномочий и порядке, установленном федеральным законом, рассматривают дела и материалы, связанные с ограничением конституционных свобод и прав на тайну переписки, телефонных и иных переговоров, почтовых, телеграфных и иных сообщений.

• Вторую группу правовой основы электронного наблюдения, его «костяк» составляют нормы УПК РФ (ст. 13, 89, 186), Федеральный закон от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности», Федеральный закон от 22 апреля 1995 года № 40-ФЗ «Об органах Федеральной службы безопасности РФ» (ст. 15)³⁰, Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи» (ст. 53, 64, 65).

• В третью группу нормативно-правовых актов можно отнести другие федеральные законы, такие как УК РФ³¹, Законы от 5 марта 1992 года № 2446-1 «О безопасности»³², от 21 июля 1993 года № 5485-1 «О государственной тайне»³³; от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информа-

ции»³⁴; законодательные акты, закрепляющие компетенцию государственных органов на проведение электронного наблюдения³⁵.

• К четвертой группе можно отнести подзаконные нормативные акты, принятые федеральными органами государственной власти. В качестве примера можно привести Указ Президента РФ от 1 сентября 1995 года № 891 «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств»³⁶, «Перечень сведений, составляющих государственную тайну»³⁷, утвержденный Указом Президента РФ от 30 ноября 1995 года № 1203, Указ Президента РФ от 18 апреля 1996 года № 567 «О координации деятельности правоохранительных органов по борьбе с преступностью»³⁸, Постановление Совета Федерации Федерального собрания РФ от 4 сентября 1998 года № 392-СФ «Об информации и. о. министра внутренних дел РФ и директора ФСБ России о криминогенной обстановке в РФ, принимаемых мерах по укреплению законности, пресечению фактов коррупции и проникновения криминальных элементов в органы государственной власти»³⁹, Постановление Правительства РФ от 15 сентября 1999 года № 1040 «О мерах по противодействию терроризму»⁴⁰.

• Пятую группу составляют нормативно-правовые акты различных министерств и ведомств, осуществляющих электронное наблюдение, а также акты межведомственного значения. Большую их часть составляют сведения об организации и тактике проведения

³⁴ Собр. законодательства РФ. 1995. № 8. Ст. 609. (Актуальна в первую очередь ст. 11 «Информация о гражданах (персональные данные)».)

³⁵ Закон РСФСР от 18 апреля 1991 г. № 1026-1 «О милиции» // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1991. № 16. Ст. 503; Закон РФ от 21 июля 1993 г. № 5473-1 «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1993. № 33. Ст. 1316; Федеральный закон от 27 мая 1996 г. № 57-ФЗ «О государственной охране» // Собр. законодательства РФ. 1996. № 22. Ст. 2594; и др.

³⁶ Собр. законодательства РФ. 1999. № 24. Ст. 2954.

³⁷ Там же. 1995. № 49. Ст. 4775.

³⁸ Там же. 1996. № 17. Ст. 1958.

³⁹ Там же. 1998. № 37. Ст. 4553.

⁴⁰ Там же. 1999. № 38. Ст. 4550.

²⁸ Надо полагать, включая и электронную почту.

²⁹ Собр. законодательства РФ. 1999. № 26. Ст. 3170.

³⁰ Рос. газ. 1995. 12 апр.

³¹ Собр. законодательства РФ. 1996. № 25. Ст. 4921.

³² Ведомости Верховного Совета РФ. 1992. № 15. Ст. 769.

³³ Рос. газ. 1993. 21 сент.; Собр. законодательства РФ. 1997. № 41. Ст. 4673.

электронного наблюдения, что, как известно, является информацией с ограниченным видом доступа, в связи с чем в данной работе они анализироваться не будут⁴¹.

• Шестую группу источников правового регулирования общественных отношений в сфере электронного наблюдения составляют нормативно-правовые акты и документы, хотя и не входящие непосредственно в правовую основу электронного наблюдения, но имеющие большое значение для его правового регулирования. Рассматриваемая группа является самой объемной по своему содержанию.

В нее входят законодательные акты, не содержащие предписаний, непосредственно направленных на регулирование электронного наблюдения, однако в силу универсального характера изложенных в них норм в обязательном порядке учитывающиеся при проведении электронного наблюдения⁴².

К ней можно отнести подзаконные акты федеральных органов государственной власти, которые, хотя и не являются оперативно-розыскными органами, тем не менее вправе принимать правовые акты, регулирующие отдельные общественные отношения в сфере электронного наблюдения⁴³.

⁴¹ В качестве примера нормативно-правового акта с открытым видом доступа к содержащейся в нем информации можно назвать инструкцию «О порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю, прокурору или в суд» (Утв. приказом Федеральной службы налоговой полиции России, Федеральной службы безопасности России, Министерства внутренних дел России, Федеральной службы охраны России, Федеральной пограничной стражи России, Государственного таможенного комитета России, Службы внешней разведки России от 13 мая 1998 г. № 175/226/336/201/410/56) // Бюл. норматив. актов федерал. органов исполнит. власти. 1998. № 23.

⁴² Федеральный закон РФ от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Рос. газ. 2001. 9 авг.

⁴³ См.: Приказ Министерства финансов РФ от 30 ноября 2001 года № 103-н «Об утверждении Положения о порядке финансирования за счет средств федерального бюджета оперативно-розыскных мероприятий» // Рос. газ. 2002. 12 янв.; Приказ Государственного комитета по связи и информатике РФ от 20 апреля 1999 года № 70 «О технических требованиях к системе технических средств, для обеспечения функции оперативно-розыскных мероприятий на сетях электросвязи РФ». Прил.: 1. Технические требования к системе по обеспечению функции оперативно-розыскных мероприятий на сетях подвижной радиотелефонной связи; 2. Технические требования к системе технических средств по обеспечению функции оперативно-ро-

А кроме того, суды также принимают специальные решения, которые предназначены разъяснять предписания законодательных и иных нормативных актов в области электронного наблюдения⁴⁴.

зыскных мероприятий на сетях персонального радиовызова общего пользования; 3. Технические требования к каналам обмена информацией между системой технических средств по обеспечению оперативно-розыскных мероприятий и пультом управления для сетей подвижной радиотелефонной связи; 4. Технические требования к системе технических средств по обеспечению функции оперативно-розыскных мероприятий на электронных телефонных станциях; 5. Технические требования к каналам обмена информацией между системой технических средств по обеспечению оперативно-розыскных мероприятий и пультом управления на электронных телефонных станциях // Связьинформ. 1999. № 6; Письмо первого заместителя Министерства связи РФ руководителям организаций и операторам связи № 2259 от 30 апреля 1996 года «О взаимодействии с органами, осуществляющими оперативно-розыскную деятельность»; Решение Государственной комиссии по электросвязи при Государственном комитете РФ по телекоммуникациям от 29 сентября 1999 года № 63 (официально опубликовано не было); Приказ Министерства РФ по связи и информатизации от 25 июля 2000 года № 130 «О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования» // Рос. газ. 2000. 29 авг.; Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность (утв. постановлением Правительства РФ от 27.08.2005 г. № 538) // Рос. газ. 2005. 2 сент.

⁴⁴ См.: Определение Конституционного суда РФ от 2 октября 2003 года № 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”» // Рос. газ. 2003. 10 дек.; Определение Конституционного суда РФ от 21 декабря 2000 года № 290-О «Об отказе в принятии к рассмотрению жалобы гражданина Идалова Тимура Саид-Магомедовича на нарушение его конституционных прав рядом статей УПК РСФСР и частью 2 статьи 8 Федерального закона “Об оперативно-розыскной деятельности”» // Собр. законодательства РФ. 2001. № 11. Ст. 1069; Определение Конституционного суда РФ от 4 февраля 1999 года № 18-О «По жалобе граждан М. Б. Никольской и М. И. Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона “Об оперативно-розыскной деятельности”» // Вестн. Конституционного суда РФ. 1999. № 3. С. 23-25; Определение Конституционного суда РФ от 14 июля 1998 года «По делу о проверке конституционности отдельных положений Федерального закона “Об оперативно-розыскной деятельности” по жалобе гражданки И. Г. Черновой» // Собр. законодательства РФ. 1998. № 34. Ст. 4368. В качестве примера актов Верховного суда РФ можно назвать: Постановление Пленума Верховного суда РФ № 13 от 24.12.1993 г. «О некоторых вопросах, связанных с применением статей 23 и 25 Конституции РФ» // Бюл. Верховного суда РФ. 1994. № 3. С. 51—53; Решение Верховного суда РФ от 25.09.2000 № ГКПИ 00-1064 // Бюл. Верховного суда РФ. 2001. № 4. С. 84.

Считаем целесообразным упомянуть также о некоторых актах международного-правового характера. Основанием отнесения такого рода документов к этим источникам служат предписания Конституции РФ, в соответствии с которой общепризнанные нормы международного права и международные договоры Российской Федерации являются частью ее правовой системы. В соответствии с ч. 4 ст. 15 Конституции РФ, если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора. Ими являются международные договоры и соглашения, а также акты, заключенные правоприменительными органами России с аналогичными органами других государств⁴⁵. Применяя на практике указанные правовые источники, следует иметь в виду, что положения официально опубликованных международных договоров Российской Федерации, не требующие издания внутригосударственных актов для применения, действуют на территории России непосредственно. В ином случае наряду с международным договором Российской Федерации необходимо применять соответствующий национальный нормативно-правовой акт, принятый для реализации положений конкретного международного договора (ч. 3 ст. 5 Федерального закона «О международных договорах РФ»)⁴⁶.

Анализируемый круг источников правового регулирования электронного наблюдения лишней раз подтверждает, что рассматриваемый институт оперативно-розыскного законодательства является комплексным. Это связано с тем, что полнота правового регулирования общественных отношений в сфере применения элект-

⁴⁵ См., например: Европейская конвенция о защите прав человека и основных свобод (принята Советом Европы 04.11.1950 г., вступила в силу 03.09.1953 г.); Конвенция об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности от 8 ноября 1990 года (Страсбург) (ратифицирована РФ 28.05.2001 г. с оговорками); Федеральный закон от 28 мая 2001 года № 62-ФЗ «О ратификации Конвенции об отмывании, выявлении, изъятии и конфискации доходов от преступной деятельности» // Рос. газ. 2001. 31 мая; Европейская конвенция о взаимной помощи по уголовным делам от 20 апреля 1959 года; Соглашение о взаимодействии министерств независимых государств в сфере борьбы с преступностью (заключено на совещании министров внутренних дел независимых государств в Алма-Ате 23—24 апреля 1992 года); и др.

⁴⁶ Собр. законодательства. 1995. № 29. Ст. 2757.

ронного наблюдения может быть достигнута только в том случае, если совокупность норм права актов оперативно-розыскного законодательства «перекроет» все множество оперативно-розыскных правоотношений применительно ко всем возможным объектам оперативно-розыскных правоотношений и субъектам, действующим в сфере применения электронного наблюдения. Целью проведения электронного наблюдения является получение информации, а поскольку она проникает во все области и направления деятельности человека, государства и общества, то и оперативно-розыскные правоотношения в сфере применения электронного наблюдения как бы пронизывают все законодательство России на федеральном уровне как по вертикали (виды нормативно-правовых актов), так и по горизонтали (отрасли российского законодательства).

Вертикальная структура оперативно-розыскных правоотношений в сфере применения электронного наблюдения, как и всего законодательства России, строится исходя из принципа верховенства закона.

Горизонтальная структура рассматриваемых правоотношений выстраивается исходя из того, что они включают в свой состав не только нормы, входящие в блок специальных нормативных актов по видам электронного наблюдения, но и нормы других отраслей законодательства России. И здесь в первую очередь необходимо назвать конституционное и административное законодательство.

Опираясь на нормативно-правовую основу электронного наблюдения, рассмотрим отдельные его виды.

§ 3. Виды электронного наблюдения

В сфере уголовного судопроизводства и оперативно-розыскной деятельности, учитывая специфику современных телекоммуникационных систем по передаче, потреблению, обработке, хранению информации в единой сети электросвязи Российской Федерации, можно выделить следующие виды электронного наблюдения, исходя из категорий сетей электросвязи РФ и способов передачи сигнала.

- Электронное наблюдение на сети связи общего пользования. Сеть связи общего пользования предназначена для возмезд-

ного оказания услуг электросвязи любому пользователю услугами связи на территории Российской Федерации и включает в себя сети электросвязи, определяемые географически в пределах обслуживаемой территории и ресурса нумерации и не определяемые географически в пределах территории Российской Федерации и ресурса нумерации, а также сети связи, определяемые по технологии реализации оказания услуг связи. Сеть связи общего пользования представляет собой комплекс взаимодействующих сетей электросвязи, в том числе сети связи для распространения программ телевизионного вещания и радиовещания, и имеет присоединение к сетям связи общего пользования иностранных государств (ст. 13 Федерального закона «О связи»).

• Электронное наблюдение на выделенных сетях связи. Выделенными сетями связи являются сети электросвязи, предназначенные для возмездного оказания услуг электросвязи ограниченному кругу пользователей или группам таких пользователей. Выделенные сети связи могут взаимодействовать между собой. Выделенные сети связи не имеют присоединения к сети связи общего пользования, а также к сетям связи общего пользования иностранных государств. Технологии и средства связи, применяемые для организации выделенных сетей связи, а также принципы их построения устанавливаются собственниками или иными владельцами этих сетей. Выделенная сеть связи может быть присоединена к сети связи общего пользования с переводом в категорию сети связи общего пользования, если выделенная сеть связи соответствует требованиям, установленным для сети связи общего пользования. При этом выделенный ресурс нумерации изымается и предоставляется ресурс нумерации из сети связи общего пользования. Оказание услуг связи операторами выделенных сетей связи осуществляется на основании соответствующих лицензий в пределах указанных в них территорий и с использованием нумерации, присвоенной каждой выделенной сети связи в порядке, установленном федеральным органом исполнительной власти в области связи (ст. 14 Федерального закона «О связи»).

• Электронное наблюдение на технологических сетях связи, присоединенных к сети связи общего пользования. Техно-

логические сети связи предназначены для обеспечения производственной деятельности организаций, управления технологическими процессами в производстве. Технологии и средства связи, применяемые для создания технологических сетей связи, а также принципы их построения устанавливаются собственниками или иными владельцами этих сетей. При наличии свободных ресурсов технологической сети связи часть этой сети может быть присоединена к сети связи общего пользования с переводом в категорию сети связи общего пользования для возмездного оказания услуг связи любому пользователю на основании соответствующей лицензии. Такое присоединение допустимо при следующих условиях:

— часть технологической сети связи, предназначенная для присоединения к сети связи общего пользования, может быть или технически, или программно, или физически отделена собственником от технологической сети связи;

— присоединяемая к сети связи общего пользования часть технологической сети связи соответствует требованиям функционирования сети связи общего пользования.

Технологической сети связи (ее части), присоединенной к сети связи общего пользования, выделяется ресурс нумерации из ресурса нумерации сети связи общего пользования в порядке, установленном федеральным органом исполнительной власти в области связи (ст. 15 Федерального закона «О связи»).

• Федеральный закон «О связи» в единой сети электросвязи России выделяет также сети связи специального назначения, но электронное наблюдение на данных сетях, как правило, не проводится⁴⁷.

В зависимости от способа передачи сигнала и используемых при этом средств связи (могут использоваться на любой из категорий сетей электросвязи) выделяются следующие виды электронного наблюдения.

⁴⁷ Сети связи специального назначения предназначены для нужд государственного управления, обороны страны, безопасности государства и обеспечения правопорядка. Эти сети не могут использоваться для возмездного оказания услуг связи, если иное не предусмотрено законодательством Российской Федерации (ст. 16 Федерального закона «О связи»).

- Электронное наблюдение на электронных (цифровых) автоматических телефонных станциях⁴⁸.
- Электронное наблюдение на сетях подвижной радиотелефонной связи⁴⁹.
- Электронное наблюдение в транкинговых системах подвижной радиотелефонной связи⁵⁰.
- Электронное наблюдение на сетях персонального радиовызова общего пользования⁵¹.
- Электронное наблюдение на сетях документальной электро-связи⁵².
- Электронное наблюдение на системе глобальной подвижной персональной спутниковой связи⁵³.

⁴⁸ Проводится на всех отечественных и импортных электронных автоматических телефонных станциях, устанавливаемых на территории России и входящих в состав единой сети электросвязи Российской Федерации («проводная» электросвязь). Включают в себя сельские, городские, управленческие, междугородные, международные и комбинированные электронные автоматические телефонные станции независимо от формы собственности и ведомственной принадлежности. Предназначено для получения информации в различных режимах времени как следственными органами (а в случае необходимости и судом), так и правоприменительными органами на основании действующего законодательства.

⁴⁹ Проводится на всех отечественных и импортных коммутаторах сотовой связи действующих федеральных стандартов (NMT-450i, AMPS, DAMPS, GSM 900/1800 МГц, CDMA). Позволяет получать информацию о всех видах дополнительных услуг, оказываемых тем или иным оператором сотовой связи. Например, службы коротких сообщений (SMS) или мультимедийных сообщений (MMS).

⁵⁰ Позволяет осуществлять контроль абонентских соединений и местоположение пользователей транкинговой подвижной радиосвязи в соответствии с действующим законодательством (название данного вида связи происходит от английского слова *trunk* — дерево). Проводится на всех отечественных и импортных коммутаторах рассматриваемого вида связи стандарта SmartTrunk, MPT-1327, SmartNet, LTR, ESAS, EDACS, TETRA и др.

⁵¹ Пейджинговая связь (от англ. *page* — страница). Позволяет осуществлять мониторинг сообщений абонентов передаваемых операторами связи в стандарте FLEX, POGSAC и др.

⁵² Сети документальной электросвязи включают себя такие трансграничные информационно-телекоммуникационные сети, как Интернет (*World Wide Web* — Всемирная информационная паутина), электронная почта, факсимильная связь, системы передачи данных различной направленности, IP-телефония (весь комплекс информации в электронном виде, передаваемой по единой сети электросвязи России).

⁵³ Позволяет осуществлять контроль информации, передаваемой по каналам спутниковой связи.

Сегодня можно акцентировать внимание на электронном наблюдении в следующих информационных системах накопления сведений об абонентах различных видов операторов и средств связи:

- информационные системы персональных данных абонентов операторов связи⁵⁴;
- технологические информационные системы операторов связи⁵⁵;
- биллинговые информационные системы операторов связи⁵⁶.

В качестве отдельного вида электронного наблюдения необходимо выделить видеозапись с использованием мультимедиа технологий. Во всех больших городах постепенно увеличивается число видеокамер, объективы которых направлены не только на транспортные узлы, но и на пешеходные зоны, магазины, офисы, автостоянки, жилые помещения и т. д.⁵⁷ Цели рассматриваемого вида наблюдения могут быть самыми различными — от обеспечения собственной безопасности до выявления и пресечения угроз национальной безопасности.

Идея электронного наблюдения с использованием видеозаписи не нова и применяется практически во всех технически развитых странах. Так, в Ганновере, Гамбурге (ФРГ) в начале восьмидесятих годов прошлого столетия полиция осуществляла контроль главных улиц и площадей 25 камерами наружного наблюдения, через два года их количество возросло до 42. Все они передавали изображения на мониторы Центра регулирования дорожного движения, размещенного на первом этаже высотного здания полиции. Каме-

⁵⁴ Базы данных, банки данных, архивы, содержащие информацию об абонентах оператора связи.

⁵⁵ Базы данных, банки данных, архивы, содержащие технологическую информацию, поступающую с коммутаторов или узлов различных видов связи, включающую в себя .CDR- или .LOG-файлы для идентификации абонентских устройств (IMEI сотового телефона), Sim-карт (IMSI — международный идентификатор Sim-карты) или IP-адресов пользователей.

⁵⁶ Базы данных, банки данных, архивы, содержащие информацию о стоимости входящих и исходящих соединениях абонентов.

⁵⁷ На одной только Трафальгарской площади вокруг колонны Нельсона установлено более 40 видеокамер наружного наблюдения. Как правило, управление видеонаблюдением является удаленным. Технологии позволяют пользователю контролировать события через Интернет с помощью Web-браузера с любого компьютера и из любой точки мира.

ры могли вращаться и были снабжены светосильной оптикой, позволяющей делать портретные снимки с расстояния 30—40 метров. По первоначальному замыслу эти камеры разрабатывались для контроля над дорожным движением. Однако уже вскоре они превратились в немых агентов-наблюдателей: в нужные моменты они «прошупывают» каждого прохожего (одежда, походка, долгое стояние у витрин и т. д.) и при целенаправленном розыске могут быстро «обшарить» в поисках объекта важнейшие участки города. Во время демонстраций или манифестаций они дают информацию о числе участников, ходе мероприятия, об участвующих группах, а также отдельных лицах. Передаваемые изображения можно было хранить, увеличивать отдельные детали и останавливать показ в нужный момент⁵⁸.

Прозрачность делает мир безопаснее. Когда в одном из районов Лондона в 1996 году было установлено 300 видеокамер наблюдения, преступность снизилась на 30 %. Там же, в Великобритании, благодаря системе видеонаблюдения было раскрыто «самое ужасное преступление 1993 года» — убийство двухлетнего мальчика⁵⁹.

В 1979 году, когда в Висбадене полицейские власти создали специальную оптико-техническую исследовательскую и испытательную лабораторию, никто и не подозревал, какие возможности может принести полиции целенаправленное развитие этих современных средств государственного контроля⁶⁰.

В настоящее время на территории Российской Федерации электронное наблюдение с использованием видеосредств стало реальностью и находит широкое применение не только в оперативно-розыскной деятельности, но и в повседневной жизни. В качестве примера можно назвать программу «Мой двор, мой подъезд» на территории г. Москвы⁶¹. Одним из приоритетных направлений названной программы называется оборудование подъездов жилых домов системами видеонаблюдения.

⁵⁸ См.: Гесснер Р., Херцог У. За фасадом права... С. 159—161.

⁵⁹ См.: Губанов Андрей. Куда пойти целоваться? // Наша газета. 2004. № 6 (429).

⁶⁰ См.: Гесснер Р., Херцог У. За фасадом права... С. 159—161.

⁶¹ См.: Постановление правительства Москвы от 28 января 2003 года № 51-ПП «Об итогах реализации программы “Мой двор, мой подъезд” в 2002 году и задачах на 2003 год» [Электрон. ресурс]. Режим доступа: <http://www.uvao.ru/news>.

Так, в плановом задании на 2003 год по установке названных систем предусматривалось произвести монтаж и сдать в эксплуатацию по Юго-Восточному административному округу г. Москвы 1900 видеокамер⁶².

Из вышеизложенного очевидно, что возможности электронного наблюдения для получения информации достаточно обширны. Полученные результаты могут быть использованы в соответствии с действующим законодательством как в уголовном судопроизводстве, так и в сфере оперативно-розыскной деятельности⁶³.

Каковы особенности получения и использования рассматриваемой информации в названных областях? Что общего и в чем заключается принципиальное различие между ними? Каковы пределы использования электронного наблюдения? На эти и другие малоисследованные вопросы постараемся ответить в ходе дальнейшего изложения материала.

⁶² См.: Распоряжение префекта Юго-Восточного административного округа от 28 февраля 2003 года № 364 «Об итогах реализации программы “Мой двор, мой подъезд” на территории Юго-Восточного административного округа в 2002 году и задачах на 2003 год» [Электрон. ресурс]. Режим доступа: <http://www.uvao.ru/news>.

⁶³ Фондом «Социум» был проведен опрос жителей г. Екатеринбурга на предмет их отношения к камерам видеонаблюдения в магазинах и других общественных местах. Всего было опрошено 246 человек. Из них 63 % высказались за необходимость их установки, т. к. считают, что камеры обеспечивают нашу безопасность; 16 % остались равнодушными к их существованию; 8 % считают, что они нужны, но вызывают раздражение; 4 % считают, что охранник или милиционер надежнее камеры, и только 3 % посчитали, что камеры не столько помогают в обеспечении безопасности, сколько влезают в частную жизнь (см. на сайте: www.socium.ur.ru).

ГЛАВА 2

ЭЛЕКТРОННОЕ НАБЛЮДЕНИЕ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

§ 1. Информация и электронное наблюдение

Как уже подчеркивалось, понятие «электронное наблюдение» по своему содержанию является намного шире таких понятий, как система технических средств по обеспечению оперативно-розыскных мероприятий или отдельно взятые виды оперативно-розыскных мероприятий, контроль и запись переговоров как следственное действие¹. Оно их объединяет, консолидирует, учитывает все их нюансы и особенности на основе единой категории — и н ф о р м а - ц и и. Если проанализировать частоту применения тех или иных понятий в научных исследованиях или даже в обыденной жизни, то, без всякого сомнения, одно из первых мест займет названная категория. Что понимается под информацией вообще, а в уголовном судопроизводстве и оперативно-розыскной деятельности в частности?

Как известно, отражение есть всеобщее свойство материи, заключающееся в воспроизведении признаков, свойств и отношений отражаемого объекта. Способность к отражению, а также характер его проявления зависят от уровня организации материи. Отражение во всем многообразии его форм, начиная от простейших механических следов и кончая человеческим разумом, происходит в процессе взаимодействия различных систем реального мира. Отражение в общем случае представляет собой процесс, результатом которого

¹ В данном случае понимается не сам процесс проведения электронного наблюдения, а его результаты.

является информационное воспроизведение свойств отражаемого предмета. Любое взаимодействие включает информационный процесс, являясь информационным взаимодействием в том смысле, что одно оставляет о себе память в другом. В самом широком, философском, смысле информация есть бытие, отраженное в ином, т. е. инобытие, как сказал бы Гегель. Информация, таким образом, есть объективная сторона процессов природы и, как таковая, является всеобщей, что, разумеется, вовсе не исключает, а напротив, предполагает ее специфику в различных сферах реального мира — неорганической природе, живых системах и социальных процессах.

Термин «информация» (от лат. *informatio* — сообщение, разъяснение, изложение) возник в социальной среде и первоначально применялся для обозначения сведений, передаваемых от одних людей другим устным, письменным или иным способом. В практическом смысле, понятном каждому, определение информации дал С. И. Ожегов: «... информация — это: 1) сведения об окружающем мире и протекающих в нем процессах; 2) сообщения, осведомляющие о положении дел, о состоянии чего-либо»².

В результате развития и усложнения процессов информации основатель современной кибернетики Н. Винер дал следующее определение: «Информация — это обозначения содержания, полученного из внешнего мира в процессе приспособления к нему наших чувств»³.

Д. И. Бедняков утверждает, что информация, полученная субъектом в результате его взаимодействия с объективным миром, есть результат отражения, это сведения, знания об объективной действительности.

Другими словами, информация есть образно-знаковая модель объективного мира. Добавим к этому: не только образно-знаковая, но и образно-понятийная модель, т. к. знак, будучи специфической разновидностью сигнала, используется только в языковом общении между людьми и, в конечном итоге, применяется для классификации образцов и выражения их с помощью понятий, суждений и умозаключений.

² Ожегов С. И. Словарь русского языка. М., 1978. С. 354.

³ Винер Н. Кибернетика, или Управление и связь в животном и машине / Пер. с англ. И. В. Соловьева; Под ред. Г. Н. Поварова. М., 1958. С. 31.

Процесс познания представляет собой отражение объективной действительности в сознании познающего субъекта с помощью органов чувств, ощущений, а информация есть результат отражения, причем отражения только на уровне сознания, и связана с формированием сведений об отраженном объективном мире⁴.

Правовое определение информации вводит Федеральный закон «Об информации, информатизации и защите информации». В соответствии с названным законом, информация — это сведения о лицах, предметах, фактах, событиях, процессах независимо от формы их представления (ст. 2).

На наш взгляд, интересно также определение информации, составляющей тайну телефонных переговоров, данное Конституционным судом РФ: «...информацией... считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи»⁵.

Хотелось бы привести еще одно определение, данное А. С. Овчинским: «...Информация — это то содержание сообщений, те составляющие сведений, те компоненты знаний, те комбинации сигналов, которые, с одной стороны, интерпретированы исходя из возможностей, интересов, преследуемых целей и стоящих задач и, с другой стороны, оказывают воздействие как на сознание, так и на подсознание людей, оставляя следы в их памяти, могут накапливаться и в результате открывают возможность и создают механизмы управления социальными системами и процессами»⁶.

Попытаться дать некое обобщающее определение информации на фоне того, что уже сказано о ней сотнями других исследователей, представляется делом весьма неблагодарным. Можно согласиться с утверждением Н. Н. Моисеева о том, что «...достаточного

⁴ См.: Бедняков Д. И. Непроцессуальная информация и расследование преступлений. М., 1991. С. 25—26.

⁵ Определение Конституционного суда РФ от 2 октября 2003 года № 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”».

⁶ Овчинский А. С. Информация и оперативно-розыскная деятельность. М., 2002. С. 27.

универсального определения просто быть не может, ибо оно неотделимо от свойств субъекта, который нуждается не в информации вообще, а во вполне определенной информации и отбрасывает ненужную ему информацию»⁷.

Все приведенные определения информации, на наш взгляд, справедливы и зависят от особенностей субъекта, участвующего в сфере ее обращения. Применительно к уголовному судопроизводству можно утверждать, что для его участников будут актуальны любые сведения, имеющие значения для уголовного дела. А для субъектов оперативно-розыскной деятельности — любая информация, отвечающая задачам указанной деятельности.

Оставим в стороне и трактовки информации как отражения разнообразия, что, как уже говорилось выше, согласуется с философской теорией отражения и с представлениями об информации как о сведениях или сообщениях, которые всегда что-то отражают — события, явления и т. п.

Обратимся к соотношению таких понятий, как информация и электронное наблюдение.

По мнению М. И. Сетрова, «сообщение для каждой категории людей несет совершенно разную информацию, соответствующую кругу интересов получателя»⁸.

Таким образом, одно и то же сообщение, по-разному интерпретированное, может нести разную информацию. При этом можно утверждать, что «...решающим для связи между сообщением и содержащейся в нем информацией является некоторое отображение, которое является либо результатом договоренности, либо результатом понимания, либо предписанным правилом. Это отображение можно обозначить как правило интерпретации»⁹.

Заметим, что некоторое правило интерпретации для отдельного сообщения чаще всего являются частным случаем более общего правила, применимого к определенному множеству сообщений, если они, в свою очередь, построены по одинаковым законам.

Однако знания только правил интерпретации отнюдь не достаточно для извлечения информации из сообщения. Сама интерпре-

⁷ Моисеев Н. Н. Универсум, информация, общество. М., 2001. С. 50.

⁸ Сетров М. И. Информационные процессы в биологических системах. Л., 1975. С. 33.

⁹ Там же.

тация определяется интересами получателя информации, его чувствами, эмоциями и, говоря более формальным языком, просто его целью. При этом несложно представить, что одним из основных условий извлечения необходимой информации из сообщения является собственно цель этого процесса.

Опираясь на такие понятия, как интерпретация и цель, можно утверждать, что информация — это то содержание сообщений, те составляющие сведения о чем-либо или о ком-либо, те компоненты знаний, которые интерпретированы исходя из преследуемых целей и задач.

Все вышесказанное в полном объеме относится и к электронному наблюдению. Из всего потока сообщений, принятых в ходе проведения электронного наблюдения, учитывая «функцию целевой интерпретации полученного сообщения»¹⁰, выделяется документированная информация, отвечающая задачам уголовного судопроизводства и оперативно-розыскной деятельности.

Под документом законодатель понимает «...материальный объект с зафиксированной на нем информацией в виде текста, звукозаписи или изображения, предназначенный для передачи во времени и пространстве в целях хранения и общественного использования»¹¹. Документировать — обосновывать документами¹². Документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать¹³.

Необходимо различать понятия «документированная информация» и «документальная информация». Так, под документальной информацией следует понимать информацию, основанную на документах, фактах.

¹⁰ Румянцев Д. Г., Монастырский Л. Ф. Путь программиста. М., 2000. С. 23.

¹¹ Федеральный закон от 29 января 1994 года № 77-ФЗ «Об обязательном экземпляре документов» (ст. 1) // Рос. газ. 1995. 17 янв.; Федеральный закон от 29 декабря 1994 года № 78-ФЗ «О библиотечном деле» (ст. 1) // Собр. законодательства РФ. 1995. № 1. Ст. 2.

¹² Ожегов С. И. Словарь русского языка. С. 158.

¹³ См.: Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» (ст. 2) // Собр. законодательства РФ. 1995. № 8. Ст. 609; Федеральный закон от 4 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене» (ст. 2) // Там же. 1996. № 28. Ст. 3347.

Определение документирования как совокупности оперативно-розыскных мер в целях сбора сведений об обстоятельствах преступлений, лицах, их совершивших, в случаях, если эти сведения зафиксированы на соответствующем носителе, дает возможность выявить в документировании и доказывании некоторые элементы сходства. Как в документировании, так и в доказывании используются такие общенаучные познавательные методы, как беседа, осмотр, наблюдение, сравнение, измерение, эксперимент и т. д. Применение последних оперативным работником, следователем, прокурором, судом может быть представлено в виде информационного процесса (информирования), состоящего из набора следственных элементов: сбор (обнаружение, фиксация, изъятие), исследование и оценка информации.

Однако методы сбора информации различны. Порядок, условия и последовательность применения средств и методов сбора доказательственной информации достаточно подробно урегулированы в уголовно-процессуальном законе, а средства и методы, применяемые для сбора материалов документирования, — в Федеральном законе «Об оперативно-розыскной деятельности» и находятся за рамками уголовного процесса.

Это дает основание говорить о документировании только как об одном из уровней удостоверительной деятельности (низшей по сравнению с доказыванием).

Если рассматривать другой аспект уголовно-процессуальной деятельности — логическое доказывание — как мыслительную деятельность по формированию выводного знания на основе достоверных доказанных суждений¹⁴, то и документирование, и доказывание осуществляются по одним и тем же законам формальной логики, и здесь между ними нет сколько-нибудь существенных отличий.

В основу наших дальнейших рассуждений можно было бы положить информационную концепцию понятия доказательства, которая, по мнению Ю. К. Орлова, «...появилась под влиянием кибернетических идей и теорий, в самый разгар “кибер-

¹⁴ См.: Орлов Ю. К. Заключение эксперта как источник выводного знания в судебном доказывании: Автореф. дис. ... канд. юрид. наук. М., 1985. С. 14; Бедняков Д. И. Непроцессуальная информация... С. 99—101.

нетического бума” и явилась мощным толчком для интенсивной разработки информационного аспекта доказывания, максимального использования достижений кибернетики в теории доказательств»¹⁵.

Центральная идея концепции — утверждение о том, что доказательство есть единство информации и ее материального носителя. Иначе говоря, в понятие доказательств включаются не сами факты, а информация о них в совокупности с источниками. В основу понятия положена материя, которая может быть выявлена, обнаружена, собрана, проверена и оценена. Концепция, таким образом, отвечает требованию, согласно которому какое доказательство не имеет заранее установленной силы и должно оцениваться по внутреннему убеждению соответствующего должностного лица или органа. Концепция получила признание, а используемое в ней понятие доказательства стало широко распространенным¹⁶.

Однако, по нашему мнению, более правильно рассматривать доказательство как информационную систему, включающую в себя фактические сведения (информацию, данные), источники, в которых они содержатся, а также способы и порядок собирания, закрепления и проверки фактических сведений и их источников¹⁷.

§ 2. Электронное наблюдение как комплексное оперативно-розыскное мероприятие

В формирующейся общей для всех субъектов оперативно-розыскной деятельности теории, а также в законотворчестве не выработано единого подхода по вопросу об оперативно-розыск-

¹⁵ Орлов Ю. К. Основы теории доказательств в уголовном процессе. М., 2000. С. 37.

¹⁶ См., например: Советский уголовный процесс: Учеб. / Под ред. Л. М. Карнеевой, П. А. Лупинской, И. В. Тыричева. М., 1980. С. 138—141; Власова Н. А. Уголовный процесс: Курс лекций. М., 2001. С. 40.

¹⁷ Более подробно об этом см.: Балакишин В. С. Доказательства в российском уголовном процессе: понятие, сущность, классификация. Екатеринбург, 2002.

ном мероприятии. Так, например, в ст. 6 Федерального закона «Об оперативно-розыскной деятельности» речь идет в основном об оперативно-розыскных мероприятиях, хотя законодатель недостаточно последователен. В статьях 5 (ч. 2) и 16 (ч. 2) названного закона приведен термин «действие». УПК РФ упоминает как об оперативно-розыскных мерах, так и об оперативно-розыскных мероприятиях (ст. 41, 95 и 157), а в модельном УПК для государств — участников Содружества Независимых Государств речь ведется как об оперативно-розыскных действиях (ст. 87, ч. 2, п. 8), так и об оперативно-розыскных мероприятиях (ст. 87, ч. 4—5). В отличие от этого, в оперативно-розыскной практике в зависимости от уровня ее организации различают три основных компонента: 1) оперативно-розыскные действия, 2) оперативно-розыскные мероприятия и 3) оперативно-розыскные операции. Итак, обоснованно можно заключить, что законодатель не дает определения понятию «оперативно-розыскное мероприятие» и тем самым не обеспечивает необходимых методологических предпосылок для единообразного понимания закона.

Одни юристы под оперативно-розыскными мероприятиями понимают проводимое уполномоченными на то лицами на основании и в порядке, предусмотренных законом, добытие фактических данных, входящих в предмет исследования по конкретному делу оперативного учета или первичным материалам, а также необходимых для решения других задач оперативно-розыскной деятельности¹⁸.

Другие правоведы считают, что оперативно-розыскные мероприятия — составной элемент структуры оперативно-розыскной деятельности, состоящей из системы взаимосвязанных действий, направленных на решение конкретных тактических задач. Оперативно-розыскные мероприятия носят разведывательно-поисковый характер и направлены на получение информации о лицах, замысляющих, подготавливающих и совершающих преступление, о наличии материальных следов противоправной дея-

¹⁸ См.: Михайлов В. И. Контролируемая поставка как оперативно-розыскная операция / Под ред. А. Ю. Шумилова. М., 1998. С. 60.

тельности, месте нахождения лиц, скрывающихся от следствия и суда, а также без вести пропавших¹⁹.

А. Ю. Шумилов под составом оперативно-розыскного мероприятия понимает систему элементов объективного и субъективного свойства, предусмотренных Федеральным законом «Об оперативно-розыскной деятельности» и нормативно-правовыми актами органов, характеризующих определенное общественно-полезное действие (мероприятие или операцию) как оперативно-розыскное мероприятие. Именно категория «состав оперативно-розыскного мероприятия» позволяет оперативному работнику (а также судье, прокурору и др.) конкретное оперативно-розыскное деяние оценить как оперативно-розыскное мероприятие, а не как иное общественно полезное деяние (следственное действие и т. п.), с одной стороны, или как некое правонарушение — с другой. С помощью нормативной категории — состава оперативно-розыскного мероприятия — должен разрешаться вопрос о наличии/отсутствии в совершенном участника оперативно-розыскной деятельности в том или ином деянии признаков оперативно-розыскного мероприятия и, следовательно, его законности. Таким образом, юридический состав оперативно-розыскного мероприятия есть нормативно-логическая модель реального оперативно-розыскного мероприятия²⁰.

Оперативно-розыскное мероприятие, на наш взгляд, — это конкретная форма осуществления оперативно-розыскной деятельности уполномоченными на то правоприменительными органами в соответствии с действующим законодательством Российской Федерации с целью получения фактической и/или оперативно-розыскной информации в интересах борьбы с преступностью, защиты прав и законных интересов граждан, общества и государства.

Перечень оперативно-розыскных мероприятий приведен в ст. 6 Федерального закона «Об оперативно-розыскной деятельности». Он

¹⁹ См.: Чечетин А. Е. Оперативно-розыскные мероприятия // Федеральный закон «Об оперативно-розыскной деятельности»: Науч.-практ. коммент. / Под ред. В. В. Николюка, В. В. Кальницкого, А. Е. Чечетина. Омск, 1999. С. 43.

²⁰ Комментарий к Федеральному закону «Об оперативно-розыскной деятельности»: С постанейным приложением нормативных актов и документов / Авт.-сост. д-р юрид. наук, проф. А. Ю. Шумилов. 5-е изд., испр. и доп. М., 2003. С. 62—63.

может быть изменен и дополнен только федеральным законом, т. е. является закрытым.

В зависимости от характера и степени общественной значимости оперативно-розыскных мероприятий их можно разделить на следующие группы.

- Оперативно-розыскные мероприятия, не ограничивающие конституционные права человека и гражданина. К этой категории относятся: опрос, наведение справок, сбор образцов для сравнительного исследования (кроме сбора образцов в жилище и сбора образцов голоса человека путем контроля его телефонных переговоров), проверочная закупка, исследование предметов и документов, наблюдение (кроме наблюдений, связанных с проникновением в жилище), отождествление личности, оперативное внедрение, контролируемая поставка.

- Оперативно-розыскные мероприятия, ограничивающие конституционные права человека и гражданина, которые проводятся только в ходе уголовно-розыскного процесса для решения задач по обнаружению признаков преступления, возбуждение уголовного дела по которым обязательно, а равно о событиях или действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации (Федеральный закон «Об оперативно-розыскной деятельности», ст. 8, ч. 2).

Рассматриваемую категорию оперативно-розыскных мероприятий можно подразделить на два вида:

- 1) оперативно-розыскные мероприятия, проведение которых всегда влечет ограничение конституционных прав человека и гражданина: контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров, снятие информации с технических каналов связи;

- 2) оперативно-розыскные мероприятия, при проведении которых конституционные права человека и гражданина ограничиваются только в специально предусмотренных законодателем случаях: оперативный досмотр, наблюдение, сбор образцов для сравнительного исследования, сопряженные с проникновением в жилище.

- Особо острые оперативно-розыскные мероприятия, которые направлены на противодействие совершению тяжких

и особо тяжких преступлений. Здесь в первую очередь имеется в виду оперативный эксперимент, но в определенных случаях сюда можно отнести наблюдение и оперативный досмотр связанных с проникновением в жилище при сложной оперативной обстановке.

- По форме осуществления оперативно-розыскные мероприятия могут быть гласными и негласными. Например, оперативное внедрение проводится только в негласной форме, а опрос может быть как гласным, так и негласным.

- По времени осуществления различают длительные оперативно-розыскные мероприятия и разовые. Например, контроль технических каналов связи допускается на основании судебного решения сроком до 180 суток, а к разовым можно отнести отождествление личности.

- По применяемым силам и средствам оперативно-розыскные мероприятия могут проводиться с участием агентов, а также с использованием технических сил и средств, т. е. комплексно²¹.

При анализе положений ст. 6 Федерального закона «Об оперативно-розыскной деятельности» нетрудно заметить, что в ней содержится лишь перечень оперативно-розыскных мероприятий, но не раскрывается их содержание. На наш взгляд, было бы целесообразно проявить последовательность и раскрыть основное их содержание, дать соответствующие дефиниции.

Исходя из темы публикации нас интересует в первую очередь оперативно-розыскные мероприятия с использованием технических сил и средств, т. е. оперативно-технические мероприятия. Законодатель также не дает понятия названной формы оперативно-розыскной деятельности. На сегодня можно с уверенностью утверждать, что нет таких оперативно-розыскных мероприятий, где бы не использовались технические средства.

Возьмем для примера такое самостоятельное оперативно-розыскное мероприятие, как опрос, т. е. сбор фактической или оперативной информации, имеющей значение для решения конкретной задачи оперативно-розыскной деятельности. При проведении опро-

²¹ См., в частности: Комментарий к Федеральному закону «Об оперативно-розыскной деятельности»... / Авт.-сост. А. Ю. Шумилов. С. 64—66.

са, согласно ч. 3 ст. 6 Федерального закона «Об оперативно-розыскной деятельности», его субъекты вправе использовать (гласно или негласно) технические и иные средства. В частности, одним из таких средств признается использование специализированного полиграфа²². Однако вопрос о законности использования подобного метода остается открытым, а основания и условия его использования предусмотрены только ведомственными нормативно-правовыми актами²³.

В правоохранительной практике зарубежных стран проверки на полиграфе, как правило, используются не в интересах получения судебных доказательств для вынесения решения по делу, а для содействия следователю в выборе более перспективного и обоснованного направления его работы²⁴.

Так как же соотносятся оперативно-техническое и оперативно-розыскное мероприятия? На наш взгляд, так же, как соотносятся часть и целое. К оперативно-техническим мероприятиям следует относить только те оперативно-розыскные мероприятия, где применяются специальные технические средства для негласного получения информации уполномоченными на то правоприменительными органами, наделенными правом осуществления оперативно-розыскной деятельности.

²² *Полиграф* — многоканальный медико-биологический прибор, который регистрирует эмоциональное состояние опрашиваемого при воздействии на него словесными или зрительными раздражителями и предназначен для одновременного учета нескольких параллельно протекающих в организме физиологических процессов (кровяное давление, дыхание, биотоки мозга, работа сердца, скелетной и гладкой мускулатуры). Полиграф применяется в клинической медицине, медико-биологических и психологических исследованиях (см.: Комментарий к Федеральному закону «Об оперативно-розыскной деятельности»... / Авт.-сост. А. Ю. Шумилов. С. 66—67).

²³ См., например: Приказ Министерства внутренних дел России от 28 декабря 1994 года № 437 «Об утверждении Инструкции о порядке использования полиграфа при опросе граждан» // Бюл. текущего законодательства МВД. 1995. Вып. 13. С. 46—49. Аналогичный акт принят Федеральной службой безопасности России (см.: Инструкция о порядке применения органами Федеральной службы безопасности опроса с использованием полиграфа. ??? 1997 года).

²⁴ См.: Громов Н. А. Новое в расследовании преступлений / Громов Н. А., Францифоров Ю. В., Николайченко В. В. // Следователь. 1998. № 2. С. 31—32.

Итак, к оперативно-техническим мероприятиям следует отнести следующие: наблюдение, контроль почтовых отправлений, телеграфных и иных сообщений, прослушивание телефонных переговоров, снятие информации с технических каналов связи²⁵.

Попытаемся определить (поскольку это не сделано в Федеральном законе «Об оперативно-розыскной деятельности») содержание названных оперативно-технических мероприятий и провести разграничение между оперативно-розыскными и оперативно-техническими мероприятиями.

• Наблюдение состоит в тайном, целенаправленном, систематическом, непосредственном (визуальном) или опосредованном (с помощью использования специальных технических средств) восприятии и фиксации фактической или оперативно-значимой информации для решения конкретных задач оперативно-розыскной деятельности.

В зависимости от метода получения информации (непосредственно или с помощью удаленного доступа) выделяют три основных вида наблюдения:

1) физическое наблюдение основано на визуальном методе получения информации и заключается в негласном непосредственном восприятии наблюдателем деятельности изучаемого лица или объекта²⁶;

2) электронное наблюдение проводится с помощью специальных технических средств с удаленного контрольного пункта и заключается в негласном направленном восприятии деятельности изучаемого лица или материального объекта посредством аудио-

²⁵ Хотелось бы сразу оговориться. При проведении обследований помещений, зданий, сооружений, участков местности и транспортных средств (в ходе оперативного досмотра), как правило, применяются специальные технические средства (вскрытие запирающих устройств). Контролируемая поставка и оперативный эксперимент также не обходятся без использования специальных технических средств. Нас интересуют специальные технические средства, применяемые в ходе проведения электронного наблюдения. На них и будем ориентироваться в дальнейшем.

²⁶ Наблюдателем является, как правило, сотрудник оперативно-поискового подразделения субъекта оперативно-розыскной деятельности или агент.

и видеосредств, с целью слухового или визуального контроля, а также документирования преступных действий²⁷;

3) смешанное (комплексное) наблюдение основано на применении двух вышеназванных видов наблюдения одновременно.

• Контроль почтовых отправлений, телеграфных и иных сообщений заключается в действиях по конспиративной перлюстрации (от лат. *perlustrare* — вскрытие и просмотр без ведома адресата) письменной или иной зафиксированной на материальном носителе корреспонденции с целью обнаружения сведений о преступной деятельности изучаемого лица, проводимой специальными подразделениями органов, осуществляющих оперативно-розыскную деятельность, посредством личного участия в организации и проведении непосредственно в учреждениях связи по месту отправления или поступления объектов контроля, используя при этом помощь должностных лиц и специалистов, обладающих научными, техническими и иными специальными знаниями, а также отдельных граждан с их согласия на гласной и негласной основе.

Субъектом рассматриваемого оперативно-технического мероприятия в соответствии с Федеральным законом «Об оперативно-розыскной деятельности» (ст. 6, ч. 4) является Федеральная служба безопасности России²⁸.

В анализируемое мероприятие не входит цензура корреспонденции осужденных и досмотр почтовых и багажных отправок, осуществляемый сотрудниками Федеральной службы безопасности России, таможенных органов и органами внутренних дел при

²⁷ Электронное наблюдение как оперативно-техническое мероприятие проводится сотрудниками оперативно-технических подразделений субъектов оперативно-розыскной деятельности. Его не стоит смешивать с электронным наблюдением, осуществляемым в публичных местах (вокзалы, метро, магазины, автомобильные стоянки и т. п.), когда преследуются совершенно другие цели, не ограничиваются конституционные права граждан и не привлекаются субъекты оперативно-розыскной деятельности. Однако материалы, полученные в ходе подобного вида электронного наблюдения, также могут быть использованы в уголовном процессе или в оперативно-розыскной деятельности.

²⁸ Детализацию этой нормы см.: п. 1 Указа Президента РФ от 1 сентября 1995 года № 891 «Об упорядочении организации и проведения оперативно-розыскных мероприятий с использованием технических средств» // Собр. законодательства РФ. 1999. № 24. Ст. 2954.

наличии данных о перевозке (пересылке) наркотических средств, психотропных веществ и их прекурсоров²⁹.

- Прослушивание телефонных переговоров — комплексное оперативно-техническое мероприятие по конспиративному слуховому контролю с обязательным использованием специальных технических средств переговоров, ведущихся лицами оперативной заинтересованности субъектов оперативно-розыскной деятельности, с использованием названными лицами линий единой сети электросвязи России и услуг операторов связи России, их документированием с целью получения фактической или оперативно-значимой информации о преступной деятельности изучаемого лица.

Субъектами данного оперативно-технического мероприятия являются Министерство внутренних дел России и Федеральная служба безопасности России. Причем территориальные подразделения МВД России обязаны согласовывать проведение рассматриваемого мероприятия с органами ФСБ, если прослушивание абонента осуществляется со станционной части средств связи³⁰.

- Снятие информации с технических каналов связи — комплексное оперативно-техническое мероприятие по конспиративному получению с последующим документированием субъектами оперативно-розыскной деятельности фактической или оперативно-значимой информации путем съема с обязательным использованием специальных технических средств электромагнитных полей, возникающих в результате передачи названной информации по линиям единой сети электросвязи России, лицами оперативной заинтересованности субъектов оперативно-розыскной деятельности.

Все перечисленные оперативно-технические мероприятия ограничивают конституционные права граждан, в связи с чем их проведение допускается только на основании судебного решения и при наличии информации, указанной в ч. 2 ст. 8 Федерального закона «Об оперативно-розыскной деятельности». Кроме того, рассматри-

²⁹ См.: Уголовно-исполнительного кодекса РФ (ст. 91, ч. 2) // Собр. законодательства РФ. 1997. № 2. Ст. 198; Федеральный закон от 8 января 1998 года № 3-ФЗ «О наркотических средствах и психотропных веществах» (ст. 48, ч. 2) // Собр. законодательства РФ. 1998. № 2. Ст. 219.

³⁰ См.: Указ Президента РФ № 891.

ваемые виды оперативно-технических мероприятий исполняются только силами и средствами территориальных органов оперативно-технических подразделений МВД и ФСБ России при надлежаще оформленном и утвержденном соответствующим руководителем субъекта оперативно-розыскной деятельности бланке задания. Запрещается проведение названных оперативно-технических мероприятий в целях оперативно-проверочной работы, а также выявления, пресечения, предупреждения и раскрытия преступлений небольшой и средней тяжести (Федеральный закон «Об оперативно-розыскной деятельности», ст. 7, ч. 2, п. 1—4, 6).

В случаях, которые не терпят отлагательства и могут привести к совершению тяжкого преступления, а также при наличии данных о событиях и действиях, создающих угрозу государственной, военной, экономической или экологической безопасности Российской Федерации, на основании мотивированного постановления одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, допускается проведение рассмотренных оперативно-технических мероприятий с обязательным уведомлением судьи в течение суток. В течение 48 часов с момента начала проведения оперативно-технического мероприятия орган, его осуществляющий, обязан получить судебное решение о проведении такого оперативно-технического мероприятия либо прекратить его проведение.

В случае возникновения угрозы жизни, здоровью, собственности отдельных лиц по их заявлению или с их согласия в письменной форме разрешается прослушивание переговоров, ведущихся с их телефонов, на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность, с обязательным уведомлением соответствующего судьи в течение 48 часов (Федеральный закон «Об оперативно-розыскной деятельности», ст. 8, ч. 3).

При необходимости в ходе проведения данных оперативно-технических мероприятий допускается прерывание предоставляемых услуг связи (Федеральный закон «Об оперативно-розыскной деятельности», ст. 15, ч. 1; Федеральный закон «О связи», ст. 64, ч. 3).

Законодателем установлен только максимальный предел возможного проведения оперативно-технического мероприятия — 180 суток со дня вынесения судьей разрешающего постановления с последу-

ющей возможностью его продления при надлежащем обосновании со стороны субъекта оперативно-розыскной деятельности.

Как видно из вышеизложенного, рассмотренные оперативно-технические мероприятия имеют не только много общего, но и ряд существенных отличий. Кроме того, перечень оперативно-розыскных мероприятий, приведенный в ст. 6 Федерального закона «Об оперативно-розыскной деятельности», на наш взгляд, оставляет неохваченными сети документальной электросвязи и телекоммуникационные системы с использованием мультимедиа технологий. К каким видам оперативно-розыскных мероприятий отнести контроль пейджинговых сообщений (в т. ч. SMS-сообщения), электронную и голосовую почту, информацию, передаваемую по единым сетям электросвязи России между Интернет-пользователями и просто между пользователями компьютеров? Процент передаваемой информации с использованием названных средств связи является достаточно внушительным, чтобы не обращать на него внимания, и с каждым днем он будет увеличиваться в геометрической прогрессии. Законодатель пока никак не отреагировал на эти изменения. Федеральный закон «О связи» в его новой редакции также обходит данный вопрос стороной. Все нормы сосредоточены на ведомственном и подзаконном уровне³¹.

Например, электронная почта не попадает по действующему Федеральному закону «Об оперативно-розыскной деятельности»

³¹ См., например: Приказ Государственного комитета по связи и информатике РФ от 20 апреля 1999 года № 70 «О технических требованиях к системе технических средств, для обеспечения функции оперативно-розыскных мероприятий на сетях электросвязи РФ» (с соответствующими приложениями); Письмо первого заместителя Министерства связи РФ руководителям организаций и операторам связи от 30 апреля 1996 года № 2259 «О взаимодействии с органами осуществляющими оперативно-розыскную деятельность»; Решение Государственной комиссии по электросвязи при Государственном комитете РФ по телекоммуникациям от 29 сентября 1999 года № 63; Приказ Министерства РФ по связи и информатизации от 25 июля 2000 года № 130 «О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования»; Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность (утвержд. Постановлением Правительства РФ от 27.08.2005 г. № 538) // Рос. газ. 2005. 2 сент.

под контроль почтовых отправлений, телеграфных и иных сообщений. Так, под почтовыми отправлениями понимаются местные и иногородние письма и почтовые открытки, бандероли и мелкие пакеты, посылки, почтовые контейнеры, печатные издания (Федеральный закон от 17 июля 1999 года № 176-ФЗ «О почтовой связи», ст. 23²).

Телеграфное сообщение — разновидность корреспонденции. Состоит в адресованной электропередаче информации по телеграфному каналу связи с фиксацией выходных данных на материальном носителе (бумаге) в виде печатного текста. Этим материальным носителем является телеграмма — краткое текстовое сообщение, передаваемое, переданное или предназначенное для передачи средствами телеграфной связи («Правила предоставления услуг телеграфной связи», утверждены Постановлением Правительства РФ от 28.08.1997 г. № 1108³³).

Иное сообщение — любая корреспонденция, кроме почтового отправления и телеграфного сообщения, отправленная по сети почтовой, электрической связи или иным способом. В частности, им может быть почтовый перевод денежных средств³⁴.

Если контроль электронной почты попытаться отнести к такому оперативно-техническому мероприятию, как снятие информации с технических каналов связи, то и здесь у законодателя нет однозначного понимания. Ни Федеральный закон «Об оперативно-розыскной деятельности», ни Федеральный закон «О связи» не содержат в своих основных понятиях определения технического канала связи³⁵.

А. Ю. Шумилов утверждает, что «...прослушивание телефонных переговоров должно заключаться в выявлении, оценке и фиксации необходимых сведений только при устных переговорах. Контроль

³² Собр. законодательства РФ. 1997. № 35. Ст. 4136.

³³ Рос. газ. 1997. 17 сент. (утратили силу).

³⁴ См.: Комментарий к ФЗ «Об оперативно-розыскной деятельности»... / Авт.-сост. А. Ю. Шумилов. С. 81.

³⁵ Федеральный закон «О связи» в ст. 2 дает определение линии связи как линии передачи, физические цепи и линейно-кабельные сооружения связи, а сети связи как технологической системы, включающей в себя средства и линии связи и предназначенной для электросвязи или почтовой связи.

всех остальных форм передачи сведений (не устных) должен быть отнесен к снятию информации с технических каналов связи»³⁶.

А. Е. Чечётин понимает под снятием информации с технических каналов связи «...оперативно-техническое мероприятие, заключающееся в перехвате с помощью специальных технических средств открытой (незашифрованной) информации, передаваемой проверяемыми лицами по техническими каналам связи»³⁷.

Одни юристы понимают под техническими каналами связи телексы, факсимильные, селекторные, радиорелейные каналы передачи данных либо абонентского телеграфирования, компьютерные сети, радиопереговорные устройства, основанные на использовании радиоволн³⁸. Другие — элементы сети электросвязи, т. е. технологические системы, обеспечивающие один или несколько видов передач: телефонную, телеграфную, факсимильную передачу данных и других видов документальных сообщений, включая обмен информацией между персональными электронно-вычислительными машинами, телевизионное, звуковое и иные виды радио- и проводного вещания³⁹. Таким образом, происходит простое механическое добавление тех или иных свойств технического канала связи, которые появляются в нашей повседневной жизни с внедрением новых услуг связи.

Под прослушивание телефонных переговоров контроль почтовых сообщений, передаваемых с помощью электронной почты, также отнести нельзя. Получить и зафиксировать информацию нам, может быть, и удастся, но вот оценить ее на слух без дополнительной обработки — вряд ли.

То же самое можно сказать по поводу пейджинговых сообщений (стандарт POGSAC) или сообщений в стандарте FLEX⁴⁰.

³⁶ Комментарий... / Авт.-сост. А. Ю. Шумилов. С. 87.

³⁷ Чечетин А. Е. Оперативно-розыскные мероприятия. С. 56—57.

³⁸ См.: Гуцин А. Н. Оперативно-розыскная деятельность: Совершенствование форм вхождения ее результатов в уголовный процесс: Учеб.-практ. пособие / Гуцин А. Н., Громов Н. А., Царева Н. П. М., 2003. С. 29.

³⁹ См.: Комментарий... С. 87; Гаврилов Ю. В., Дубоносов Е. С. Исследование контроля и записи телефонных и иных переговоров в раскрытии и расследовании преступлений: Учеб. пособие. М., 2003. С. 12—13.

⁴⁰ Стандарт POGSAC отличается от стандарта FLEX тем, что первый является открытым, т. е. не подвержен дополнительной кодировке передаваемого сигнала. Если следовать рассуждениям А. Е. Чечётина, то перехват сообщений стандарта FLEX

Если взять голосовую почту, то, с большой оговоркой, можно говорить о контроле телефонных переговоров. Ведь переговоры проводиться не будут. Поток передаваемой информации всегда будет односторонним. Сначала от автора оставленного сообщения, затем к потребителю оставленного письма. Подобные рассуждения можно продолжить и по поводу контроля сетей документальной электросвязи. Система технических средств по обеспечению оперативно-розыскных мероприятий направлена в первую очередь на решение технической стороны получения информации в ходе проведения оперативно-розыскной деятельности, но остается за рамками Федерального закона «Об оперативно-розыскной деятельности».

Сегодня, на наш взгляд, нецелесообразно отдельно выделять два таких оперативно-технических мероприятия, как прослушивание телефонных переговоров и контроль технических каналов связи, а также систему технических средств по обеспечению оперативно-розыскных мероприятий. В этом просто нет необходимости. Большинство операторов связи оказывают свои услуги в комплексе (предоставляют так называемый пакет услуг). Например, сотовая телефонная компания предоставляет услуги связи в широкополосном режиме⁴¹. Имея современный ноутбук, пользователь может одновременно со своего сотового телефона осуществлять выход в Интернет, передавать и получать сообщения по электронной почте, получать сообщения из своего голосового почтового ящика, передавать и получать пейджинговые сообщения (SMS-сообщения), передавать и принимать видеоизображения, передавать факсимильную информацию и, наконец, пользоваться им, как обыкновенным

не попадает под такое оперативно-техническое мероприятие, как контроль технических каналов связи. Тем более что путь прохождения сигнала от телефона абонента, посланного сообщение на пейджер клиента, до самого приемника достаточно сложен. Вначале контроль рассматриваемого сообщения попадает под оперативно-техническое мероприятие «прослушивание и запись телефонных переговоров» (если сообщение было передано, например, с проводного телефонного аппарата), а затем, очень условно, под контроль технических каналов связи (например, при проведении мониторинга радиоэфира). А если сообщение отправлено через международную телефонную связь? Здесь сигнал может неоднократно преобразовываться и попадать формально под разные виды оперативно-технических мероприятий. Так чем же руководствоваться? Точкой подключения специальных технических средств? Местом их установки или внедрения?

⁴¹ См.: Федеральные стандарты GSM 900/1800 МГц, CDMA.

телефонным аппаратом с помощью переадресации на проводной телефон.

Какой вид оперативно-розыскного мероприятия может быть проведен в отношении такого абонента? А если передаваемая информация для дополнительного обеспечения конфиденциальности шифруется оператором связи? Как поступать в этом случае сотрудникам правоприменительных органов и судьям? Вопросов по этой проблеме больше, чем ответов.

Хотелось бы еще раз обратить внимание на то, что оперативно-технические мероприятия — самые острые из оперативно-розыскных мероприятий и в наибольшем объеме ограничивают конституционные права граждан Российской Федерации. Нельзя проводить названные мероприятия, не имея четко установленных для них законодателем рамок и пределов, не понимая их содержания и руководствуясь только ведомственным нормотворчеством.

Предусматривать в Федеральном законе «Об оперативно-розыскной деятельности» на каждый вид связи или форму носителя информации самостоятельный вид оперативно-розыскных мероприятий нецелесообразно. Технологии и далее будут развиваться в геометрической прогрессии. На наш взгляд, было бы логично объединить имеющиеся оперативно-технические мероприятия, такие как прослушивание телефонных переговоров и контроль технических каналов связи, в одно оперативно-техническое мероприятие с учетом имеющихся наработок в области системы технических средств по обеспечению оперативно-розыскных мероприятий, а именно внести в ст. 6 Федерального закона «Об оперативно-розыскной деятельности» новое оперативно-розыскное мероприятие — электронное наблюдение, исключив тем самым два вышеназванных:

Электронное наблюдение — комплексное оперативно-техническое мероприятие, проводимое на основании судебного решения, заключающееся в конспиративном получении оперативно-техническими подразделениями субъектов оперативно-розыскной деятельности фактической или оперативно-значимой информации с помощью специальных технических средств, фиксирующих и копирующих названную информацию во время ее передачи объектами оперативной заинтересованности через единые сети электросвязи России.

При этом под э л е к т р о с в я з ь ю 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 (Федеральный закон «О связи», ст. 2).

Порядок проведения электронного наблюдения, его сроки и оформление идентичны порядку, срокам и оформлению таких оперативно-технических мероприятий, как прослушивание телефонных переговоров и контроль технических каналов связи.

Предлагаемое содержание электронного наблюдения в качестве нового вида оперативно-технического мероприятия позволяет четко определить границы уже рассмотренных выше оперативно-технических мероприятий, а именно контроля почтовых отправлений, телеграфных и иных сообщений и наблюдения.

По нашему мнению, наблюдение должно включать в себя только визуальный метод получения информации и заключаться в негласном, непосредственном восприятии наблюдателем деятельности изучаемого лица или объекта. Электронная его составляющая должна быть поглощена предлагаемым видом оперативно-технического мероприятия.

Под контролем почтовых отправлений, телеграфных и иных сообщений будем понимать оперативно-техническое мероприятие, проводимое на объектах почтовой связи и почтовых маршрутов операторов почтовой связи, обеспечивающих прием, обработку, перевозку (передачу), доставку (вручение) почтовых отправлений, а также осуществление почтовых денежных переводов.

Говоря об электронном наблюдении как о новом виде оперативно-технического мероприятия, необходимо отметить, что его появление имеет под собой достаточно прочный фундамент организационных и технических мероприятий по внедрению системы технических средств по обеспечению оперативно-розыскных мероприятий на единых сетях электросвязи России.

После принятия новой редакции Федерального закона «Об оперативно-розыскной деятельности» не утихает полемика в средствах массовой информации о законности и целесообразности внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий. Мнения самые полярные — от попыток признания

системы технических средств по обеспечению оперативно-розыскных мероприятий антиконституционной до объявления ее приоритетным направлением в сфере оперативно-розыскной деятельности.

В качестве примеров различных точек зрения на данную тему можно привести следующие мнения.

Так, О. А. Иконникова утверждает, что в последнее время в прессе появились сведения о разработке нового проекта системы оперативно-розыскных мероприятий на сетях документальной электросвязи, так называемой СОРМ-2. Текущий проект названной системы 20 августа 1998 года был утвержден на совещании в Госкомсвязи России под названием «Общих технических требований к системе технических средств по обеспечению функций оперативно-розыскных мероприятий на сетях (службах) документальной электросвязи». Использование подобных методов борьбы с компьютерной преступностью, с точки зрения автора статьи, может повлечь обратный эффект. Учитывая, что одни только слухи о разработке СОРМ-2 вызвали бурю неприятия и молниеносно появились ответные средства защиты компьютерной информации, можно догадываться, что последует за претворением подобного проекта в жизнь. По мнению автора, в наше время даже взломы сверхзащищенных компьютерных сетей Центрального разведывательного управления и Пентагона — реальность, что уж говорить об ответной реакции граждан, конституционные права которых могут оказаться под угрозой, ведь среди этих граждан нет-нет да и окажется кто-то, превосходно разбирающийся в компьютерных технологиях и жаждущий мести.

Вопрос о целесообразности и законности уже применяемых и только планируемых к применению оперативно-розыскных мероприятий, к сожалению, является лишь одной гранью гораздо более сложной и глубокой проблемы, касающейся защиты компьютерной информации от несанкционированного доступа (как преступного, так и «правомерного») и в конечном счете — естественных прав личности на неприкосновенность частной жизни⁴².

Радует, что автор признает наличие «специалистов» в России, способных осуществить «взлом сверхзащищенных сетей Централь-

⁴² См. об этом: *Иконникова О. А.* Права человека: СОРМ-2 — новый электронный колпак // Юрист. 1999. №2. С. 27, 28.

ного разведывательного управления» и, наверное, готовых проделать то же самое в отношении отечественных сетей подобного уровня защиты. Огорчает непонимание того, что система технических средств по обеспечению оперативно-розыскных мероприятий направлена на выявление и предупреждение несанкционированного доступа в сети документальной электросвязи, а значит, на охрану, а не на нарушение конституционных прав граждан и вторжение в их частную жизнь.

Вот как комментирует газета «Московский комсомолец — Урал» издание приказа Министерства РФ по связи и информатизации от 25 июля 2000 года № 130 «О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования» в своей заметке. Неизвестный автор пишет, что все телефонные, сотовые и пейджинговые компании уже встали по стойке «смирно» в связи с приказом министра связи России, разрешающего прослушивать телефонные разговоры частных лиц. Более того, операторы связи готовы открыть курсы обучения по пользованию прослушивающими системами.

Упомянутый приказ 9 августа 2000 года утвердило Министерство юстиции России. Весной 2000 года слухи о возможности тотальной прослушки наделали немало шума: вспомнились советские времена, когда все мы были «на крючке у Комитета государственной безопасности»⁴³. Поэтому, чтобы узаконить законность приказа, соответствующие органы для соблюдения демократических норм отправили документ на согласование с Минюстом. Произошла настоящая революция в прослушивании. Если до сего дня на подключение к частному телефону необходимо было разрешение соответствующих органов — прокуратуры, Федеральной службы безопасности, суда, то теперь «добро» дано заранее для всех свыше. При этом, видимо, не следует рассчитывать, что спецслужбы всегда будут соблюдать нормы законности.

Более того, по некоторым сведениям в приказе рекомендовано в каждой телефонной компании устанавливать новейшую аппаратуру, дабы клиента не беспокоили щелчки в трубке⁴⁴.

⁴³ Из уха в ухо // Моск. комсомолец — Урал. 2000. 31 авг. С. 12.

⁴⁴ Там же.

Комментарии излишни, а заметка в газете даже не подписана. Автор статьи полностью не представляет содержания затронутой темы, но все же пытается высказать свое мнение (в данном случае от имени целой газеты, имеющей достаточно солидный тираж). Отмечу лишь, что прокуратура в связи с принятием Конституции РФ лишена права давать санкцию на прослушивание телефонных и иных переговоров, а Федеральная служба безопасности вообще никогда подобным правом не обладала. В соответствии со ст. 23 Конституции РФ разрешение для проведения названного оперативно-розыскного мероприятия выдается только судом и при наличии законных оснований.

В обсуждении затронутой темы не отстают и электронные информационные системы, в частности Интернет⁴⁵.

В споре, как говорится, рождается истина, и законодателю следует принимать во внимание данные высказывания (пусть и анонимные), авторы которых, безусловно, правы в одном: система технических средств по обеспечению оперативно-розыскных мероприятий не должна способствовать удорожанию услуг связи. Государству необходимо подробнейшим образом регламентировать распределение затрат в ходе ее внедрения и основную часть расходов взять на себя.

Анализируя правовую основу внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий, следует отметить, что законодатель практически не раскрывает содержания данного понятия ни в Федеральном законе «Об оперативно-розыскной деятельности», ни в Федеральном законе «О связи»⁴⁶.

⁴⁵ Приведем в этой связи лишь некоторые электронные адреса, где система технических средств по обеспечению оперативно-розыскных мероприятий обсуждается с самых разнообразных точек зрения: <http://www.agentura.ru/timeline/1998/sorm>; <http://www.aboutphone.info/lib/sorm.html>; <http://www.hro.org/gilc/sormsp.html>; <http://www.libertarium.ru/sorm>; http://www.cat.doi.ru/books/Safety/glava_08-1.htm; <http://www.taf.ilim.ru/-taf/public/sorm1.html>; <http://www.telecomnews.ru/sorm/S3.html>; <http://www.rusawm.com./articles.php?id=132>; <http://www.svcons.ru/normdoc/sorm.shtml>; http://www.infoyar.ru/bp.php?show=/Docum/DocumShou_DocumID_16963.htmlsorm и мн. др.

⁴⁶ Упоминание о системе технических средств по обеспечению оперативно-розыскных мероприятий на уровне федерального закона присутствует только в Федеральном законе «Об органах Федеральной службы безопасности РФ» (ст. 15, п. 4).

На наш взгляд, это можно объяснить тем, что методика и тактика проведения оперативно-технических мероприятий представляет собой информацию с ограниченным доступом лиц. И это вполне оправданно в отношении оперативного досмотра, негласного наблюдения с использованием аудио- или видеозаписи и т. д. Но внедрение системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях электросвязи проводится гласно и представляет собой одно из основных требований лицензии на предоставление услуг связи. Поэтому содержание названной системы должно быть раскрыто на уровне федерального закона.

Для устранения образовавшегося пробела, на наш взгляд, необходимо внести дополнение в ч. 3 ст. 6 Федерального закона «Об оперативно-розыскной деятельности», а также дать общее определение системы технических средств по обеспечению оперативно-розыскных мероприятий как составляющей предлагаемого оперативно-технического мероприятия — электронного наблюдения и изложить это в следующей редакции:

В ходе проведения оперативно-розыскных мероприятий используются информационные системы, системы технических средств по обеспечению оперативно-розыскных мероприятий, видео- и аудиозапись, кино- и фотосъемка, а также другие технические и иные средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде.

Система технических средств по обеспечению оперативно-розыскных мероприятий является одной из составляющих электронного наблюдения как одного из оперативно-розыскных мероприятий и входит в состав аппаратных и программных средств дополнительного оборудования стационарной аппаратуры средств связи, независимо от их формы собственности и ведомственной принадлежности.

В ходе наших дальнейших рассуждений рассмотрим возможность использования оперативно-розыскной информации, полученной в ходе проведения электронного наблюдения и других видов оперативно-розыскных мероприятий, в целях доказывания в уголовном судопроизводстве.

§ 3. Использование оперативно-розыскной информации, полученной в ходе проведения электронного наблюдения, в доказывании по уголовным делам

Следует согласиться с тем, что соотношение уголовно-процессуальной деятельности и оперативно-розыскной деятельности по уголовным делам может иметь форму зависимости результатов оперативно-розыскной деятельности от уголовно-процессуальных процедур, призванных разрешить вопрос о доступе оперативно-розыскной информации в уголовно-процессуальную сферу⁴⁷.

Анализ целей и задач оперативно-розыскной деятельности позволяет сделать вывод о том, что ей не придается самодовлеющего значения⁴⁸, но в своей основе она направлена прежде всего на успешное решение задач уголовного процесса, на «обеспечение доказывания по уголовному делу»⁴⁹. Поэтому большое значение имеет совершенствование правовых норм, указывающих на связь оперативно-розыскной деятельности и уголовного процесса. Так, С. А. Шейфер обращает внимание на некоторые черты общности уголовного процесса и оперативно-розыскной деятельности, выделяя в качестве таковых подобие задач, приемов получения нужной информации, а также сходство результатов этой деятельности. Общность приемов и, в известной мере, полученных результатов, не должна вызывать недоумения. В любом познавательном процессе, направленном на установление правонарушения, предметом исследования являются следы, оставленные событием, а само исследование представляет собой отражательный процесс⁵⁰.

Сегодня эта связь довольно отчетливо прослеживается в предписаниях ст. 11 Федерального закона «Об оперативно-розыскной

⁴⁷ См.: Основы оперативно-розыскной деятельности: Учеб. / Под ред. В. Б. Руншайло. СПб., 2000. С. 62.

⁴⁸ См.: *Зажитский В. И.* Связь оперативно-розыскной деятельности и уголовного процесса // Государство и право. 1995. № 6. С. 57.

⁴⁹ *Гришин А. И.* Использование результатов оперативно-розыскной деятельности в доказывании // Проблемы реализации судебной реформы в России. Вып. 1. Саратов, 1998. С. 80.

⁵⁰ См.: *Шейфер С. А.* Доказательственное значение Закона об оперативно-розыскной деятельности // Государство и право. 1994. № 1. С. 94—97.

деятельности». В соответствии с ними результаты названной деятельности могут быть использованы для подготовки и осуществления следственных и судебных действий, а также в доказывании по уголовным делам в соответствии с положениями уголовно-процессуального закона, регламентирующими собирание, проверку и оценку доказательств⁵¹. Хотя указанный Федеральный закон и не устанавливает какой-либо процессуальной формы проведения оперативно-розыскных мероприятий, можно сделать вывод, что он в то же время допускает использование полученных таким путем данных в качестве доказательств по уголовным делам после их проверки на следствии и в суде⁵².

В юридической литературе отмечается, что доказывание представляет собой информационный процесс, т. е. получение информации, значимой для расследования уголовного дела⁵³.

Информация, полученная в ходе электронного наблюдения, которую использует следователь или дознаватель в своей работе по уголовному делу, весьма разнообразна. В зависимости от способов получения и доказательственного значения ее можно разделить на две основных группы — процессуальную и непроцессуальную.

Процессуальная информация может быть получена следователем либо другим субъектом уголовно-процессуальной деятельности с обязательным соблюдением установленного уголовно-процессуальным законодательством порядка. Уголовно-процессуальный закон указывает на конкретные способы извлечения информации из определенного носителя и соблюдения порядка, условий и последовательности применения этих способов в ряде процессуальных действий. Будучи заключенной в предусмотренную законом форму и отвечая требованиям относимости и допустимости, она

⁵¹ См.: *Пономаренков В. А.* Проблемы представления и использования доказательств в уголовном процессе: Автореф. дис. ... канд. юрид. наук. Саратов, 1998. С. 129—134.

⁵² См.: *Петрухин И. Л.* Частная жизнь (правовые аспекты) // Государство и право. 1999. № 1. С. 68.

⁵³ См. например: *Рапинов А. Р.* Вопросы следственного мышления в свете теории информации // Вопр. кибернетики и права. М., 1967. С. 180—200; *Трусов А. И.* Судебное доказывание в свете идей кибернетики // Там же. С. 20—25; *Белкин Р. С., Винберг А. И.* Криминалистика и доказывание. М., 1969. С. 167—215.

приобщается к уголовному делу и рассматривается в качестве доказательства — это первый и основной критерий разграничения процессуальной и непроцессуальной информации.

Непроцессуальная информация не обладает такими свойствами. К ней относятся также сведения, предоставляемые следователю или дознавателю оперативно-розыскными службами и полученные при проведении электронного наблюдения и других оперативно-розыскных мероприятий⁵⁴.

По признаку открытости и защищенности законом от разглашения непроцессуальная информация субъектов оперативно-розыскной деятельности подразделяется на гласную, полученную с помощью гласных мероприятий из гласных источников (например, при опросе граждан, оказавшихся на месте происшествия, видеокамер наружного наблюдения открыто размещенных в местах массового скопления людей), и негласную, полученную при проведении негласных мероприятий (например, оперативное внедрение, электронное наблюдение и т. п.) от негласного источника (негласный сотрудник оперативно-поискового или оперативно-технического подразделения либо лицо, сотрудничающее с осуществляющими оперативно-розыскную деятельность органами на конфиденциальной основе, и т. д.).

Необходимость использования в борьбе с преступностью наряду с гласными и официальными методами скрытых, разведывательных мер вполне очевидна.

Трудно представить себе противодействие преступности, тем более решительное наступление на нее с позиции абстрактного гуманизма и законности, учитывая, с одной стороны, размах преступности, ее структуру, динамику, характеристику преступных деяний и лиц, их совершивших, а с другой стороны — современные возможности правоприменительных органов. «Благо общества, — отмечал Вольтер, — столь несомненно является единственной мерой нравственного добра и зла, что мы вынуждены бываем в случае

⁵⁴ Сразу оговоримся: в том случае, если электронное наблюдение проводится в рамках оперативно-розыскной деятельности, а не следственного действия в рамках уголовного дела и по поручению следователя.

нужды изменять все наши идеи, созданные нами себе относительно справедливого и несправедливого»⁵⁵.

Вторым критерием разграничения процессуальной (доказательной) и непроцессуальной информацией является соответствие источника информации предъявляемым законом требованиям⁵⁶.

Требования закона, предъявляемые к доказательствам, позволяют отграничивать доказательственную и непроцессуальную информацию и, кроме того, называть источники последней. Анализируя УПК РФ, к источникам непроцессуальной информации можно отнести следующие:

- результаты следственных действий, проведенных с нарушением закона;
- показания свидетеля, который не может указать источник своей осведомленности;
- показания защитника об обстоятельствах, которые ему стали известны в связи с выполнением своих обязанностей;
- показания лица, не способного в силу своих психических и физических недостатков правильно воспринимать обстоятельства, имеющие значение для дела, и давать о них правильные показания;
- документы, имеющие значение для дела, но не удостоверенные юридическими и должностными лицами или гражданами;
- заключение некомпетентного эксперта;
- показания священнослужителя, если сведения получены им на исповеди;
- наличие свидетельского иммунитета⁵⁷.

Следует отметить, что при определенных условиях непроцессуальная негласная информация, полученная в ходе проведения электронного наблюдения, может быть преобразована в установ-

⁵⁵ Вольтер Ф. М. Философские сочинения / Пер. с франц. С. Я. Шейман-Топштейн; Под ред. В. Н. Кузнецова. М., 1988. С. 271.

⁵⁶ См.: Овчинский С. С. Значение уголовно-правовых и уголовно-процессуальных институтов для оперативно-розыскной деятельности в борьбе с организованной преступностью // Следователь. 1999. №9. С. 31.

⁵⁷ Здесь необходимо уточнение. Из вышеназванных источников может быть получена и процессуальная информация, но она является недопустимой как доказательство.

ленном законом порядке в процессуальную и гласную⁵⁸. Однако до того, как это произойдет, она не подлежит оглашению и не имеет доказательной силы.

Согласно ч. 1 ст. 11 Федерального закона «Об оперативно-розыскной деятельности» результаты оперативно-розыскной деятельности⁵⁹ могут быть использованы для подготовки и осуществления следственных и судебных действий, проведения оперативно-розыскных мероприятий по выявлению, предупреждению, пресечению и раскрытию преступлений, выявлению и установлению лиц, их подготавливающих, совершающих или совершивших, а также для розыска лиц, скрывающихся от органов дознания, следствия и суда, уклоняющихся от исполнения наказания и без вести пропавших. Предписания этой правовой нормы открывают широкие возможности для информационного обеспечения процесса доказывания по уголовным делам.

Формы использования процессуальной информации, полученной в ходе электронного наблюдения, наиболее разнообразны. Как и непроцессуальная информация, она может служить в этих случаях для ориентации следователя при выборе оптимальных и организационных решений. Вместе с тем, в отличие от непроцессуальной информации, она может быть положена в основу принятия планируемых мер процессуального принуждения по уголовному делу, использована в качестве доказательств при производстве следственных действий в тактических целях (например, путем предъявления доказательств при допросе).

Все непроцессуальные виды информации имеют более ограниченные возможности использования при расследовании. Их достоверность не проверена процессуальным путем, и это необходимо учитывать, имея в виду их исключительно ориентирующий характер.

⁵⁸ См. Приложение к приказу Федеральной службы налоговой полиции России, Федеральной службы безопасности России, Министерства внутренних дел России, Федеральной службы охраны России, Федеральной пограничной стражи России, Государственного таможенного комитета России, Службы внешней разведки России от 13 мая 1998 года №175/226/336/201/286/410/56 «Инструкция о порядке предоставления результатов оперативно-розыскной деятельности органу дознания, следователю, прокурору или в суд» // Бюл. норматив. актов федеральных органов исполнит. власти. 1998. № 23. С. 86—92.

⁵⁹ Включая и электронное наблюдение.

Гласная непроцессуальная информация может использоваться следователем относительно свободно: на нее нельзя ссылаться как на доказательство и предъявлять в качестве такового при допросе, но можно использовать для формулировки вопросов допрашиваемому, применения не противоречащих закону психологических «хитростей»⁶⁰.

Д. И. Бедняков по вопросу о возможности предъявления в ходе допроса предметов и документов, полученных оперативным путем, имеет иное мнение. Он утверждает, что в ходе допроса могут быть прямо использованы оперативные данные о характере преступления, его размерах, материальном положении допрашиваемого и т. д. Сложнее решается вопрос о предъявлении в ходе допроса предметов и документов, полученных оперативным путем. Ответ на него связан с теорией и практикой запретов использования в расследовании (в т. ч. и в ходе допросов) доказательств, полученных незаконными методами либо способами, процессуальный порядок которых однозначно в законе не урегулирован до сих пор. Представляется, что ознакомление допрашиваемого с полученными предметами и документами без объяснения их происхождения вполне допустимо⁶¹.

С мнением Д. И. Беднякова по данному вопросу, на мой взгляд, трудно согласиться, и позиция названных ранее авторов представляется более правильной.

Сложнее использовать информацию оперативно-розыскных служб, полученную из негласных источников или путем проведения электронного наблюдения, которые не подлежат разглашению. Здесь требуется особая осторожность. Формы реализации такой информации следователю и дознавателю желательно согласовать с руководителем органа, осуществляющего оперативно-розыскную деятельность, от которого эта информация поступила.

⁶⁰ См. например: *Рашинов А. П.* Судебная психология для следователей. М., 1967. С. 163—171; *Горский Г. Ф.* Судебная этика / Горский Г. Ф., Кокорев Л. Д., Котов Д. П. Воронеж, 1973; *Соловьев А. Б.* О психологических приемах допроса // Проблемы предварительного следствия в уголовном судопроизводстве. М., 1980. С. 63—81.

⁶¹ См. об этом: *Бедняков Д. И.* Непроцессуальная информация... С. 109.

Б. Т. Безлепкина выдвигает и обосновывает идею о том, что в определенных случаях в качестве судебного доказательства могут быть использованы добытые негласным путем материалы, источник которых по соображениям конспирации не может быть указан. По мнению ученого, это возможно при одном неперемennom условии: источник и способ получения соответствующего предмета и документа не имеют значения для оценки доказательства, относимости и допустимости информации, которую он несет⁶².

Это предложение на первый взгляд особенно актуально не только с правовых, но и с нравственных позиций, поскольку входит в противоречие с моральными постулатами вроде «суд должен знать все» и не может принимать в качестве источника доказательства материалы, происхождение которых «затемнено» и уводит в глубины негласной деятельности оперативно-розыскных служб. В действительности же здесь нет принципиальной нравственной коллизии. Суд не может знать все, он должен знать только то, что входит в рамки предмета доказывания. Если орган дознания, следователь, прокурор и суд по уголовному делу, находящемуся в производстве, используют свои полномочия и процессуальные средства для исследования обстоятельств, не входящих в предмет доказывания, эта деятельность не только бесполезна, но и вредна, т. к. загромождает уголовное дела излишней информацией.

Проблема, в сущности, сводится к вопросу о том, возможны и существуют ли в реальности такие ситуации, когда источник информации, полученной в результате негласного оперативно-технического мероприятия, полностью безразличен с точки зрения ее достоверности. Практика положительно отвечает на этот вопрос. Видеозапись, отображающая определенную сцену, действие и участников этого действия, в определенных случаях значима сама по себе, независимо от того, кто и при каких обстоятельствах ее произвел. То же самое можно сказать и в отношении фонограммы.

Проверка подобного доказательства (в частности, экспертным путем) должна касаться исключительно самой записи. Все остальные фактические обстоятельства лишены обязательного признака

⁶² Безлепкина Б. Т. Проблемы уголовно-процессуального доказывания // Сов. государство и право. 1991. № 8. С. 100.

доказательства — относимости, и муссировать их в уголовном процессе в подобных случаях можно разве только из любопытства⁶³.

По своему содержанию получаемая следователем от оперативно-розыскных служб ориентирующая информация подразделяется на две группы: 1) содержащая сведения об источниках доказательств по уголовному делу и 2) содержащая сведения об обстоятельствах, имеющих значение для правильной организации расследования и тактики производства следственных действий. В первом случае это сведения о лицах, показания которых могут иметь значение для выяснения подлежащих доказыванию обстоятельств, наличия и месте нахождения орудий преступления, сведения о похищенных ценностях и денежных средствах, предметах, носящих следы преступления, и т. д. Во втором — сведения о конфликтах в преступной группе, индивидуальных особенностях личности потерпевших, свидетелей, обвиняемых, их ценностной ориентации, характере взаимоотношений, другие обстоятельства, которые могут не входить в предмет доказывания по делу, но имеют большое значение для организации и планирования расследования, повышения результатов следственных действий и расследования в целом.

В случаях, когда орган, осуществляющий оперативно-розыскную деятельность, является одновременно и органом дознания по уголовным делам, требующим предварительного расследования, он вправе возбудить уголовное дело и произвести неотложные следственные действия на основании ориентирующей информации, содержащей сведения, достаточные для квалификации преступления (время, место, способ, ущерб, состав преступления, конкретные обстоятельства дела и т. д.).

Ориентирующая следствие информация может быть получена при производстве любых оперативно-розыскных мероприятий, в т. ч. и электронного наблюдения. При ее использовании во вспомогательных целях (не для формирования доказательств) важно не то, из каких источников и каким образом она получена, а ее содержание и степень достоверности, которая позволила бы избежать направления расследования по ложному пути, ненужной затраты сил и средств.

⁶³ См.: Безлепкина Б. Т. Проблемы уголовно-процессуального доказывания. С. 99.

Результаты электронного наблюдения на разных этапах предварительного расследования могут быть использованы по одному и тому же делу и как вспомогательная, не включенная в его материалы информация, и как непосредственный источник формирования доказательств. В качестве примера можно привести ситуацию, имевшую место по уголовному делу № 945802.

К., второй по иерархии человек в банде «А»⁶⁴, согласился дать показания. В ходе разговора с оперативным работником было проведено электронное наблюдение с использованием негласной аудиозаписи. К., по веским для него причинам, рассказал о деятельности банды, что было с успехом использовано в уголовном деле при выдвижении версий о времени, месте, способе совершения преступлений и участвовавших в них лицах при планировании расследования.

В ходе дальнейшего расследования по возбужденному уголовному делу К. отказался от данных им показаний, но представленная следователю фонограмма разговора (текст на 50 листах) в предусмотренном УПК РСФСР порядке была приобщена к уголовному делу в качестве вещественного доказательства⁶⁵.

Таким образом, проведение электронного наблюдения в данном случае существенно помогло в раскрытии целого ряда преступлений и направило расследование по истинному пути, позволив сэкономить большое количество людских и материальных ресурсов, а также предотвратить совершение новых противоправных деяний, спасло не одну человеческую жизнь. Суд учел данную фонограмму как вещественное доказательство и сделал ссылку на нее в приговоре.

Проведение электронного наблюдения наиболее актуально на первоначальном этапе расследования преступного деяния.

Термин «первоначальный этап расследования» используется в ряде криминалистических и уголовно-процессуальных работ, в т. ч. и в некоторых учебниках по криминалистике.

⁶⁴ Бандой «А» в период с 1992 по 1996 год на территориях Свердловской и Челябинской областей, других субъектов Российской Федерации, а также стран СНГ и Венгрии совершено более двух десятков умышленных убийств и других тяжких и особо тяжких преступлений (убийство Доронина в Москве, взрыв самолета в Венгрии и т. д.).

⁶⁵ По материалам уголовного дела № 945802 из архива Свердловского областного суда (1997).

Е. П. Ищенко определяет первоначальный этап как период начала расследования по уголовному делу, направленность которого зависит от следственной ситуации и криминалистической характеристики преступления, необходимый для установления обстоятельств преступления и лица, его совершившего⁶⁶. Длительность данного периода составляет не более 10 суток с момента обнаружения преступления⁶⁷.

А. Б. Соловьев дает следующее понятие названному этапу. По его мнению, к первоначальному этапу расследования относят, как правило, период от возбуждения уголовного дела до окончания производства неотложных следственных действий продолжительностью не более 10—15 суток. Несмотря на столь краткий период, его значение для выполнения задач уголовного судопроизводства трудно переоценить. Достаточно сказать, что от 70 до 80 % доказательств, приводимых в обвинительных заключениях следователей и приговорах судов, относятся к числу собранных именно в это время⁶⁸.

По нашему мнению, обе точки зрения являются правильными и не требуют каких-либо дополнений.

Специфика расследования преступлений на данном этапе характеризуется особенностями решаемых задач, и прежде всего — раскрытием их «по горячим следам», установлением и закреплении следов преступления, подверженных исчезновению и утрате, обнаружением и изъятием оружия, взрывчатых веществ, наркотиков, похищенного имущества и ценностей до того, как преступниками будут приняты меры к их сокрытию, реализации или уничтожению.

Исследования, проводившиеся на протяжении многих лет⁶⁹, убедительно подтверждают тот факт, что первоначальные показания потерпевших и свидетелей, в первую очередь очевидцев преступления, полученные в первые часы после происшествия, как правило, наиболее точно и правдиво отражают события, участника-

⁶⁶ См.: Ищенко Е. П. Проблемы первоначального этапа расследования преступлений. Красноярск, 1987. С. 9.

⁶⁷ См.: Там же. С. 7.

⁶⁸ См.: Соловьев А. Б. Следственные действия на первоначальном этапе расследования преступлений. М., 1994. С. 4.

⁶⁹ См., в частности: Корневский Ю. В., Токарева М. Е. Использование результатов оперативно-розыскной деятельности в доказывании по уголовным делам: Метод. пособие. М., 2000.

ми или свидетелями которых им пришлось быть. Позднее многие важные детали могут стереться в памяти, а показания о них исказиться в результате собственных домыслов допрашиваемых, а также под воздействием уговоров, угроз, подкупа со стороны заинтересованных лиц, а порой — просто из нежелания участвовать в уголовном процессе.

Обнаружению и успешному сбору доказательств на первоначальном этапе способствует получение правдивых показаний подозреваемых. Однако их результативный допрос требует тщательной подготовки и во многом зависит от наличия у следователя ориентирующей информации об обстоятельствах совершенного преступления и его участниках.

8 сентября 1996 года прокуратурой Волгодонска было возбуждено уголовное дело по факту исчезновения Д. А. Филимонова. В тот же день местными подразделениями управления по борьбе с организованной преступностью была получена и представлена прокурору информация о причастности к исчезновению Д. А. Филимонова трех жителей города. С помощью проведенного оперативным подразделением электронного наблюдения довольно быстро удалось установить местонахождение этих лиц. Оперативным путем была получена также информация об их связях, образе жизни и пр. Умелая тактика их допросов, осуществлявшихся в условиях внезапного вызова каждого, исключения возможности взаимных контактов, сопровождавшихся демонстрацией осведомленности следователя об обстоятельствах совершенных преступлений без указания источников получения информации, а также применение других тактических приемов с использованием ориентирующих данных оперативно-розыскной деятельности и противоречий в показаниях допрашиваемых позволили не только установить факт убийства Филимонова, участвовавших в его совершении лиц, место сокрытия трупа, но раскрыть и другие преступления банды, к которой, как выяснилось из полученных показаний, принадлежали допрошенные⁷⁰.

По результатам электронного наблюдения нередко сразу после возбуждения уголовного дела удается осуществить задержание подозреваемых. Наличие ориентирующей информации особенно

⁷⁰ Цит. по: *Корневский Ю. В., Токарева М. Е.* Использование результатов оперативно-розыскной деятельности... С. 45—46.

важно, т. к. она позволяет заранее определить тактику как самого задержания (количество лиц, планируемых для задержания, наличие у них оружия и взрывчатых веществ, их планов и т. п.), так и неотложных следственных действий (обыск, выемка).

Так, летом 1998 года в Екатеринбурге около жилого дома по улице Ферганской при задержании боевиков одной из преступных групп по подозрению в совершении ими тяжких и особо тяжких преступлений ориентирующая информация, полученная в ходе проведения электронного наблюдения, позволила спасти не одну человеческую жизнь. Спецподразделению было известно о количестве бандитов, наличии у них двух гранат типа Ф-1, огнестрельного оружия, их намерении оказать сопротивление и о пути планируемого отхода. При захвате преступники были поставлены в невыгодные для них условия и при приращении одним из них гранаты нанесли ранения себе, а не группе сотрудников правоприменительных органов⁷¹.

В качестве примера можно привести также захват заложников в следственном изоляторе Екатеринбурга летом 1994 года. Без ориентирующей информации, полученной спецподразделениями Управления Федеральной службы безопасности по Свердловской области в ходе проведения электронного наблюдения (количество преступников, наличие у них оружия, их планы и возможные связи на территории следственного изолятора и вне его, число заложников и их место нахождения), трудно было бы держать ситуацию под контролем и успешно локализовать ее без человеческих жертв.

В деятельности оперативно-розыскных подразделений с первых часов задержания подозреваемых и взятия под стражу обвиняемых проводятся такие оперативно-розыскные мероприятия, как наблюдение и оперативное внедрение, результаты которых позволяют в ряде случаев получить полезную для следствия информацию⁷². Это сведения о неизвестных соучастниках и эпизодах преступной деятельности, местах возможного нахождения скрывшихся от следствия и суда лиц, местах сокрытия жертв преступлений, транспортных средств, оружия и т. д.

⁷¹ Данные получены в одном из органов дознания Свердловской области.

⁷² См.: *Жук О. Д.* Организованная преступность в современной России: Раскрытие и расследование преступлений, совершаемых организованными преступными формированиями. Томск, 1998. С. 149, 169.

Обобщение писем прокуроров субъектов Российской Федерации позволяет сделать вывод о том, что ориентирующая информация оперативно-розыскных служб по многим уголовным делам об убийствах и других особо тяжких преступлениях помогла своевременно, по горячим следам установить причастных к ним лиц и произвести обыски, выемки не только по месту жительства подозреваемых и обвиняемых, но в других местах, получив при этом важные вещественные доказательства⁷³.

В качестве основания для обыска у подозреваемого или обвиняемого достаточно самого факта процессуального положения этих лиц. Обыск в жилых или иных помещениях физических и юридических лиц требует специального обоснования материалами уголовного дела. Поэтому необходимо, чтобы оперативно-розыскные подразделения в письменном виде представляли результаты электронного наблюдения и других оперативно-розыскных мероприятий, дающих основания предполагать нахождение интересующих следствии предметов, ценностей, документов в каком-то конкретном месте. Как правило, в качестве такого документа выступает рапорт оперативного работника, подписанный руководителем уполномоченного на то органа или оперативно-розыскного подразделения.

В процессе дальнейшего расследования обычно решается вопрос о предъявлении обвинения, избрании меры пресечения, дальнейшем собирании и проверке доказательств, изобличающих виновных, и с большей остротой встает проблема выполнения требований уголовно-процессуального закона о всесторонности, полноте, объективности исследования обстоятельств, подлежащих доказыванию по уголовному делу⁷⁴.

По делам о многоэпизодных и групповых преступлениях это означает, в частности, выявление всех эпизодов преступной деятельности лица или лиц, участвовавших в преступлении или преступлениях.

⁷³ Корневский Ю. В., Токарева М. Е. Использование результатов оперативно-розыскной деятельности... С. 51.

⁷⁴ См.: Соловьев А. Б. Прокурорский надзор за всесторонностью, полнотой и объективностью расследования преступлений / Соловьев А. Б., Багатулин Ф. Н., Филиппов М. Н. М., 1996.

Без использования ориентирующей информации оперативно-розыскных подразделений в отношении сложных по доказыванию преступлений работа следователя часто оказывается недостаточно целеустремленной, эффективной, а то и вовсе безрезультатной. В то же время практика совместной деятельности следователей и работников дознания на протяжении всего периода расследования вплоть до его окончания в рамках следственно-оперативных групп дает хорошие результаты.

Так, благодаря профессионально налаженному взаимодействию следователей и работников оперативно-розыскных служб при проведении электронного наблюдения и других оперативно-розыскных и следственных действий была раскрыта и изобличена преступная деятельность лидеров центральной преступной группировки (Вагин, Сивков, Фокин, Оганесян, Филатов, Портнягин, Муранов и др.), банд Терентьева-Курдюмова, братьев Коротковых, Трифона-Овчины, Зимина, дело «Новой гильдии» и мн. др.

Среди основных направлений взаимодействия следователя с органами, осуществляющими оперативно-розыскную деятельность после окончания первоначального этапа расследования, необходимо отметить следующие:

- с помощью проведения электронного наблюдения продолжалась работа по установлению лиц, совершивших преступление, если таковые не были установлены или установлены не полностью;
- проверялись версии о не установленных следствием эпизодах преступной деятельности лиц, привлеченных по уголовному делу в качестве подозреваемых и обвиняемых;
- была получена ориентирующая информация о недостаточно исследованных по делу обстоятельствах, подлежащих доказыванию, и возможных источниках собирания доказательств, в т. ч. касающихся индивидуализации мотивов совершения групповых преступлений, распределения ролей в преступной группе, характера и размера причиненного преступлением ущерба, мест укрытия жертв преступления, хранения наркотиков, оружия, похищенного имущества и ценностей, установления каналов их сбыта;
- проверка защитных версий подозреваемого, обвиняемого, их защитников;

- получение ориентирующей информации о личностях подозреваемых, обвиняемых, других участников уголовного процесса, а также об иных обстоятельствах, которые могут быть использованы для оптимальной организации и планирования расследования, подготовки и правильного выбора тактики производства допросов и других следственных действий;

- получение ориентирующей информации о планируемых и реализуемых преступниками способах сокрытия следов преступления и противодействия следствию⁷⁵.

Кроме того, из материалов уголовных дел об особо тяжких преступлениях, прежде всего преступлениях организованных преступных сообществ, видно, что подозреваемые, обвиняемые, а также потерпевшие и свидетели нередко, а порой неоднократно меняют свои показания на предварительном следствии и в суде, объясняя это различными, порой мало убедительными причинами. Для правильного выбора тактики повторных допросов таких лиц, разоблачения их ложных показаний и установления истины по уголовному делу следователю важно получить хотя бы непроцессуальную информацию о фактических обстоятельствах и причинах, побудивших лицо менять свою позицию на следствии. А получение вышеназванной ориентирующей и непроцессуальной информации возможно, как правило, только при проведении электронного наблюдения.

Прав Д. И. Бедняков утверждающий, что «процессуальная деятельность без применения непроцессуальных методов была бы невозможной, а непроцессуальная деятельность без последующего использования ее результатов в уголовном процессе — бесцельной»⁷⁶.

Особо следует остановиться на использовании результатов электронного наблюдения по приостановленным уголовным делам. Следственные действия по ним согласно УПК РФ не производятся. Однако оперативно-розыскные мероприятия, и в т. ч. электронное наблюдение, по поручению следователя и с целью розыска скрывшихся преступников, установления их местопребывания, а также

выявления лиц, подлежащих привлечению в качестве обвиняемых, продолжают осуществляться.

В качестве примера можно назвать проведение электронного наблюдения в отношении Сергея Курдюмова, находящегося в розыске и по сей день. Лидер «криминального уралмашевского спецназа» все равно будет задержан и предстанет перед судом за неоднократные убийства на территории г. Екатеринбурга и Венгрии. Уголовное дело в отношении С. Курдюмова выделено в отдельное производство и приостановлено, но электронное наблюдение (по поручению следователя) будет продолжаться вплоть до его ареста⁷⁷.

Своевременное проведение электронного наблюдения позволило в достаточно короткий срок выявить местонахождение и произвести задержание Терентьева. По звонку, поступившему на квартиру сожительницы Терентьева (в Екатеринбурге), сотрудниками спецслужб был определен номер телефона, с которого поступил звонок (Н. Новгород), и его адрес установки. Данная информация была сразу передана в Н. Новгород, где Терентьев и был задержан⁷⁸.

Правовой основой ввода результатов электронного наблюдения в уголовный процесс служат положения УПК РФ и оперативно-розыскного законодательства России.

Использование названных результатов для подготовки и осуществления следственных действий сложностей в ряде случаев не вызывает, а вот при реализации данных результатов в качестве доказательств по уголовным делам возникают значительные трудности.

Затруднения созданы неопределенным подходом законодателя к правовому регулированию такой относительно самостоятельной части процесса доказывания, как собирание доказательств. Он устанавливает, что доказательства могут собираться только путем производства предусмотренных Кодексом следственных и иных процессуальных действий. Но, с другой стороны, тот же закон допускает возможность представления доказательств в виде письменных документов и предметов подозреваемым, обвиняемым, потерпевшим,

⁷⁵ Корневский Ю. В., Токарева М. Е. Использование результатов оперативно-розыскной деятельности... С. 54—55.

⁷⁶ Бедняков Д. И. Непроцессуальная информация... С. 77.

⁷⁷ См.: Приоткрыв завесу секретности: К 85-летию образования Управления Федеральной службы безопасности России по Свердловской области. Екатеринбург. 2003. С. 127—140.

⁷⁸ Данные получены в одном из органов дознания Свердловской области.

гражданским истцом, гражданским ответчиком и их представителями. Кроме того, согласно ст. 86 УПК РФ защитник также вправе собирать доказательства путем получения предметов, документов и иных сведений, опроса лиц с их согласия, а также истребования справок, характеристик, иных документов от органов государственной власти и местного самоуправления, общественных объединений и организаций. Другими словами, в первом случае законодатель исходит из возможности формирования доказательств только в процессе производства следственных и судебных действий, во втором он допускает их существование в готовом виде и вне уголовного процесса. Если попытаться проанализировать ст. 70 УПК РСФСР и ст. 86 УПК РФ («Собирание доказательств»), то в буквальном смысле это выражение нужно трактовать так, что выше-названные участники уголовного судопроизводства посредством перечисленных действий собирают полноценные доказательства. Между тем в действительности ситуация складывается в принципе иначе. Даже полученным в ходе выполнения следственных действий фактическим данным и их источникам нельзя придать статус доказательства. Тем более преждевременно называть доказательствами то, что получено иными процессуальными способами. Прежде чем рассматривать полученное в этом качестве и оперировать им как доказательствами, необходимо его оценить на предмет соответствия требованиям закона, и не только в целом, но и каждый его элемент в отдельности. Для этого, очевидно, может потребоваться не только их изучение, но и проведение проверочных действий, в т. ч. следственных. Например, лицо, пострадавшее от преступного посягательства, подлежит освидетельствованию, а в случае необходимости проводится судебно-медицинская экспертиза (несмотря на возможное наличие медицинских документов, выданных, например, лечащим врачом). И только после этого полученные данные приобщаются к делу в качестве доказательств.

Таким образом, хотя закон и говорит о собирании уже «готовых» доказательств, но, как справедливо пишет А. Р. Белкин, «...по тексту ст. 70 УПК РСФСР представляется, что речь идет о “будущих” доказательствах (т. е. об информации, которая потенциально может иметь доказательственное значение)»⁷⁹. Следовательно, в этой ста-

⁷⁹ Белкин А. Р. Теория доказывания. М., 1999. С. 38—39.

тье УПК говорится о собирании фактических данных и их источников, но еще не доказательств, хотя они становятся таковыми после их надлежащей проверки и закрепления. Данные условности имеют место, и не говорить о них нельзя.

Из изложенного вытекает, что название анализируемых статей не совсем точно отражает их содержание. Поэтому можно было бы озаглавить рассматриваемые статьи как «Собирание фактических данных (или фактической информации) и их (ее) источников». В данном контексте рассматривает названную проблему и В. С. Балакшин⁸⁰.

Под собиранием фактической информации и ее источников следует понимать уголовно-процессуальную деятельность уполномоченных органов и должностных лиц по выявлению, отысканию, обнаружению и получению названной информации и ее источников с целью установления обстоятельств, имеющих значение для правильного разрешения уголовного дела.

Отдельные ученые толкуют понятие «собирание» расширительно, включая в него выявление, закрепление (фиксацию), изъятие и сохранение⁸¹. А. М. Ларин, Л. Д. Кокорев и другие авторы наряду с обнаружением и закреплением включают в собирание доказательств в качестве процессуального элемента их розыск⁸², а С. А. Шейфер — еще и правообеспечительные операции⁸³. По нашему мнению, при формировании указанного понятия нужно исходить из требований уголовно-процессуального закона, а также из необходимости рассматривать закрепление фактической информации в качестве самостоятельного элемента процесса доказывания по уголовному делу.

⁸⁰ Балакшин В. С. Доказательства в российском уголовном процессе... С. 70—75.

⁸¹ См., например: Винберг А. И. Криминалистика: Введение в криминалистику. Вып. 1. М., 1950. С. 8; Белкин Р. С. Собирание, исследование и оценка доказательств: Сущность и методы. М., 1966. С. 44—53; Он же. Криминалистика: проблемы, тенденции, перспективы: Общие и частные теории. М., 1987. С. 217—218.

⁸² См.: Ларин А. М. Работа следователя с доказательствами. М., 1966. С. 43—66; Горских Г. Ф. Проблемы доказательств в советском уголовном процессе / Горских Г. Ф., Кокорев Л. Д., Элькин П. С. Воронеж, 1978. С. 211.

⁸³ См.: Шейфер С. А. Собирание доказательств в советском уголовном процессе: методологические и правовые проблемы. Саратов, 1986. С. 41—42.

Интересно, что ст. 89 УПК РФ «Использование в доказывании результатов оперативно-розыскной деятельности» изложена в редакции, полярной ее наименованию: «В процессе доказывания запрещается использование результатов оперативно-розыскной деятельности, если они не отвечают требованиям, предъявляемым к доказательствам настоящим Кодексом». В таком виде эта норма по существу любые материалы, полученные в ходе проведения электронного наблюдения и других оперативно-розыскных мероприятий, обрекает на признание недопустимыми и на исключение из материалов уголовного дела. Причины следующие: 1) получение материалов оперативно-розыскной деятельности за рамками уголовного процесса и не уполномоченными на выполнение следственных и иных процессуальных действий должностными лицами; 2) фиксация сведений вне предусмотренных уголовно-процессуальным законом источников; 3) несоблюдение предусмотренного УПК РФ порядка и способов собирания и закрепления фактической информации, значимой для уголовного дела.

Здесь более приемлемой была бы норма, предлагавшаяся в ст. 85 одного из проектов УПК РФ (хотя и ее нельзя признать удачной): «Результаты оперативно-розыскной деятельности, полученные при соблюдении требований Федерального закона “Об оперативно-розыскной деятельности”, могут использоваться в доказывании по уголовным делам в соответствии с положениями настоящего Кодекса, регламентирующего собирание, проверку и оценку доказательств».

Какие возражения могли возникнуть у законодателя при рассмотрении названного проекта УПК РФ и указанной нормы в частности? На наш взгляд, это вопрос о том, что необходимо понимать под «результатами оперативно-розыскной деятельности»: фактическую информацию или материалы, полученные в ходе ее проведения, либо и то и другое вместе? Кроме того, вызывает сомнение стилистическая выверенность первой части текста статьи. Как понимать фразу «...полученные при соблюдении требований Федерального закона “Об оперативно-розыскной деятельности”»? Следуя смыслу приведенного словосочетания, можно сделать следующие выводы, негативные для уголовного процесса:

— оперативно-розыскная деятельность может осуществляться и за рамками требований федерального закона;

— как обоснованно указала П. А. Лупинская, формулировка закона «...может дать основания для вывода, что оперативные материалы уже с момента их представления должны рассматриваться как доказательства»⁸⁴ — подобное толкование было чревато появлением на практике фактов фальсификации доказательств.

Довольно широкое распространение среди ученых-процессуалистов получило представление о том, что сведения, полученные в ходе электронного наблюдения, могут стать содержанием доказательств по уголовному делу. Так, по мнению В. И. Зажицкого, «...фактические данные, полученные оперативно-розыскным путем, могут стать содержанием доказательств по уголовному делу при строгом выполнении соответствующих требований уголовно-процессуального закона»⁸⁵. Правда, в дальнейшем он изменил свою позицию в данном вопросе и пришел к выводу о том, что при осуществлении оперативно-розыскной деятельности обнаруживаются не доказательства, а следы преступления, которые могут стать содержанием доказательств, если войдут в уголовный процесс посредством законных источников и законными способами⁸⁶. Аналогичной точки зрения по данному вопросу придерживаются и некоторые другие авторы⁸⁷.

Противоречивую позицию в данном вопросе занимает Г. М. Миньковский, считающий, что фактические данные (сведения), полученные путем производства оперативно-розыскных мероприятий, могут быть признаны доказательствами по уголовным делам, но только лишь в том случае, если они собраны, проверены и оценены в соответствии с требованиями уголовно-процессуального законодательства⁸⁸.

⁸⁴ Лупинская П. А. Проблемы допустимости доказательств при рассмотрении дел судом присяжных // Рассмотрение дел судом присяжных. Варшава, 1997. С. 117.

⁸⁵ Зажицкий В. И. Правовая регламентация деятельности по обнаружению признаков преступления // Правоведение. 1992. № 4. С. 104.

⁸⁶ Зажицкий В. И. Закон об оперативно-розыскной деятельности не идеален // Сов. юстиция. 1993. № 5. С. 20.

⁸⁷ См.: Бедняков Д. И. Непроцессуальная информация... С. 67; Лупинская П. А. Основания и порядок принятия решений о недопустимости доказательств // Рос. юстиция. 1994. № 11. С. 3; Китнис Н. М. Допустимость доказательств в уголовном судопроизводстве. М., 1995. С. 9; Кокорев Л. Д., Кузнецов Н. П. Уголовный процесс: доказательства и доказывание. Воронеж, 1995. С. 164.

⁸⁸ Комментарий к УПК РСФСР М., 1995. С. 111.

Правильным на данный момент является мнение Е. А. Доля, что результаты оперативно-розыскной деятельности не могут быть собраны по правилам уголовно-процессуального законодательства. Их формирование осуществляется согласно требованиям оперативно-розыскного законодательства. В уголовном процессе собираются, проверяются и оцениваются не результаты оперативно-розыскной деятельности, а уголовно-процессуальные доказательства⁸⁹.

Результаты электронного наблюдения, связанные в силу объективных причин с образующимися (образовавшимися) обстоятельствами предмета доказывания и побочными фактами, правомерно использовать в уголовном процессе, но не в качестве доказательств. Они могут и должны служить основой для формирования последних.

Несмотря на то, что содержание формируемых в уголовном процессе доказательств могут составлять сведения о тех же фактах и обстоятельствах, которые уже нашли отражение в результатах электронного наблюдения, это не причина для отождествления названных результатов с доказательствами.

Отображение средствами и методами, присущими оперативно-розыскной и соответственно уголовно-процессуальной деятельности одного и того же, но часто изменяющегося факта (обстоятельства, явления), не дает оснований как для отождествления, так и для смешения получаемых при этом результатов, фактической информации — оперативных доказательств и доказательств в уголовно-процессуальном смысле. Их формирование происходит в условиях различных видов деятельности с присущими каждому из них правовыми требованиями к содержанию и форме получаемых сведений, принципами и методами деятельности, системами гарантий соблюдения прав и законных интересов граждан.

В доказывании используются не те фактические данные, которые были добыты в результате электронного наблюдения в ходе оперативно-розыскной деятельности, а иные фактические данные, полученные в рамках уголовно-процессуальной деятельности при формировании доказательств. Вот они-то и образуют содержание доказательств в уголовном процессе.

⁸⁹ Доля Е. А. Новая Конституция и уголовно-процессуальная деятельность // Рос. юстиция. 1994. № 4. С. 19.

В пользу такого вывода свидетельствует и факт получения указанных данных в совершенно разных пространственно-временных условиях со всеми вытекающими из этого последствиями — применением для их формирования и последующего использования различных правовых режимов. Хотя в отдельных случаях данные пространственно-временные условия бывают едва различимы.

В качестве примера можно привести похищение малолетнего Д. Н. Вершинина. Ребенок был похищен 7 марта 2004 года. Участники преступной группы требовали от родителей похищенного 500 тысяч долларов США, в противном случае угрожая убийством их сына.

Учитывая особую общественную опасность совершенного преступления, руководство ГУВД обратилось в Управление Федеральной службы безопасности России по Свердловской области с просьбой оказать содействие в проведении оперативно-розыскных и оперативно-технических мероприятий по установлению участников организованной преступной группы и освобождению мальчика, в связи с чем была создана объединенная оперативно-следственная группа.

В течение пяти дней неизвестные периодически звонили родителям похищенного и торопили их с выплатой выкупа, воспроизводя аудиозапись голоса ребенка. В указанный период времени в ходе проведения оперативно-розыскных мероприятий на основе анализа информации, полученной в ходе проведения электронного наблюдения за переговорами похитителей, были установлены лица, возможно причастные к похищению Д. Н. Вершинина. Выявлены и взяты под электронное наблюдение все имеющиеся средства связи подозреваемых. Определен сектор местности, с которого велись телефонные переговоры, как наиболее вероятное место содержания мальчика — один из автомобильных боксов гаражно-строительного кооператива «Южный» г. Екатеринбурга.

В ночь на 15 марта 2004 года в результате спецоперации ребенок был освобожден. В результате проведения электронного наблюдения были установлены четыре участника преступления, три из которых задержаны. Проведенными обысками изъяты наркотические средства и газовый пистолет, переделанный под стрельбу боевыми патронами. Задержанными лицами даны признательные показания.

Все материалы, полученные в ходе проведения электронного наблюдения, были приобщены к уголовному делу в качестве дока-

зательств⁹⁰. В данном случае проведение комплексного оперативно-технического мероприятия позволило выявить круг лиц, причастных к совершению преступления, а также место, время и способ его совершения, в максимально короткие сроки установить местонахождение заложника и освободить его без риска для его жизни и жизни сотрудников правоприменительных органов.

Вполне очевидно, что проверить соблюдение требований закона при проведении электронного наблюдения и других оперативно-розыскных мероприятий достаточно сложно. Как мы уже упоминали, большинство из них проводятся в условиях конспирации.

Сомнения в допустимости использования результатов электронного наблюдения возникли, например, при рассмотрении дела в отношении Фокина. Краснодарский краевой суд с участием присяжных заседателей исключил из числа доказательств результаты оперативно-розыскной деятельности, полученные до возбуждения уголовного дела, сославшись на ст. 119 УПК РСФСР. Президиум Верховного суда РФ отменил приговор по делу, указав, что согласно ст. 7 и ст. 11 Федерального закона «Об оперативно-розыскной деятельности» оперативно-розыскная деятельность может проводиться и до возбуждения уголовного дела, а результаты ее могут служить поводом и основанием для возбуждения уголовного дела и, кроме того, доказательством⁹¹.

Однако считать проблему исчерпавшей себя исходя из состоявшегося решения по указанному делу нельзя. На наш взгляд, правоотношения, возникающие в процессе рассмотрения вопросов о признании материалов оперативно-розыскной деятельности доказательствами по уголовному делу, являются уголовно-процессуальными и, следовательно, должны регламентироваться нормами уголовно-процессуального закона. Кроме того, нельзя оставить без внимания принципиальную позицию, содержащуюся в Концепции судебной реформы, согласно которой «...результаты опросов, розыска и негласного наблюдения доказательственного значения

⁹⁰ Из материалов уголовного дела № 1301 (прокуратура Ленинского района г. Екатеринбург, 2004).

⁹¹ См.: *Золотых В. В.* Проверка допустимости доказательств в уголовном процессе. М.; Ростов н/Д, 1999. С. 87—88.

не имеют»⁹². В юридической литературе также высказываются различные мнения по поводу процессуально-правовой природы видео- и аудиозаписи. Одни авторы считают их приложениями к протоколу следственного действия, которые не имеют самостоятельного доказательственного значения⁹³, другие полагают, что эти материалы становятся самостоятельным доказательством после того, как их в установленном порядке «ввели» в уголовный процесс, и рассматривают их как и н о й документ⁹⁴.

На позиции признания за результатами оперативно-розыскной деятельности статуса уголовно-процессуальных доказательств стоит и Н. П. Кузнецов, полагающий, что фактические данные, полученные непроцессуальным путем, сами по себе не являются доказательствами, но они могут приобрести такое качество в случае их получения следователем и судом законными способами (представление, истребование, производство следственного действия) и должного процессуального закрепления⁹⁵.

Следует подчеркнуть, что в процессе представления, истребования, производства следственных действий, о которых пишет Н. П. Кузнецов, получают не оперативные данные, а формируются процессуальные доказательства (однако объем оперативной, а в дальнейшем и процессуальной информации может и совпадать). По этой причине нельзя рассматривать в качестве вполне допустимого способа придания сведениям, полученных непроцессуальным путем, доказательственного значения и допрос в качестве свидетеля оперативного работника об обстоятельствах производства того или иного оперативного действия (например, проверочной закупки, наблюдения).

В этих ситуациях допрос оперативного работника в качестве свидетеля допустим, а в ряде случаев просто необходим, но содер-

⁹² Концепция судебной реформы в Российской Федерации. М., 1992. С. 93.

⁹³ См.: *Зинченко И. А.* Использование в уголовно-процессуальном доказывании фотоснимков, кинолент и видеограмм. Ташкент, 1988. С. 25; *Семенов В. А.* Следственные действия: Учеб. пособие. Екатеринбург, 2003. С. 66.

⁹⁴ См.: *Ищенко Е. П.* Использование современных научно-технических средств при расследовании уголовных дел. Свердловск, 1985. С. 15.

⁹⁵ *Кокорев Л. Д., Кузнецов Н. П.* Уголовный процесс: доказательства и доказывание. Воронеж, 1995. С. 164.

жание свидетельских показаний в данном случае образуют не те оперативные сведения (данные), которые были сформированы в условиях производства таких оперативно-розыскных мероприятий, как проверочная закупка, электронное наблюдение, а иные сведения — те, которые были получены в ходе допроса оперативного работника в качестве свидетеля.

Приведем в качестве примера электронное наблюдение за членами банды братьев Коротковых на вещевом рынке «Таганский ряд» г. Екатеринбурга. Преступники вымогали деньги у предпринимателей. Когда, не получив желаемой суммы денег, один из братьев Коротковых достал пистолет с глушителем и открыл огонь на поражение по одному из торговцев, сотрудникам правоприменительных органов ничего не оставалось делать, как произвести меры по задержанию. Бандитами, кроме огнестрельного оружия была использована также граната. Три оперативных работника ГУВД Свердловской области получили ранения средней тяжести. Впоследствии все работники, участвовавшие в задержании, были допрошены следователем, а затем и судом. Их показания послужили доказательствами по уголовному делу⁹⁶.

Таким образом, было предотвращено особо тяжкое преступление и возможная гибель ни в чем не повинных людей. Факт преступления был задокументирован, соучастники задержаны на месте преступления.

Принимая во внимания сложность разграничения содержания оперативных данных, полученных в ходе электронного наблюдения, и процессуальных доказательств, остановимся на этом несколько подробнее.

Применительно к показаниям свидетеля их содержание образуют не те сведения (хотя и имеющие значения для уголовного дела), которые лицо сообщило органам, осуществляющим оперативно-розыскную деятельность, в процессе содействия им на конфиденциальной основе, а иные данные, содержащиеся в устном сообщении этого лица, полученном на допросе. Для формирования относимых к уголовному делу и допустимых показаний свидетеля, соблюдения при этом прав и законных интересов граждан будет иметь значение

⁹⁶ По материалам уголовного дела № 34805 из архива Железнодорожного суда г. Екатеринбурга (1998).

учет всей правовой регламентации допроса как способа собирания данного вида доказательств — начиная с соблюдения оснований допроса, правил вызова свидетеля, обеспечения его правового статуса, обязанности и пределов использования приемов познания и заканчивая выполнением требований, предъявляемых к оформлению протокола допроса (УПК РФ, ст. 79, 187—191, 278).

Аналогичное положение будет иметь место при оформлении такого вида доказательств, как протоколы следственных и судебных действий (УПК РФ, ст. 83). При производстве, например, таких следственных действий, как осмотр, обыск, предъявление для опознания, следственный эксперимент, выемка, контроль и запись переговоров, их участниками могут непосредственно восприниматься те же обстоятельства и факты (или их часть), которые уже ранее воспринимались в ходе проведения оперативно-розыскных мероприятий по проверочным закупкам, наблюдению, обследованию помещений, зданий, сооружений, участков местности и транспортных средств, контролю почтовых отправлений, телеграфных и иных сообщений, прослушиванию телефонных переговоров, контролируемым поставкам (Федеральный закон «Об оперативно-розыскной деятельности», ст. 6, ч. 1, п. 4, 6, 8—10, 13). Но содержание протоколов названных следственных действий образуют не те сведения, которые были получены в результате восприятия участниками указанных оперативно-розыскных мероприятий фактов и обстоятельств, имеющих значение для уголовного дела, а фактические данные, сформированные субъектами следственных действий в ходе непосредственного восприятия ими указанных обстоятельств и фактов при условии, что они сохранились на момент производства соответствующего процессуального действия.

Точно так же содержание заключения эксперта в уголовном процессе образует выводное знание, полученное с применением специальных познаний на основе проведенного им исследования предметов и документов, имеющих значение для уголовного дела, осуществленное при условиях и в порядке, предусмотренном для проведения экспертизы (УПК РФ, ст. 80, 195—207), а не выводы, к которым пришел специалист в ходе выполнения такого оперативно-розыскного мероприятия, как исследование предметов и доку-

ментов (Федеральный закон «Об оперативно-розыскной деятельности», ст. 6, ч. 1, п. 5).

Таким образом, только полученные в установленном законом порядке доказательства, а не результаты оперативно-розыскной деятельности должны подвергаться проверке в соответствии с уголовно-процессуальным законом и использоваться в процессе оценки доказательств.

В зависимости от особенностей отражения в результатах оперативно-розыскной деятельности обстоятельств и фактов, имеющих значение для дела, они могут входить в уголовный процесс и использоваться в доказывании согласно процессуальным режимам, предъявляемым к соответствующим видам доказательств.

Отметим еще раз, что на основе полученных оперативным путем данных формируются такие виды доказательств, как показания (свидетелей, потерпевших, реже — подозреваемых и обвиняемых), вещественные доказательства, иные документы, протоколы следственных действий и судебного заседания. Названные виды доказательств могут быть получены в условиях производства таких следственных (судебных) действий, как допрос, осмотр, обыск, выемка, назначение и производство экспертизы, освидетельствование, контроль и запись переговоров.

Наведение справок представляет собой получение необходимых для дела данных от предприятий, учреждений, организаций, органов государственной власти или местного самоуправления, а также от граждан. Это официальное действие, и полученные таким образом документы могут быть без каких-либо препятствий приобщены к делу.

Что касается других оперативно-розыскных мероприятий, указанных в ст. 6 Федерального закона «Об оперативно-розыскной деятельности», то в первую очередь следует рассмотреть те из них, которые более распространены на практике и при введении результатов которых в уголовный процесс возникают трудности.

Как свидетельствует практика, чаще всего в доказывании по уголовным делам используются результаты оперативно-розыскной деятельности, полученные при проведении оперативно-розыскных мероприятий по прослушиванию телефонных перегово-

ров. Об этом свидетельствуют и многочисленные публикации на эту тему⁹⁷. В меньшей мере в доказывании используются результаты оперативно-розыскной деятельности, сформированные в ходе проведения оперативно-розыскных мероприятий с применением видеозаписи: наблюдение, оперативный эксперимент, контролируемая поставка, обследование зданий, помещений (оперативный досмотр), сооружений, участков местности и транспортных средств. Учитывая, что фонограммы телефонных и иных переговоров и видеозаписи могут при определенных условиях быть использованы для формирования одних и тех же видов доказательств, рассмотрим ввод в уголовный процесс только видеозаписи.

В и д е о з а п и с ь с запечатленными на ней фактами и обстоятельствами, имеющими значение для уголовного дела, снятая при проведении оперативно-розыскного мероприятия, может на предварительном следствии и в суде послужить основой для формирования вещественного доказательства при соблюдении следующих условий. Видеозапись должна быть официально представлена органом, уполномоченным на ведение оперативно-розыскной деятельности, с соответствующим препроводительным документом. В нем должны быть отражены сведения о происхождении видеозаписи: времени, месте, условиях и обстоятельствах ее получения, технических характеристиках применяемой аппаратуры, лице, осуществившем видеозапись⁹⁸.

Отличительные характеристики видеозаписи, относимые к уголовному делу, ее свойства и состояние должны быть восприняты органами чувств следователя и понятых (судей, других участников

⁹⁷ См., например: *Данилюк С.* Как прослушать телефонный разговор / Данилюк С., Виноградов С., Щерба С. // Социалист. законность. 1991. № 2. С. 32—33; *Комлев В.* О порядке прослушивания телефонных переговоров // ??? 1991. № 7. С. 54—55; *Козусев А.* Законность прослушивания телефонных переговоров // Законность. 1993. № 2. С. 9—11; *Козырев Г.* Документирование прослушивания и звукозапись телефонных и иных переговоров // Законность. 1993. № 4. С. 32—36.

⁹⁸ На такие носители информации как на доказательства обвинения ссылается в своей практике высший орган правосудия нашего государства — см.: Определение Судебной коллегии по уголовным делам Верховного суда РФ от 9 декабря 1993 года и от 17 ноября 1994 года // Бюл. Верховного суда РФ. 1994. № 11. С. 47; 1995. № 5. С. 49.

процесса) в ходе ее осмотра с применением соответствующих технических средств, привлечением необходимых специалистов в условиях производства такого следственного, судебного действия, как осмотр, и надлежащим образом зафиксированы в протоколе. О признании указанных свойств и состояния видеозаписи содержанием вещественного доказательства и его приобщении к уголовному делу необходимо вынести постановление (определение), в соответствии с которым в уголовном деле устанавливается надлежащий правовой режим обращения с данным доказательством — обеспечение условия сохранения видеозаписи в неизменном виде (она хранится при деле).

Таким образом, результаты оперативно-розыскной деятельности, связанные с указанной видеозаписью, могут использоваться в доказывании по уголовному делу не напрямую, а лишь в соответствии с процессуальным режимом, предназначенным для формирования такого вида доказательств, как вещественные. При этом вещественным доказательством будут являться не результаты оперативно-розыскной деятельности (видео пленка, полученная в ходе проведения электронного наблюдения), а результаты уголовно-процессуальной деятельности, сформированные при осмотре и вынесении постановления.

При использовании в доказывании аудио-, видео-, кино- и фотоматериалов, полученных в результате оперативно-розыскных мероприятий⁹⁹, нередко возникает необходимость в их экспертном исследовании.

На практике вопросы, разрешение которых требует специальных познаний, чаще всего проявляются в связи с проверкой подлинности аудио-, видеозаписей, а также принадлежности записанного голоса (полученного изображения) тому или иному лицу. Разрешение подобных вопросов относится к компетенции сравнительно новых видов криминалистических экспертиз — фоноскопической (фонографической) и портретной.

При соблюдении ранее упомянутых требований (известность места, времени, условий и обстоятельств ее получения, техниче-

ских характеристик аппаратуры) она может послужить основой для формирования такого вида доказательств, как заключение эксперта, при соблюдении свойственного ему режима собирания и использования в уголовном процессе.

Для этого следователь, в производстве которого находится уголовное дело, должен вынести мотивированное постановление о назначении фоноскопической (портретной) экспертизы на предмет идентификации голосов (изображений) людей, зафиксированных в ходе негласной аудио-, видеозаписи. У обвиняемых с соблюдением соответствующих процедур (УПК РФ, ст. 202) должны быть получены образцы голоса, необходимые для сравнительных исследований.

Вместе с тем все отмеченные трудности отнюдь не свидетельствуют о том, что нужно вообще запретить использование в уголовно-процессуальном доказывании материалов, полученных в ходе оперативно-розыскной деятельности. Просто исследуемую проблему необходимо решать творчески и обстоятельно, тщательно изучив большинство поставленных правоприменительной практикой вопросов. Сегодня же, по нашему мнению, материалы оперативно-розыскной деятельности (информация, полученная в ходе проведения электронного наблюдения и других оперативно-розыскных мероприятий) могут вводиться в уголовный процесс только после их проверки следственным путем и лишь при условии, что при их собирании и закреплении применялись способы и порядок, предусмотренные Федеральным законом «Об оперативно-розыскной деятельности», а содержащиеся в них сведения отвечают требованиям относимости, допустимости и достоверности. Думается, что по правовой и процессуальной природе эти материалы можно приравнять к источникам фактической информации, представляемым органам дознания, следователю, прокурору и суду. Формирование данного источника, как и других упомянутых ранее, происходит за рамками уголовного процесса, способы их представления субъектам, на которых лежит бремя доказывания, аналогичны.

Для подтверждения вышеизложенного представляют интерес следующие примеры использования электронного наблюдения.

⁹⁹ В том числе и электронного наблюдения.

1
УГОЛОВНОЕ ДЕЛО
ЦЕНТРАЛЬНОЙ ОРГАНИЗОВАННОЙ ПРЕСТУПНОЙ ГРУППИРОВКИ
ПО ОБВИНЕНИЮ ВАГИНА, СИВКОВА, ФОКИНА, ОГАНЕСЯНА
И МНОГИХ ДРУГИХ¹⁰⁰

Интересен эпизод похищения предпринимателя Д. (август 1992 года). Бандиты связывают его и увозят в частный дом, где размещается одна из их коммерческих фирм. После этого один из похитителей с телефона названной коммерческой фирмы звонит в казино киноконцертного театра «Космос» — бизнес-клуб «Глобус», просит Вагина, представляется: «...звонит С. Фокин». Вагин, подозревая, что данный телефон может прослушиваться, просит перезвонить на другой номер телефона (он тоже контролировался сотрудниками спецслужб). Продолжение диалога: «...ну что? (Вагин). Всё, мы его взяли (Фокин)». Вагин дает команду о том, чтобы Д. привезли в бизнес-клуб.

Преступники привозят данного человека, далее происходит факт вымогательства. После достижения соглашения по денежной сумме и сроку ее уплаты Д. отпускают.

После анализа данной информации был определен номер телефона коммерческой фирмы, установлены ее юридический адрес и лица, в ней работающие. Кроме этого, сотрудники спецслужб вышли на Д. Он написал заявление, по факту которого было возбуждено уголовное дело по ст. 127 и 163 УК РСФСР. Д. был допрошен, его показания были приобщены к уголовному делу, фонограмма телефонного разговора была также легализована и использована в качестве вещественного доказательства. Более того, фонограмма была подвергнута экспертизе для идентификации голосов Вагина и Фокина. Заключение эксперта также было приобщено к уголовному делу в качестве доказательства.

Все виновные лица были задержаны и осуждены. Вагин задержан не был: его «партнеры по бизнесу» 26 октября 1992 года успели свести с ним счеты.

Таким образом, в результате проведения электронного наблюдения была получена информация, позволившая пресечь деятельность наиболее активного организованного преступного сообщества и нейтрализовать его лидеров. Применение традиционных следственных методов успеха не имело. Только благодаря полученным сведениям был найден свидетель противоправных деяний Вагина. До это-

¹⁰⁰ По материалам уголовного дела № 864501 из архива Ленинского суда г. Екатеринбурга (1992).

го эпизода свидетели либо физически устранялись преступниками, либо таковых найти было невозможно по разным причинам¹⁰¹.

2

Военнослужащий Г. одной из воинских частей Уральского военного округа производит наезд на пешехода на трассе Екатеринбург — Тюмень. Человек умирает, по факту чего военной прокуратурой Екатеринбургского гарнизона было возбуждено уголовное дело. Предварительный анализ дорожно-транспортного происшествия показал, что Г. не виновен в случившемся (условия плохой видимости, небольшая скорость движения автомобиля, состояние алкогольного опьянения погибшего, свидетели происшествия, заключение инспекторов ГИБДД).

Несмотря на это, следователь военной прокуратуры Ю. А. Сухоруков на одном из допросов заявил обвиняемому, что: «...движение уголовного дела будет зависеть от того, что будет изложено в заключении эксперта». Предполагалось провести повторную экспертизу. Следователь предложил Г. познакомить его с экспертом, который будет проводить данную экспертизу. При встрече «эксперт» за услугу запросил 5 миллионов неденоминированных рублей. Г. написал заявление в органы военной контрразведки. По согласованию с военным прокурором было принято решение о проверке данного факта. Проводятся два оперативно-розыскных мероприятия (наблюдение с использованием негласной аудиозаписи): 1) запись и оперативное документирование повторной встречи заявителя со следователем, 2) то же самое, но в отношении «эксперта». В момент передачи денег мнимый эксперт был задержан. Им оказался бывший капитан внутренних войск, дознаватель, ранее закрепленный по роду выполнения своих функциональных обязанностей за Ю. А. Сухоруковым. По данному факту возбуждается уголовное дело.

Материалы оперативно-розыскных мероприятий были легализованы и приобщены к делу в качестве вещественных доказательств и по-

¹⁰¹ Эффективность проведения электронного наблюдения по рассматриваемой категории преступлений подтверждают материалы следующих уголовных дел: 1) № 2-75/03 — в отношении Р. Т. Мамедова и А. В. Лисьева, признанных виновными в совершении умышленного убийства с особой жестокостью А. С. Обласова (архив Свердловского областного суда, 2003); 2) № 2-131/03 — в отношении А. А. Астратова, С. Е. Богданова, Д. Н. Галкина, И. И. Галкина, обвиняемых в совершении тяжких и особо тяжких преступлений в отношении А. С. Новикова, Ю. И. Чистякова, А. П. Торпуриды, Л. В. Пармановой, В. А. Сухова (архив Свердловского областного суда, 2003).

ложены в основу обвинительного заключения. Суд вынес обвинительный приговор в отношении обоих подсудимых¹⁰².

3

Уральский военный округ, г. Чебаркуль. Женщина приобрела у командира воинской части дачу. Являясь вольнонаемной данной воинской части, она претендовала на выделение благоустроенного жилья. При постановке на очередь (как выяснилось в дальнейшем, на льготных основаниях) на получение жилья подделала документы, дающие на это право. Факт фальсификации становится известным органам военной прокуратуры Чебаркульского гарнизона. Заместитель военного прокурора вызывает эту женщину для дачи объяснений. В ходе разговора предлагает ей переписать необходимые документы на право собственности приобретенной ею дачи на себя, взамен он (зам. военного прокурора) «закрывает глаза» на факт подделки документов на получение жилплощади и помогает получить квартиру.

Женщина пишет заявление о данном факте в органы военной контрразведки. По согласованию с военным прокурором Уральского военного округа принимается решение о проверке данного факта. Проводится оперативно-розыскное мероприятие (наблюдение с использованием негласной аудиозаписи) в ходе повторной встречи гражданки с «представителем законности» в данной воинской части. Все факты подтверждаются, о чем ставится в известность военный прокурор Уральского военного округа. Возбуждается уголовное дело.

Материалы проведенного оперативно-розыскного мероприятия легализуются, вводятся в уголовный процесс в качестве вещественного доказательства, проводится фоноскопическая экспертиза, составляется заключение эксперта по идентификации голоса заместителя военного прокурора. После проведения предварительного расследования составляется обвинительное заключение, дело передается в суд.

Суд выносит обвинительный приговор в отношении подсудимого¹⁰³.

Приведенные примеры наглядно показывают эффективность применения электронного наблюдения по пресечению и документированию фактов вымогательства материальных ценностей со стороны работников военной прокуратуры и дознания. Получение факти-

¹⁰² По материалам уголовного дела № 232-96 из архива Уральского окружного военного суда (1996).

¹⁰³ По материалам уголовного дела № 309-97 из архива Уральского окружного военного суда (1997).

ческой информации процессуальными методами здесь невозможно, т. к. лица, которые должны проводить необходимые следственные действия, являются вымогателями и взяткополучателями. Латентность подобных преступлений является очень высокой, и именно электронное наблюдение позволяет зафиксировать подобные противоправные деяния любых субъектов состава преступления¹⁰⁴.

4

Город Екатеринбург. В отношении несовершеннолетнего подростка совершены насильственные действия сексуального характера со стороны неизвестного мужчины. Данные действия были произведены в одном из автомобильных боксов гаражного массива «Старая Сортировка». По заявлению законных представителей несовершеннолетнего возбуждается уголовное дело по ст. 132 УК РФ.

В ходе проведения оперативно-розыскных мероприятий выясняется владелец бокса, им оказывается сотрудник ГУВД Свердловской области (точнее, водитель одного из руководителей ГУВД). В гараж внедряется спецтехника, ведется наблюдение. При попытке совершить подобные действия с другим подростком преступник задерживается. Аудиозапись с информацией легализуется и приобщается к уголовному делу.

В ходе судебного разбирательства выясняется, что мужчина совершал подобные действия неоднократно.

Аудиозапись была представлена суду в качестве вещественного доказательства и положена в основу обвинения. Суд вынес обвинительный приговор¹⁰⁵.

В результате проведения рассмотренных действий были пресечены другие тяжкие преступления. Подобные деяния всегда очень тщательно скрываются преступником, а жертвы противоправных действий предпочитают умалчивать о случившемся с ними. Электронное наблюдение — как наиболее острое оперативно-техническое мероприятие — будет актуальным и по подобным категориям дел.

¹⁰⁴ Материалы электронного наблюдения послужили основой обвинительного приговора в отношении И. В. Анучина и Д. В. Окунева, совершивших покушение на получение должностным лицом через посредника взятки в виде денег в крупном размере за действия в пользу взяткодателя (по материалам уголовного дела № 2-25/03 из архива Свердловского областного суда, 2003).

¹⁰⁵ Из архива Верх-Исетского суда г. Екатеринбурга (1997). Номер уголовного дела не приводится по соображениям морали и в интересах потерпевших.

Выполненные при производстве оперативного досмотра с применением соответствующих технических средств фотоснимки (видеозапись) тайника (его содержимого), копии, слепки, сделанные с обнаруженных в нем предметов, могут быть признаны производными вещественными доказательствами в случае, если тайник с находившимися в нем предметами был уничтожен заинтересованными лицами или не сохранился по каким-либо другим причинам на момент производства следственных (судебных) действий по соответствующему уголовному делу.

Так, Т. В. Варфоломеева дает следующее определение производных вещественных доказательств: «Производными вещественными доказательствами являются материальные физические модели первоначальных вещественных доказательств, непосредственно воспроизводящие существенные признаки последних и служащие для их замены в процессе доказывания. Они передают необходимую информацию о первоначальном вещественном доказательстве и выступают в процессе доказывания как самостоятельные источники доказательств»¹⁰⁶.

Материалы, полученные в ходе данного вида оперативно-технического мероприятия, представляются органам расследования и в процессе осмотра, проведенного по правилам, предусмотренным ст. 176, 177, 180 УПК РФ, получают статус названного доказательства.

Подобным образом может войти в уголовный процесс и ксерокопия, снятая с выявленного в ходе контроля почтовых отправлений письма (если оно не сохранилось на момент предварительного расследования), содержащего данные о времени и месте совершения преступления.

Результаты оперативно-розыскной деятельности, полученные в ходе проведения электронного наблюдения, могут быть использованы и в тактических целях — для повышения эффективности подготовки и производства следственных действий (обыск, выемка и т. д.), направленных на формирование в уголовном процессе такого вида доказательства, как протоколы следственных и судебных действий (УПК РФ, ст. 83).

¹⁰⁶ Варфоломеева Т. В. Производные вещественные доказательства. М., 1980. С. 10.

Например, по оперативным данным получена информация о том, что некий гражданин возит под креслом своего легкового автомобиля две гранаты. При производстве оперативного досмотра данный факт подтверждается. Следователь прокуратуры на основании рапорта оперативного работника оформляет постановление о задержании и производстве обыска. В момент выезда данного автолюбителя с автостоянки производится его задержание.

На основании обыска автомашины и обнаружения в ней гранат возбуждается уголовное дело по ст. 222 УК РФ¹⁰⁷.

Способами собирания иных документов в уголовном судопроизводстве является истребование и представление.

Иной документ, исходящий от органа, осуществляющего оперативно-розыскную деятельность, хотя и должен быть связан с преступлением, но только текстом, содержащим сведения об обстоятельствах предмета доказывания и побочных фактах. Он не порождается преступлением. Документ должен исходить от соответствующего государственного органа, на который возложена обязанность применения оперативно-технических средств в предусмотренных законом целях, иметь дату составления, печать и подпись должностного лица.

В основу формирования иных документов могут быть положены результаты электронного наблюдения и других видов оперативно-розыскных мероприятий.

Необходимо также отметить, что ст. 86 УПК РФ предусматривает возможность получения доказательств путем их представления. Именно такой путь превращения результатов оперативно-розыскной деятельности в доказательства предлагает С. А. Шейфер, полагающий, что если доказательства — это любые сведения, полученные законным способом, то превращение результатов оперативно-розыскной деятельности в доказательства в процессуальном смысле возможно путем представления оперативных материалов следователю от широкого круга лиц¹⁰⁸.

В данном случае праву оперативного работника представить доказательства соответствует обязанность следователя принять материалы оперативно-розыскных мероприятий. Это не значит, что

¹⁰⁷ Данные получены в одном из органов дознания Свердловской области.

¹⁰⁸ См.: Шейфер С. А. Доказательственные аспекты Закона об оперативно-розыскной деятельности. С. 98.

они должны автоматически приобщаться к делу, т. к. следователь должен провести определенные процессуальные действия. Такие материалы «могут стать доказательствами по уголовному делу только при условии, если лицо, уполномоченное на ведение предварительного следствия, или суд получают их путем проведения процессуальных действий»¹⁰⁹.

Подводя итоги всему сказанному, подчеркнем еще раз, что принятие решения об использовании результатов оперативно-розыскной деятельности в доказывании по уголовному делу должно включать не только положительные ответы на вопросы, связанные с относимостью к уголовному делу данных, содержащихся в делах оперативного учета, невозможностью без них установить существенные обстоятельства дела, выбором вида доказательства, через который они будут введены в уголовный процесс, но и с представлением органам расследования (суду) сведений, необходимых для формирования, проверки и оценки соответствующих видов доказательств в процессе доказывания. Отрицательный ответ хотя бы на один из вышеперечисленных вопросов должен привести к отказу от использования результатов оперативно-розыскной деятельности в доказывании по уголовному делу. Вместе с тем это не исключает возможности их использования для поиска других возможных источников фактической информации, выработки оптимальной тактики производства следственных действий и методики расследования.

Информация, полученная в ходе проведения электронного наблюдения, может быть признана в качестве доказательства, если она:

— относится к существенным обстоятельствам дела по ст. 73 УПК РФ;

— собрана, проверена и оценена по правилам ст. 17, 88 УПК РФ, а равно уголовно-процессуального закона, регламентирующего соби́рание, проверку и оценку доказательств того вида, к которому в данном конкретном случае предлагается отнести результаты электронного наблюдения.

¹⁰⁹ Лутинская П. А. Основания и порядок принятия решений о недопустимости доказательств // Рос. юстиция. 1994. № 11. С. 3.

С учетом вышесказанного, было бы логично изложить ст. 89 УПК РФ в следующей редакции:

1. Результаты оперативно-розыскной деятельности являются источником фактических данных и могут быть приобщены к уголовному делу в качестве доказательств в соответствии с требованиями уголовно-процессуального закона.

2. Представление результатов оперативно-розыскной деятельности органу дознания, следователю, прокурору или в суд осуществляется на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность, и означает передачу в установленном законодательством Российской Федерации порядке оперативно-служебных документов, предметов, которые могут быть приобщены к уголовному делу.

Инициатива в получении результатов оперативно-розыскной деятельности может исходить от органов предварительного расследования или суда.

3. Перед представлением материалов оперативно-розыскной деятельности сведения, содержащие государственную тайну, подлежат рассекречиванию на основании мотивированного постановления руководителя органа, осуществляющего оперативно-розыскную деятельность, либо представляются в порядке и соответствии с законом.

4. Результаты оперативно-розыскной деятельности могут быть представлены следователю, прокурору или в суд в виде справки-меморандума, в которой излагается полученная информация в обобщенном виде или в виде подлинников соответствующих оперативно-служебных документов.

Представляемые материалы должна сопровождать информация о времени, месте и обстоятельствах изъятия в ходе оперативно-розыскной деятельности предметов и документов, получения видео- и аудиозаписей, кино- и фотоматериалов, копий и слепков, должно быть приведено описание индивидуальных признаков указанных предметов и документов.

В последние годы ученые-процессуалисты и практики активно обсуждают вопрос о целесообразности наличия нормы права о прослушивании телефонных и иных переговоров в уголовно-процессуальном законе. Так, Е. А. Доля склоняется к выводу, что для получения информации о содержании телефонных переговоров у правоприменительных органов также должны быть как оперативно-розыскные, так и уголовно-процессуальные средства, позволяющие получать данные для использования их в процессе доказывания по уголовным делам¹¹⁰. Но есть и противники этой идеи. Так, С. А. Шейфер считает, что прослушивание телефонных переговоров надо рассматривать как специальное оперативно-розыскное мероприятие, и попытка трансформировать его в следственное действие является несостоятельной¹¹¹.

Попытаемся дать анализ названному следственному действию с учетом введенного нами понятия электронного наблюдения.

¹¹⁰ См.: Доля Е. А. Прослушивание телефонных и иных переговоров — следственное ли это действие? // Сов. юстиция. 1992. № 19 20. С. 2.

¹¹¹ См.: Шейфер С. А. Доказательственные аспекты Закона об оперативно-розыскной деятельности. С. 98.

ГЛАВА 3

ЭЛЕКТРОННОЕ НАБЛЮДЕНИЕ В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ

§ 1. Электронное наблюдение как следственное действие

Такое следственное действие, как контроль и запись телефонных и иных переговоров, имеет значительное сходство с прослушиванием телефонных переговоров, осуществляемым в качестве оперативно-технического мероприятия. В этой связи высказывалось мнение об ошибочности регламентации такого действия в уголовно-процессуальном законе¹. На наш взгляд, законодатель поступил обоснованно. Необходимость прослушивания переговоров иногда вытекает не из оперативных материалов, а из уголовных дел. В таких случаях ранее возникали тупиковые ситуации. Следователь не мог самостоятельно получить санкцию суда на прослушивание, т. к. уголовно-процессуальный закон такого действия не предусматривал. Если же следователь давал поручение оперативным службам о проведении прослушивания телефонных переговоров на основании Федерального закона «Об оперативно-розыскной деятельности», то нарушался такой принцип взаимодействия, как самостоятельность органа дознания в выборе средств исполнения поручения следователя. Но, на наш взгляд, не это было самым негативным, значительно хуже было то, что оперативные подразделения не располагали «своими» сведениями (наработками), позволявшими им обратиться в суд за разрешением и эффективно обосновать ходатайство. На практике встречались случаи, когда санкцию на прове-

¹ См.: Шейфер С. А. Следственные действия: Система и процессуальная форма. М., 1981. С. 63; Он же. Проблемы развития системы следственных действий в УПК РФ // Уголов. право. 2002. № 3. С. 90—91.

дение оперативно-розыскного мероприятия испрашивал сотрудник оперативного подразделения правоприменительного органа на основании процессуальных сведений, не зная их досконально. Поэтому, несмотря на то, что контроль и запись телефонных и иных переговоров не в полной мере отвечает всем разработанным в теории признакам следственного действия, его необходимо сохранить в УПК РФ именно в этом качестве, и не только сохранить, но и уточнить, в чем-то принципиально пересмотреть на фоне современных телекоммуникационных средств передачи информации. Уголовно-процессуальная деятельность должна быть самодостаточной. Утверждение, что следователь вполне может обойтись дачей поручения органам, осуществляющим оперативно-розыскную деятельность, представляется не совсем правильным и логичным.

Следственные действия являются одним из основных способов собирания фактической информации для дальнейшего формирования доказательств как таковых. Необоснованное их проведение, так же как и оперативно-розыскные мероприятия, способно существенно ограничить конституционные права граждан, что абсолютно недопустимо. Возросшие требования к процессуальному порядку собирания доказательств диктуют необходимость тщательного соблюдения положений закона, регламентирующих производство следственных действий.

Термин «следственные действия», многократно встречающийся в законе, не включен в ст. 5 УПК РФ и не раскрыт в ней в числе основных понятий, используемых в Кодексе. Нет в нем и исчерпывающего обозначения видов следственных действий.

На наш взгляд, к числу следственных действий относится та часть уголовно-процессуальных действий следователя (дознателя), которая направлена на собирание и закрепление фактической информации.

Под следственными действиями обычно понимаются регламентированные процессуальным законом действия, непосредственно направленные на обнаружение, закрепление, проверку доказательств². С. А. Шейфер следственные действия определяет как

² См.: Алексеев Н. С. Очерк развития науки советского уголовного процесса / Алексеев Н. С., Даев В. Г., Кокорев Л. Д. Воронеж, 1980. С. 186; Семенцов В. А. Следственные действия: Учеб. пособие. Екатеринбург, 2003. С. 5.

«...комплекс регламентированных уголовно-процессуальным законом и осуществляемых следователем (судом) поисковых, познавательных и удостоверительных операций, соответствующих особенностям следов определенного вида и приспособленных к эффективному отысканию, восприятию и закреплению содержащейся в них доказательственной информации»³.

Эти выводы подтверждаются положениями ст. 86 (ч. 1) УПК РФ, в которой предусмотрено, что собирание доказательств осуществляется путем производства следственных действий. Таким образом, следственные действия — это установленная законом форма процессуально прописанных действий, при помощи которых обнаруживается, проверяется и закрепляется фактическая информация.

Контроль и запись телефонных и иных переговоров — новое следственное действие, появившееся в уголовно-процессуальном законе сравнительно недавно. Сегодня можно дать четкие критерии разграничения между контролем и записью переговоров как следственным действием и прослушиванием телефонных переговоров как оперативно-розыскным мероприятием⁴.

В качестве субъектов рассматриваемого следственного действия выступают следователи, уполномоченные в пределах своей компетенции, предусмотренной УПК РФ, осуществлять предварительное следствие по возбужденному уголовному делу, в то время как прослушивание телефонных переговоров отнесено к сфере деятельности сотрудников органов, осуществляющих оперативно-розыскную

³ См.: Шейфер С. А. Собирание доказательств в советском уголовном процессе: (Методологические и правовые проблемы). Саратов, 1986. С. 104; см. также: Он же. Следственные действия. С. 6—14.

⁴ Анализируемое следственное действие принципиально новым назвать можно только условно. О его аналоге уже упоминалось в Основах уголовного судопроизводства Союза ССР и союзных республик (ст. 29 и 35-1), где речь шла о прослушивании телефонных и иных переговоров. Статья 35-1 названных Основ не охватывала всех особенностей производства рассматриваемого следственного действия, что на практике порождало немало вопросов. Наличие общих правовых оснований для прослушивания переговоров как следственного действия и как оперативно-розыскного мероприятия негативно сказывалось на процессе расследования преступлений. Так, зачастую следователи, имея возможность и основания провести прослушивание телефонных и иных переговоров, отказывались от производства данного следственного действия или, проявляя осторожность, давали органу дознания поручение о производстве этого оперативно-розыскного мероприятия.

деятельность (Федеральный закон «Об оперативно-розыскной деятельности», ст. 13).

По временным параметрам анализируемое следственное действие и созвучное оперативно-розыскное мероприятие также существенно отличаются. Следователь вправе провести контроль и запись телефонных и иных переговоров строго в рамках предварительного расследования по уголовному делу, находящемуся у него в производстве. Возможность же осуществить прослушивание телефонных переговоров предоставляется оперативным работникам задолго до того, как к ней подключается следователь. Проведение указанного оперативно-розыскного мероприятия может быть воплощено в жизнь как исключительно в рамках оперативной разработки, так и в стадии возбуждения уголовного дела, предварительного расследования, а также по приостановленному уголовному делу.

Различное правовое регулирование уголовно-процессуальной и оперативно-розыскной деятельности находит свое отражение и в применении данного способа получения информации. Использование контроля и записи переговоров следователем основывается на положениях уголовно-процессуального закона⁵, а действия субъектов оперативно-розыскной деятельности регламентируются оперативно-розыскным законодательством⁶.

При рассмотрении средств и методов, которыми обеспечивается решение задач уголовно-процессуальной деятельности, также наблюдаются принципиальные различия. Несмотря на то, что рассматриваемые субъекты в равной степени отвечают за раскрытие преступления, они идут к общей цели разными путями, используя различные методы, но достигать своих целей следователи обязаны только процессуальными средствами.

Оперативно-розыскные средства и методы позволяют получить информацию, которая сама по себе доказательством не является, но может иметь существенное значение для раскрытия и расследования уголовного дела, а также использоваться для формирования

⁵ См.: УПК РФ ст. 5 п. 14-1; ст. 13, 29, 164-170, 186; ст. 213, ч. 2, п. 8; ст. 239, ч. 3, п. 2; ст. 476, прил. 89, 90, 91; ст. 477, прил. 11.

⁶ Подробнее об этом см. гл. 1 нашей книги.

доказательств после их представления или истребования в соответствии с уголовно-процессуальным законом.

Сущность контроля и записи переговоров как следственного действия состоит в том, что следователь выносит мотивированное постановление об обращении в суд с целью получения судебного решения на проведение названного действия, а также в его последующих актах, направленных на истребование и использование фактической информации в доказывании по уголовным делам. Кроме того, рассматриваемое следственное действие, по мнению законодателя, должно включать в себя осмотр и прослушивание полученных фонограмм (если такие будут получены), а также приобщение их в качестве вещественных доказательств к материалам уголовного дела.

Уголовно-процессуальный закон позволяет различать две разновидности контроля и записи переговоров, вытекающих из целей этого действия: 1) контроль и запись переговоров в целях осуществления уголовного преследования; 2) контроль и запись переговоров в целях защиты участников судопроизводства от преступных посягательств.

Принятие следователем решения о необходимости и возможности осуществления контроля и записи переговоров возможно при наличии фактических и юридических оснований⁷.

В целях уголовного преследования достаточным основанием для проведения названного действия являются сведения о том, что в переговорах подозреваемого, обвиняемого и иных лиц может содержаться информация, имеющая значение для дела. Основанием контроля и записи переговоров в целях защиты участников судопроизводства выступают сведения, устанавливающие факты преступного воздействия определенных лиц на потерпевшего, свидетеля, их родственников и близких лиц.

⁷ Фактическое основание — это объективная причина проведения следственного действия, а юридическое основание — это предусмотренное уголовно-процессуальным законом и документально оформленное судебное решение или письменное заявление потерпевшего свидетеля (см.: Комментарий к Федеральному закону «Об оперативно-розыскной деятельности»: С постатейным приложением нормативных актов и документов / А. Ю. Шумилов. М., 2003. С. 106—107).

Контроль и запись телефонных и иных переговоров допускаются лишь при производстве по уголовным делам о тяжких и особо тяжких преступлениях⁸.

При этом следует иметь в виду, что тяжесть преступления не всегда определяется статьей, по которой возбуждено уголовное дело или предъявлено обвинение. Иногда в процессе расследования уголовного дела могут стать известными сведения, факты, прямо свидетельствующие о совершении или приготовлении к совершению подозреваемым, обвиняемым или иными связанными с ними лицами, деятельность которых проверяется в ходе расследования возбужденного уголовного дела, другого, ранее не известного деяния, подпадающего под категорию тяжкого или особо тяжкого преступления. Все эти обстоятельства будут являться предметом рассмотрения в судебном заседании⁹.

Круг лиц, чьи переговоры могут быть подвергнуты контролю, строго не определен и допускается на усмотрение следователя. Закон относит к ним подозреваемого, обвиняемого и других лиц, чьи переговоры могут содержать информацию о преступлении либо иные сведения, имеющие значения для уголовного дела.

⁸ Под тяжкими и особо тяжкими преступлениями в соответствии со ст. 15 УК РФ понимаются умышленные преступления, за совершение которых судом может быть назначено наказание свыше пяти лет лишения свободы.

⁹ Не допускается проведения контроля и записи переговоров по опасным преступлениям средней тяжести: незаконное лишение свободы (УК РФ, ст. 127, ч. 2); вовлечение несовершеннолетнего в совершение преступления (УК РФ, ст. 150, ч. 1); вымогательство (УК РФ, ст. 163, ч. 1); получение взятки (УК РФ, ст. 290, ч. 1) и ряд других преступлений. На наш взгляд, законодатель руководствовался тем, что проведение рассматриваемого следственного действия слишком глубоко проникает в охраняемую сферу частной жизни граждан. Но такая позиция уязвима, т. к. указанные составы преступлений встречаются очень часто и, как правило, в дальнейшем перерастают в тяжкие и особо тяжкие преступления. Защита частной жизни гражданина противопоставляется тяжести преступления. И в данном случае, по нашему мнению, чаша весов должна склоняться в сторону ограничения конституционных прав граждан на тайну частной жизни. К сожалению, этот пробел не может быть восполнен и возможностями оперативно-розыскных служб: в соответствии с п. 3 ст. 8 Федерального закона «Об оперативно-розыскной деятельности» прослушивание телефонных и иных переговоров, в отличие от других оперативно-розыскных мероприятий, тоже допускается только в отношении лиц, подозреваемых или обвиняемых в совершении тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях.

К объектам, подпадающим под контроль и запись переговоров в целях защиты от преступных посягательств, относятся потерпевшие, свидетели, все их родственники и близкие лица. Цель следственного действия здесь иная — оградить добросовестного гражданина от противоправного деяния. Такой контроль может осуществляться в том числе на основе добровольного волеизъявления граждан. Представляется, что контроль и запись переговоров в этих случаях осуществляются по делам любой категории преступлений.

В соответствии с действующим законодательством контроль и запись переговоров возможны только на основании судебного решения. Ходатайство следователя перед судом о даче разрешения на контроль и запись переговоров возбуждается с согласия прокурора и оформляется в виде постановления, содержание которого регламентировано законом (УПК РФ, ст. 476, прил. 89). По результатам рассмотрения ходатайства судья выносит постановление (УПК РФ, ст. 477, прил. 11).

Указанное ходатайство подлежит рассмотрению единолично судьей районного суда или военного суда соответствующего уровня по месту производства предварительного следствия или производства следственного действия не позднее 24 часов с момента поступления рассматриваемого ходатайства. В судебном заседании вправе участвовать прокурор и следователь.

Повторим, что контроль и запись переговоров потерпевшего, свидетеля или их близких родственников, родственников, близких лиц допускаются при наличии угрозы совершения насилия, вымогательства и других преступных действий в связи с их участием в данном уголовном деле и по их письменному заявлению.

Соблюдение названных условий дает следователю право производства контроля и записи переговоров без судебного решения. Однако закон не вменяет следователю в обязанность уведомлять соответствующий суд о начале производства следственного действия. На наш взгляд, судебный контроль должен быть сохранен даже при свободном волеизъявлении гражданина подвергнуться ограничениям в конституционных правах, но превратиться из предварительного в последующий, как это предусмотрено при осмотре жилища, обыске и выемке в жилище, а также личном обыске (УПК РФ, ст. 165, ч. 5). Кстати, в оперативно-розыскной деятельности

прослушивание переговоров без судебного решения производится с обязательным уведомлением суда в течение 48 часов (Федеральный закон «Об оперативно-розыскной деятельности», ст. 8, ч. 4).

Б. Т. Безлепкин, Ю. Г. Торбин и И. А. Цополов в своих комментариях к ст. 186 УПК РФ пишут, что контроль и запись переговоров в процессе уголовного судопроизводства могут проводиться только по возбужденному уголовному делу, в связи с чем в ходатайстве следователя обязательно указывается номер уголовного дела, дата его возбуждения, основания, объясняющие необходимость и законность данного следственного действия, фамилия, имя и отчество лица, чьи переговоры подлежат контролю и записи, какие именно переговоры и с какого телефона (если речь идет о его прослушивании), срок осуществления контроля и записи, орган, которому поручается техническое осуществление контроля и записи¹⁰.

Анализируя комментарии к УПК разных авторов, необходимо отметить, что в постановлении следователя о возбуждении ходатайства о производстве контроля и записи телефонных и иных переговоров, а затем и в постановлении судьи о разрешении рассматриваемого следственного действия должны быть в обязательном порядке указаны установочные данные лица, в отношении которого планируется провести испрашиваемое действие, и номера телефонов. А всегда ли это возможно и целесообразно?

Допустим, расследуется уголовное дело, возбужденное по ст. 228 УК РФ. Необходимо провести контроль и запись переговоров с телефона арендодателя частного дома с целью установления круга лиц, причастных к незаконному изготовлению, приобретению, хранению, перевозке, пересылке либо сбыту наркотических средств и психотропных веществ. Владелец в указанном доме в настоящее время не проживает. Круг лиц, пользующихся телефоном, не известен. Как быть в этом случае?

¹⁰ См.: Безлепкин Б. Т. Комментарий к Уголовно-процессуальному кодексу Российской Федерации (постатейный) / Безлепкин Б. Т., Торбин Ю. Г., Цополов И. А. 4-е изд., перераб. и доп. М., 2004. С. 273; Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Под общ. и науч. ред. А. Я. Сухарева. 2-е изд., перераб. и доп. М., 2004. С. 332; Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Под общ. ред. В. И. Радченко. 2-е изд., перераб. и доп. М., 2004. С. 499—502.

Другой пример. Возбуждено уголовное дело по ст. 222 УК РФ. Необходимо провести контроль и запись переговоров установленного лица. Подозреваемый пользуется сотовым телефоном стандарта GSM. Оператор связи оказывает свои услуги в определенном тарифе, предусматривающем присвоение нового абонентского номера при истечении времени оплачиваемого разговора¹¹. На какой телефонный номер испрашивать судебное разрешение?

М. А. Пешков в статье, посвященной проблеме электронного наблюдения в уголовном процессе США, пишет о том, что принципиальным новшеством стало наблюдение за блуждающим объектом (*roving surveillance*), подразумевающее прослушивание не конкретного средства связи, указанного в ордере, а лица, где и какой бы связью он ни пользовался. В Меморандуме Министерства юстиции США, сопровождавшем проект нового закона, говорилось, что «закон не содержит точного указания предмета прослушивания и, таким образом, позволяет получать ордер на прослушивание разговоров конкретного лица, а не телефонного аппарата или помещения»¹².

На наш взгляд, было бы логичным в определенных и строго оправданных случаях испрашивать и получать необходимое судебное постановление на контроль и запись переговоров (в первом примере — на конкретный телефонный номер без указания установочных данных пользующихся им лиц, а во втором — на подо-

¹¹ Подобную услугу связи, на первый взгляд достаточно необычную, предоставляют многие операторы сотовой связи. Например, на территории Екатеринбург и Свердловской области подобный тариф имеет ООО «Екатеринбург-2000» («Моби NEXT GSM»). Абонент, желающий воспользоваться данной услугой, покупает sim-карту, имеющую определенный номер телефона, рассчитанный на определенное количество минут разговора (5, 10, 15 и т. д. в зависимости от потребности), и вставляет ее в свой телефон. Установочные данные такого абонента в компании не регистрируются. Выговорив положенные минуты, клиент выбрасывает названную карту и в случае необходимости покупает новую.

В Австралии в последние годы широкое распространение получили «разовые» сотовые телефоны. Принцип пользования ими подобен описанному выше с той только разницей, что, используя оплаченное время, клиент выбрасывает саму телефонную трубку, а в случае необходимости приобретает новую, естественно с новым абонентским номером.

¹² Цит. по: Пешков М. А. Прослушивание и электронное наблюдение в уголовном процессе США // Рос. юстиция. 1997. № 4. С. 29—31.

зреваемое или обвиняемое лицо, без указания конкретного номера телефона). Это ни в коей мере не ограничит конституционные права рассматриваемых лиц, т. к. все необходимые процессуальные вопросы будут соблюдены, а кроме того, позволит эффективней использовать рассматриваемое следственное действие.

Срок проведения данного следственного действия не может превышать 6 месяцев. Оно прекращается по постановлению следователя, если необходимость в данной мере отпадает, но не позднее истечения срока расследования по уголовному делу. Однако, если по обстоятельствам дела, срок расследования которого не истек, требуется возобновление осуществления контроля и записи переговоров, следователь, отменив предыдущее постановление, вправе с согласия прокурора обратиться в суд с новым ходатайством, который его рассматривает на основании вновь представленных материалов.

Учитывая специфичность деятельности по организации и техническому обеспечению контроля и записи переговоров, к тому же связанных с подключением к станционной аппаратуре предприятий связи, мероприятия такого рода обычно поручают субъектам оперативно-розыскной деятельности в лице территориальных органов Федеральной службы безопасности и Министерства внутренних дел России.

В соответствии с ч. 5 ст. 64 Федерального закона «О связи» при проведении уполномоченными государственными органами следственных действий операторы связи обязаны оказать этим органам содействие в соответствии с требованиями уголовно-процессуального закона.

Как видно, приведенная норма права является бланкетной. К сожалению, какое именно содействие и какие конкретные требования к операторам связи должны быть предъявлены при проведении следственных действий, и в первую очередь контроля и записи переговоров, уголовно-процессуальный закон не оговаривает. Думается, законодателю придется восполнить допущенный пробел.

На наш взгляд, было бы целесообразным в рассматриваемой области использовать имеющийся богатый опыт у зарубежных стран, и в частности США. Так, Уголовно-процессуальный закон штата Нью-Йорк содержит следующую норму, посвященную ис-

пользованию приборов регистрации входящей и исходящей информации, в соответствии с которой решение суда, санкционирующее установку и использование приборов, регистрирующих исходящую и входящую информацию, предписывает:

...Постановление должно быть скреплено печатью, если иначе не оговорено судом; и лицо, владеющее или арендующее канал связи, в который внедряется прибор, регистрирующий исходящую и входящую информацию, или лицо, которому судом было предписано обеспечить содействие заявителю (должностному лицу правоприменительной структуры), не разглашало информацию о наличии приборов, регистрирующих исходящую и входящую информацию, и факт проведения расследования пользователю услуг (лицу, в отношении которого проводится расследование) или другому лицу, если или пока иначе не оговорено судом.

По запросу заявителя (должностного лица), имеющего право на использование прибора, регистрирующего исходящую информацию, в соответствии с данной статьей провайдер проводных и электронных услуг связи, арендодатель, должностное лицо или другое лицо обязаны предоставить заявителю или его агенту (помощнику) незамедлительно всю информацию, оборудование и техническую помощь, необходимую для производства незаметной установки прибора, регистрирующего исходящую информацию, с минимальными помехами для тех услуг, которые лицо (провайдер), получившее об этом указание суда, предоставляет стороне, в отношении которой планируется произвести установку и применение названного прибора, если такое содействие производится на основании судебного постановления, как предписано в разделе 705.10 данной статьи.

По запросу заявителя (должностного лица), имеющего право на получение результатов применения прибора, регистрирующего входящую информацию, согласно данной статье провайдер проводных и электронных услуг связи, арендодатель, должностное лицо или другое лицо должны незамедлительно установить такое устройство на требуемом канале связи и немедленно предоставить такому заявителю (должностному лицу) всю информацию, оборудование и техническую помощь, включая незаметную установку и работу прибора и с минимальными помехами для услуг, которые данное лицо, получившее об этом постановление суда, предоставляет стороне, в отношении которой установка и применение (приборов) будет иметь место, если такая установка и содействие производится в соответствии с судебным постановлением, как предписано в разделе 705.10 данной

статьи. Если иначе не оговорено судом, то результаты применения приборов, регистрирующих входящую информацию, должны быть предоставлены заявителю (должностному лицу) или его агенту (помощнику) через приемлемые промежутки времени в рабочие часы в течение срока действия постановления.

Любому провайдеру проводных и электронных услуг связи, арендодателю, должностному лицу или другому лицу, которое предоставляет оборудование или техническую помощь, в соответствии с данным разделом должна быть предоставлена компенсация в разумных размерах за обоснованные расходы, понесенные при предоставлении этого оборудования или помощи.

Согласно данной статьи никакое основание не должно быть признано законным ни в каком суде для возбуждения иска против любого провайдера проводных и электронных услуг связи, его должностных лиц, сотрудников, агентов или других оговоренных лиц за предоставление информации, оборудования или содействия, в соответствии с условиями, предписанными судом (перевод наш. — Ю. С.)¹³.

Изучая текст приведенной нормы, необходимо отметить следующее:

- Рассматриваемая норма содержится в тексте Уголовно-процессуального закона штата Нью-Йорк, а не в другом нормативно-правовом акте.

- Закон прямо предписывает оператору связи, какое именно содействие он должен оказать сотруднику правоприменительного органа в проведении контроля входящей и исходящей информации абонента.

- Проведение контроля входящей и исходящей информации абонента выполняется конфиденциально, разглашение факта проведения расследования пользователю услуг связи запрещено.

- Установка и эксплуатация специальных технических средств операторами связи производится незамедлительно, по первому требованию сотрудника правоприменительного органа при наличии у него решения суда.

- Материалы контроля предоставляются уполномоченному лицу через приемлемые промежутки времени в рабочие часы, в течение срока действия постановления суда.

¹³ Criminal Procedure Law // N. Y. Criminal Stat. and Rules». 2002. LexisNexis. P. 452.

- Провайдеру предоставляется компенсация в разумных размерах за обоснованные расходы, понесенные им при установке и эксплуатации специальных технических средств.

- Вся ответственность за законность рассматриваемого деяния возложена на правоприменительные органы¹⁴.

Если бы подобная норма права содержалась в действующем УПК РФ, то ч. 5 ст. 64 Федерального закона «О связи» соответствовала бы своему содержанию.

Продолжая наши рассуждения об уголовно-процессуальной характеристике контроля и записи переговоров как следственного действия, необходимо отметить, что следователь в течение всего срока производства названного действия вправе в любое время истребовать от органа, его осуществляющего, фонограмму для осмотра и прослушивания (если таковая имеется). Она передается следователю в опечатанном виде с сопроводительным письмом (с пометкой «лично»), в котором должны быть указаны дата и время начала и окончания записи указанных переговоров и краткие характеристики использованных при этом технических средств. Закон не предусматривает предварительного прослушивания следователем произведенных записей для целей отбора относящейся к делу информации. Представляется, что он имеет право истребовать записи по своему усмотрению, остальные же, как не относящиеся к делу, уничтожить. Все поступившие к нему фонограммы должны быть в установленном порядке осмотрены с обязательным участием понятых путем внешнего обследования и прослушивания. Специалист, а также лица, чьи переговоры записаны, приглашаются для осмотра по усмотрению следователя.

Привлечение к осмотру лиц, чьи переговоры записаны, имеет смысл тогда, когда эти лица идут на сотрудничество со следствием. Их участие в осмотре и прослушивании позволит более точно изложить прослушанную звукозапись, сделать акцент на наиболее важной части фонограммы, а также внести в протокол комментарии и замечания к тексту фонограммы.

¹⁴ Подобные нормы права содержатся не только в законодательствах штата, но и на федеральном уровне (см.: 18 U.S.C., параграф 3123 (c); 18 U.S.C., параграф 3123 (d, 2); 18 U.S.C., параграф 3124 (a, b); 18 U.S.C., параграф 3124 (c), 18 U.S.C., параграф 3124 (d, e).

По смыслу ст. 169 УПК РФ следователь при необходимости вправе привлечь к осмотру и прослушиванию также переводчика.

Процесс контроля и записи переговоров не протоколируется. Протокол составляется лишь при осмотре фонограммы. Статья 186 (ч. 7) УПК РФ предписывает, что о результатах осмотра и прослушивания фонограммы следователь с участием понятых и при необходимости специалиста, а также лиц, чьи переговоры записаны, составляет протокол, в котором должна быть дословно изложена та часть фонограммы, которая, по мнению следователя, имеет отношение к данному уголовному делу. Лица, участвующие в осмотре и прослушивании фонограммы, вправе в том же протоколе или отдельно изложить свои замечания к протоколу.

При наличии в фонограмме фактической информации следователь выносит постановление о приобщении ее к материалам уголовного дела в качестве вещественного доказательства. В дальнейшем фонограмма хранится в опечатанном виде в условиях, исключающих возможность прослушивания и тиражирования ее посторонними лицами и обеспечивающих сохранность аудиозаписи и техническую пригодность для повторного прослушивания, в т. ч. в зале судебного заседания.

В литературе, отмечая значимость фонограммы, некоторые авторы вполне объективно считают, что она является и документом, и вещественным доказательством¹⁵.

Для установления или подтверждения подлинности приобщенной к уголовному делу фонограммы следователь может принять решение о направлении ее в экспертно-криминалистическое подразделение для проведения фоноскопической (фонографической) экспертизы. При этом следователь обязан вынести постановление о назначении названного вида экспертизы¹⁶. В этом случае заключение эксперта также становится источником доказательств.

¹⁵ См., в частности: *Козырев Г.* Документирование прослушивания и звукозаписи телефонных и иных переговоров // *Законность.* 1993. № 4. С. 36.

¹⁶ Сегодня фоноскопические экспертизы уже перестали быть уникальными. Основными задачами, решаемыми при исследовании фонограмм, являются идентификация человека по голосу и диагностика особенностей его личности (пол, национальная и социальная принадлежность, культурный уровень и т. д.), в связи с чем необходимо различать диагностическую и идентификационную

Истребование сведений о входящих и исходящих сигналах соединений, продолжительности разговора и другой информации, содержащейся в протоколах соединений абонентов, должно осуществляться на основании судебного решения в рамках рассматриваемого следственного действия, поскольку распространение этой информации ограничивает тайну телефонных переговоров и иных сообщений¹⁷.

Рассматриваемое следственное действие предусматривает контроль и запись переговоров, называя две их разновидности: телефонные и иные.

Под телефонными переговорами по смыслу п. 14-1 ст. 5 УПК РФ подразумеваются переговоры путем использования любых средств коммуникации.

В. В. Кальницкий полагает, что это слишком широкое толкование. По его мнению, тайна переговоров с использованием радиостанций законом не охраняется, поэтому доступ к ним возможен без судебного разрешения. На его взгляд, то же имеет место и в случаях, когда переговоры ведутся по служебным каналам связи внутри учреждения, организации, предприятия¹⁸.

фоноскопические экспертизы. Рассматриваемые виды экспертиз основаны на том, что голос человека индивидуален (специфическая форма и размеры ротовой и носовой полости, горла, органов дыхания), поэтому физические характеристики звуков (частота, длительность, интенсивность) у каждого человека строго индивидуальны. Акустическая характеристика голоса относительна, устойчива во времени и остается индивидуальной даже при морфологических и патологических изменениях органов речи.

В основу методики фоноскопических исследований положены акустические и лингвистические анализы устной речи. Комплексный лингвоакустический анализ позволяет проводить идентификацию человека даже по фонограммам низкого качества и малой длительности. Фоноскопические исследования проводятся с помощью измерительно-вычислительных комплексов, включающих высококачественную звукозаписывающую и воспроизводящую аппаратуру, совмещенную с современными средствами персональных электронно-вычислительных машин (более подробно см.: *Аверьянова Т. В.* Криминалистика: Учеб. для вузов / *Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г.* и др.; Под ред. Р. С. Белкина. М., 2001. С. 363—367).

¹⁷ См.: Определение Конституционного суда РФ от 2 октября 2003 года № 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»» // *Рос. газ.* 2003. 10 дек.

¹⁸ См.: *Кальницкий В. В.* Следственные действия: Учеб. пособие. 2-е изд., перераб. и доп. Омск, 2003. С. 36.

С его мнением можно согласиться, но с одной оговоркой. В Федеральном законе «О связи» нет такого понятия, как служебный канал связи, а есть понятия линии связи и сети связи общего пользования (Федеральный закон «О связи», ст. 2, 13). Охрана конституционных прав граждан на тайну телефонных и иных переговоров по смыслу названного Федерального закона должна распространяться исходя не из вида пользовательского оборудования, а из сети связи, по которым данные переговоры ведутся. На наш взгляд, граждане могут обоснованно рассчитывать на тайну своих переговоров, если сигнал передается по сетям связи общего пользования или присоединенным (переведенным) к названным сетям выделенным или технологическим сетям связи¹⁹.

Ю. В. Гаврилин и Е. С. Дубоносов утверждают, что телефонные переговоры — это передача сообщений по городской, междугородной и международной сетям электросвязи (проводной линии телефонной сети). Они пишут, что телефонные переговоры на этом не ограничиваются, они включают также телеграфные и факсимильные виды услуг. К числу «иных переговоров» названные авторы относят направление в области связи с применением систем компьютерной телефонии. В качестве названных систем понимаются системы голосовой почты, конференц-связи, тарификации, записи телефонных переговоров²⁰.

Как уже упоминалось, новый Федеральный закон «О связи» не содержит понятий городской, междугородной и международной сети электросвязи (такие понятия, как городские, междугородные и международные переговоры, а телеграфные и факсимильные виды услуг к телефонным переговорам вообще не относятся: телеграфные услуги всегда относились к объекту почтовой сети связи, а факсимильные — к сообщениям, передаваемым по сетям документальной электросвязи.

Необходимо подчеркнуть принципиальное различие между переговорами и сообщениями. П о д п е р е г о в о р а м и понимается

¹⁹ Информация, передаваемая по сетям связи специального назначения, охраняется Законом о государственной тайне.

²⁰ См.: Гаврилин Ю. В., Дубоносов Е. С. Использование контроля и записи телефонных и иных переговоров в раскрытии и расследовании преступлений: Учеб. пособие. М., 2003. С. 12—13.

информация, передаваемая и воспринимаемая с помощью речевого и слухового аппарата человека в устной форме, как непосредственно, так и посредством использования оконечного оборудования единой сети электросвязи России. А п о д с о о б щ е н и я м и — переданная информация, которая воспринимается только визуально: пейджинговые или SMS-сообщения; почтовые, телеграфные или сообщения, переданные электронной почтой, телематические услуги связи.

На наш взгляд, представляет определенный интерес толкование анализируемых понятий Б. Я. Гавриловым, В. В. Кальницким и И. А. Цополовым в научно-практических комментариях к УПК РФ. Так, под телефонными переговорами названные юристы понимают переговоры, ведущиеся с помощью аппаратов, использующих проводные линии, радиотелефонные каналы, каналы сотовой, космической связи и т. д. А п о д к о н т р о л е м и з а п и с ь ю иных переговоров понимается, например, применение прослушивающих устройств в служебном помещении, съем информации с применением технических средств через оконное стекло офиса и т. д.²¹

Раздел 18 Свода законов США (18 U.S.C.) определяет телефонные переговоры как «...любую воспринимаемую на слух информацию, передаваемую полностью или частично по проводам, кабелям или другим подобным соединениям между исходящей точкой и точкой приема (включая использование таких соединений на коммутируемой станции), производимые любым лицом»²². В приведенном определении самое важное заключается в том, что телефонные переговоры должны содержать ч е л о в е ч е с к и й г о л о с, или, как предписывает законодатель, у с т н у ю п е р е д а ч у. Если передаваемая информация не содержит оригинального (настоящего) чело-

²¹ См.: Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Под общ. ред. В. П. Верина, В. В. Морзякова. М., 2004. С. 455—457; см. об этом также: Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Отв. ред. В. И. Радченко; Науч. ред. В. Т. Томин, М. П. Поляков. М., 2004. С. 450—453; Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Под общ. ред. В. И. Радченко. 2-е изд., перераб. и доп. М., 2004. С. 499—502.

²² 18 U.S.C., параграф 2510 (1).

веческого голоса одного человека или группы лиц, то данная информация не может рассматриваться как телефонные переговоры²³.

Если по поводу понятия «телефонные переговоры» еще можно говорить о наличии общего понимания устных односторонних, двусторонних или многосторонних переговоров, ведущихся с использованием пользовательского оборудования по линиям связи, то относительно значения термина «иные переговоры» единого мнения не существует.

Традиционно, поскольку ранее контроль и запись переговоров относились лишь к оперативно-розыскным мероприятиям, под контролем иных переговоров понималось снятие информации с технических каналов связи, к которым, например, Министерство внутренних дел России относил телексовые, факсимильные, селекторные, радиорелейные и т. п. каналы передачи данных. Сюда же могли быть отнесены компьютерные сети и различные радиопереговорные устройства, основанные на использовании электромагнитного излучения.

Думается, что снятие информации с технических каналов связи и иные переговоры суть не одно и то же. Термин «контроль переговоров» прежде всего предполагает фиксацию устной речи независимо от того, каким способом говорящие обмениваются информацией. По техническим же каналам связи устная речь не передается. Поэтому под иными переговорами, по нашему мнению, правильно будет понимать устную речь, передаваемую без помощи оконечного оборудования и линий связи.

Контроль и фиксация такой речи могут осуществляться с помощью акустической аппаратуры, в т. ч. сопряженной с записью видеоизображения. В связи с чем законодатель предоставил следователю право в процессе доказывания по уголовному делу фиксировать не только телефонные переговоры, но и устную речь с помощью аудио- и видеотехники. Такая аппаратура негласно может быть установлена, например, в служебном кабинете или ином помещении, для проникновения в которое не требуется специального судебного решения.

²³ См.: S. Rep. No. 99—541, at 12 (1986), reprinted in 1986 U.S.C.C.A.N.3555; United States v. Torres, 751 F. 2d 875, 885—886 (7th Cir. 1984).

Таким образом, контроль и запись переговоров позволяют получить информацию, имеющую отношение к расследуемому уголовному делу, путем документирования телефонных и других устных переговоров лиц в целях осуществления уголовного преследования или защиты участников уголовного судопроизводства от преступных посягательств. Вся иная информация, передаваемая по единой сети электросвязи России, остается, на наш взгляд, за рамками рассматриваемого следственного действия, т. е. контроль пейджинговых сообщений, информации, передаваемой по сетям документальной электросвязи, сообщений, передаваемых по электронной почте, информации, обращающейся в сети Интернет, сообщений межкомпьютерного обмена, цифровых каналов связи, любой другой информации, передаваемой в знаковой или кодированной форме, не воспринимаемой или не понимаемой человеком на слух, следовательно самостоятельно произвести не может. Он вынужден, как и прежде, давать поручение оперативным службам получать необходимую информацию, но уже в рамках оперативно-розыскной деятельности. Данные пробелы в уголовно-процессуальном законодательстве существенно сужают и ограничивают процессуальную самостоятельность следователя и, как уже было отмечено выше, органа дознания в выборе средств исполнения поручений.

В отличие от нашего законодательства, в уже упомянутом нами разд. 18 Свода законов США дается определение электронному сообщению, под которым понимается

...любая передача знаков, сигналов, письменных сообщений, звуков, данных или информации любого характера, передаваемой целиком или частично по проводам, радио-, электромагнитным, фотоэлектронным или оптическим системам, которые используются при общении между штатами и между городами, за исключением:

- a) любой передачи устной информации по проводной связи;
- b) любой информации, передаваемой на пейджер в тоновом режиме;
- c) любой информации, передаваемой с устройства слежения;
- d) информации о передаче электронных счетов, хранимых финансовым учреждением в коммуникационной системе²⁴.

²⁴ См.: 18 U.S.C., параграф 2510 (1).

Как видно из приведенного определения, электронная информация — это широкая категория, а большинство сообщений, передаваемых через Интернет (включая электронную почту), являются информацией в электронном виде.

XXI век — век цифровых технологий. В научной литературе совершенно справедливо отмечается, что названные технологии уверенно завоевывают позиции практически во всех сферах создания, хранения, обработки и распространения сведений и данных²⁵, но у этого, как и у всякого дарованного технических прогрессом блага, есть и обратная сторона. Права И. П. Малинова, утверждая, что «...масштабы и характер лавинообразно нарастающих проблем, связанных с использованием информационных технологий, требуют не только законодательного регулирования, но и принятия адекватных мер со стороны властных институтов»²⁶. Поэтому анализируемое следственное действие нуждается в дальнейшем организационном, методическом и правовом совершенствовании.

На наш взгляд, было бы логично расширить рамки контроля и записи переговоров как следственного действия, включив в него не только устную речь, передаваемую непосредственно или при помощи оконечного оборудования и линий связи, но и иные сообщения, продуцируемые и представляемые человеком посредством единой сети электросвязи.

С учетом вышеизложенного считаем целесообразным предусмотреть в уголовно-процессуальном законе новое следственное действие, которое поглотит своим объемом контроль и запись переговоров, восполнив имеющиеся пробелы.

Для этого необходимо изменить наименование ст. 186 УПК РФ и изложить ее в следующей редакции.

²⁵ См.: Митрофанов Е. А., Каретников М. К. Некоторые проблемы нормативного регулирования применения и оборота специальных технических средств // Состояние, проблемы применения и совершенствования законодательства о борьбе с организованной преступностью и коррупцией. М., 2001.

²⁶ Малинова И. П. Регулирование информационной стихии как проблема современной культуры // Информ. о-во: право и власть: Сб. науч. ст. Екатеринбург, 2001. С. 4.

СТАТЬЯ 186. ПРОВЕДЕНИЕ ЭЛЕКТРОННОГО НАБЛЮДЕНИЯ

1. При наличии достаточных оснований полагать, что телефонные и устные переговоры, любая другая информация, передаваемая по сетям электросвязи общего пользования и присоединенным к названной сети выделенным или технологическим сетям связи, подозреваемого, обвиняемого и других лиц может содержать сведения, имеющие значения для уголовного дела, ее документирование, фиксация на материальном носителе и оценка допускаются при производстве по уголовным делам средней тяжести, тяжким и особо тяжким преступлениям только на основании судебного решения, принимаемого в порядке, установленном статьей 165 настоящего Кодекса.

2. В случае возникновения угрозы жизни, здоровью, собственности потерпевшего, свидетеля или их близких родственников, родственников близких лиц проведение электронного наблюдения допускается на основании постановления следователя, по заявлению или с согласия в письменной форме указанных лиц, с обязательным уведомлением судьи в течение 24 часов, а при отсутствии такого заявления — на основании судебного решения.

3. В ходатайстве следователя о проведении электронного наблюдения указывается:

- уголовное дело, при производстве которого необходимо применение данной меры;
- основания, по которым производится данное следственное действие;
- фамилия, имя, отчество лица, чьи телефонные, устные переговоры, любая другая информация документируются. Для уточнения круга лиц, подозреваемых в совершении преступления, допускается указание нумерации средства связи без приведения установочных данных пользующихся им лиц;
- срок проведения электронного наблюдения;
- наименование органа дознания и/или оператора связи, которому поручается техническое осуществление электронного наблюдения.

4. Постановление о проведении электронного наблюдения направляется следователем для исполнения в соответствующий орган дознания и/или оператору связи.

5. Оператор связи²⁷ на основании судебного решения, а в случаях, указанных в части второй настоящей статьи, на основании постановления прокурора, следователя или руководителя органа дознания обязан обеспечить содействие прокурору, следователю или дознавателю и не вправе разглашать информацию о факте проведения расследования абоненту или другому лицу.

Прокурор, следователь или дознаватель предупреждают оператора связи о недопустимости разглашения ставших известными ему данных предварительного расследования, о чем у него берется подписка с предупреждением об ответственности в соответствии со ст. 310 УК РФ.

На основании решения суда оператор связи должен незамедлительно предоставить следователю всю необходимую информацию, оборудование и техническую помощь в течение срока действия судебного решения.

Оператору связи, предоставляющему оборудование или техническую помощь следователю в соответствии с данной статьей, может быть предоставлена компенсация за обоснованные расходы, понесенные им при предоставлении этого оборудования или помощи.

6. Проведение электронного наблюдения может быть установлено на срок до 180 суток²⁸. Оно прекращается по постановлению следователя, если необходимость в данной мере отпадает, но

²⁷ Оператора связи можно отнести к «иным» участникам уголовного судопроизводства. Это лицо, обладающее специальными познаниями (т. е. специалист) в области телекоммуникационных средств связи и не заинтересованное в исходе уголовного дела, действия которого регламентированы ст. 58, 168, 251, 270 УПК РФ.

²⁸ Указанный срок обусловлен прежде всего тем, что электронное наблюдение проводится, как правило, по сложным и многоэпизодным уголовным делам, когда установить круг лиц, причастных к совершенному (совершаемому) преступлению, и размер причиненного ущерба по «горячим следам» не представляется возможным. В связи с этим предварительное следствие по уголовному делу не может быть закончено в срок, не превышающий 2 месяца со дня его возбуждения, и, как правило, продляется в установленном законе порядке до 6 месяцев прокурором района, города и приравненным к нему военным прокурором и их заместителями (УПК РФ, ст. 162, ч. 4). Изучение

не позднее окончания предварительного расследования по данному уголовному делу.

7. Следователь в течение всего срока проведения электронного наблюдения вправе в любое время истребовать от органа дознания или оператора связи, его осуществляющего, фонограмму или иную информацию для осмотра и прослушивания. Она передается следователю в опечатанном виде с сопроводительным письмом, в котором должны быть указаны дата и время начала и окончания проведения электронного наблюдения и краткие характеристики использованных при этом технических средств.

8. О результатах осмотра и прослушивания фонограммы или иной информации, полученной в ходе проведения электронного наблюдения, следователь с участием понятых и, при необходимости, специалиста составляет протокол, в котором должна быть дословно изложена та часть фонограммы или иная фактическая информация, которая, по мнению следователя, имеет отношение к данному уголовному делу. Лица, участвующие в осмотре и прослушивании фонограммы, осмотре иной предоставленной информации, вправе в том же протоколе или отдельно изложить свои замечания к протоколу.

9. Фонограмма или фактическая информация в полном объеме приобщаются к материалам уголовного дела на основании постановления следователя в качестве вещественного доказательства или иного документа и хранятся в опечатанном виде в условиях, исключающих возможность прослушивания и тиражирования указанных объектов посторонними лицами и обеспечивающих их сохранность и техническую пригодность для повторного прослушивания или предъявления, в том числе в судебном заседании.

Иная информация, полученная в ходе электронного наблюдения и обладающая признаками, указанными в ч. 1 ст. 81 настоящего Кодекса, признается вещественным доказательством.

А кроме того, необходимо привести в соответствие образцы процессуальных документов, приведенных в прил. 89, 90, 91 ст. 476

следственной и судебной практики, выполненное автором этой книги, подтверждает данный факт. Поэтому максимальный срок проведения рассматриваемого следственного действия целесообразно установить именно в 180 суток.

и в прил. 11 ст. 477 УПК РФ, с предлагаемым следственным действием²⁹.

Проведение электронного наблюдения в рамках предварительного расследования существенно расширит процессуальные возможности следователя для поиска и получения фактической информации с целью формирования полноценных доказательств в рамках уголовного процесса, предоставит следователю возможность самостоятельно испрашивать разрешение суда на проведение электронного наблюдения и выбирать оптимальный путь расследования уголовного дела с учетом полученных материалов. Появится возможность контроля современных средств электросвязи подозреваемых, обвиняемых и других лиц в целях уголовного преследования или более эффективной защиты участников судопроизводства от преступных посягательств. Электронное наблюдение позволит явственнее очертить границы такого следственного действия, как наложение ареста на почтово-телеграфные отправления при передаче сообщений в электронном виде, включив их в свое содержание, что немало важно для укрепления законности при ограничении конституционных прав граждан, где произвольная интерпретация является слишком большой роскошью.

Эффективность проведения электронного наблюдения во многом определяется не только уровнем организации этой деятельности и ее сочетанием с тактическим разнообразием применяемых приемов и способов, но и умелым использованием полученных результатов предлагаемого следственного действия в ходе расследования уголовного дела. Постараемся осветить этот вопрос подробнее.

§ 2. Использование результатов электронного наблюдения в процессе доказывания по уголовным делам

Под результатами электронного наблюдения будем понимать полученную органами предварительного следствия на основании и в порядке, предусмотренном уголовно-процессуальным

²⁹ Образцы (проекты приложений) процессуальных документов приведены в прил. 1—4 нашей книги.

законом, фактическую информацию, зафиксированную на материальном носителе, имеющую значение для расследования уголовного дела.

Названные результаты, в зависимости от преследуемых целей использования, условно можно разделить на следующие две категории.

1. Материалы информационного характера, обеспечивающие выбор организационных и тактических приемов осуществления других следственных действий. Например, связи подозреваемого, обвиняемого или других лиц, причастных к совершению расследуемого преступления; место, время, цель встречи указанных лиц с предполагаемыми сообщниками или пособниками; места хранения предметов материального мира или иных документов, могущих впоследствии получить статус доказательств; различного вида установочные данные по лицам и/или средствам передвижения и т. д.

Названная информация может не содержать конкретных сведений о совершенном, дящемся или готовящемся преступлении, но используется для проведения и подготовки таких следственных действий, как обыск, выемка, осмотр, допрос, очная ставка и др. Кроме того, подобные материалы позволят принять превентивные меры, препятствующие уничтожению орудий преступления, денежных средств, полученных преступным путем, а также подкупу или запугиванию потенциальных свидетелей.

2. Собственно результаты электронного наблюдения, имеющие непосредственное доказательственное значение, т. е. прямо указывающие на признаки преступления и причастных к нему лиц. В дальнейшем такая информация может быть доведена до сотрудников органов, осуществляющих оперативно-розыскную деятельность и включенных в следственную группу по расследованию преступления (особенно многоэпизодного), или использоваться для формирования полноценного доказательства в процессе расследования после ее соответствующей проверки, оценки и процессуального закрепления. Возможность использования указанной информации в качестве доказательств определяется следователем, а при продолжении оперативной разработки организованной преступной группы — по согласованию с инициатором разработки.

Результаты электронного наблюдения, полученные следователем в ходе его проведения, могут быть им использованы в следующих целях:

- планирование расследования уголовного дела при выдвижении и проверке следственных версий;
- подготовка и проведение следственных действий, выбор при этом наиболее эффективных тактических приемов и средств по расследуемым уголовным делам;
- установление мест нахождения лиц, скрывшихся или скрывающихся от следствия и суда;
- формирование доказательств.

Под планированием расследования понимается сложный мыслительный процесс компетентного лица, заключающийся в определении направленности и задач расследования, способов и средств их решения в рамках закона.

Планирование проводится в течение всего срока предварительного следствия. Следователь разрабатывает план расследования, в котором находят отражение вопросы обеспечения следственных действий имеющимися силами и средствами.

Мы уже упоминали о том, что первоначальный этап расследования характеризуется обычно информационной неопределенностью. Скучность исходных данных зачастую заставляет следователя довольствоваться лишь типичными версиями. Здесь характерно определение круга таких следственных действий, неотложных по своему существу, которые способны расширить доказательственную базу для перехода к следующему этапу расследования. Наряду с такими традиционными следственными действиями, как осмотр места происшествия, допросы очевидцев и других свидетелей, обыски у подозреваемых лиц, на наш взгляд, будет востребовано и электронное наблюдение. Предлагаемое следственное действие будет обеспечивать поступление новой, востребованной информации, необходимой для динамичности расследования и своевременной корректировки составленного плана.

Особое значение в этой связи приобретают вопросы взаимодействия с оперативными подразделениями, определения круга используемых специальных технических средств для контроля требуемой информации, получения с участием специалистов необходимых

образцов голоса для сравнительного исследования и использования результатов фоноскопической экспертизы в расследовании уголовного дела.

Вместе с тем для определения направления расследования следователем могут выдвигаться различные версии, которые позволят развить значение от вероятного (предположительного) к достоверному (истинному) знанию изучаемого события или отдельных его обстоятельств. Именно поэтому они играют роль метода познания в расследовании преступления³⁰.

Для построения версий имеют значение непосредственно установленные следователем обстоятельства, содержащие сведения о событии преступления. Основу их построения составляют факты, полученные в ходе следственных действий, в т. ч. и при проведении электронного наблюдения в отношении подозреваемого и его сообщников. Следователь, просмотрев полученную информацию, может планировать проведение других целенаправленных следственных действий.

Материалы, полученные в ходе проведения электронного наблюдения, облегчат работу следователя в изобличении ложных показаний допрашиваемых лиц, их мотивов (подкуп, шантаж, желание выгородить или смягчить вину подозреваемого или обвиняемого в силу дружеских отношений, боязнь мести со стороны преступника и т. д.), помогут выявить информацию о роли подозреваемого в преступной группе, его связях, убедиться в достоверности его показаний.

Суд может учесть приобретенную информацию в ходе электронного наблюдения для принятия решения об избрании меры пресечения виновному лицу, а также воспринять ее как достаточное основание для проведения других следственных действий, ограничивающих конституционные права подозреваемого и обвиняемого.

Материалы электронного наблюдения могут быть успешно использованы для розыска обвиняемого. Так, следователь, исходя из полученной информации, может:

— моделировать ситуации, вынуждающие разыскиваемого к установлению связей с соучастниками преступления, родствен-

³⁰ Ермолович В. Ф., Ермолович М. В. Построение и проверка версий / Под ред. И. И. Басецкого. Минск, 2000. С. 8.

никами или к посещению заранее известного правоприменительным органам места;

— проводить целенаправленные поисковые мероприятия по ограничению свободы передвижения лица, находящегося в розыске;

— принимать меры, препятствующие сокрытию следов преступления;

— убеждать обвиняемого к явке с повинной с помощью лиц, пользующихся у него авторитетом;

— проводить комплекс следственных и розыскных мероприятий в местах вероятного нахождения или появления обвиняемого.

Решение о возможности использования результатов электронного наблюдения в процессе доказывания принимается следователем. При рассмотрении вопроса об относимости и допустимости результатов предлагаемого следственного действия в качестве доказательств следователем в первую очередь должны учитываться следующие обстоятельства:

— наличие в полученных материалах фактической информации, имеющей отношение к расследуемому уголовному делу;

— указание на источник полученных сведений;

— наличие в сопроводительных документах обязательных реквизитов и подписей должностных лиц, уполномоченных на проведение электронного наблюдения.

Материалы электронного наблюдения могут использоваться в процессе доказывания в качестве самостоятельного источника доказательств и получить свое выражение в одной из следующих форм, предусмотренных УПК РФ:

1) фонограммы телефонных переговоров и других устных разговоров подозреваемого, обвиняемого и других лиц — в качестве вещественных доказательств. Названная форма однозначно предусмотрена действующим законодательством и достаточно подробно освещена во многих работах ученых-юристов³¹;

³¹ См., например: *Быков В. М., Тренбак В. М.* Основания и критерии признания доказательств недопустимыми // *Следователь.* 1998. № 9; *Громов Н. А.* Понятие доказательств в уголовном судопроизводстве // *Государство и право.* 1998. № 3; *Громов Н. А., Пономаренков В. А.* Доказательства и доказывание в уголовном процессе. Самара, 1999; *Доля Е. А.* Использование результатов оперативно-розыскной деятельности в доказывании // *Рос. юстиция.* 1995. № 5; *Карнеева Л. М.* Доказатель-

2) другая фактическая информация, полученная следователем и задокументированная на материальном носителе, — в виде и н ы х документов или вещественных доказательств;

3) при назначении и проведении необходимых видов экспертиз — в форме заключения или показания эксперта. Указанная форма также широко освещена в специальной литературе³².

Поскольку, как мы уже упомянули, первая и третья формы рассмотрены учеными-правоведами достаточно подробно³³, на них мы останавливаться не будем. Обратим более пристальное внимание на формирование доказательств на базе «другой» фактической информации, полученной следователем в ходе проведения электронного наблюдения.

Под другой фактической информацией, полученной следователем, будем понимать любые знаки, сигналы, письменный текст, изображения, звуки или сообщения любого рода, передаваемые по радиосистемам, проводной, оптической и другим электро-

ства и доказывание в уголовном процессе. М., 1995; *Китнис Н. М.* Допустимость доказательств в уголовном судопроизводстве. М., 1995; *Шейфер С. А.* Использование непроцессуальных познавательных мероприятий // *Государство и право.* 1997. № 9.

³² См. об этом: *Арсеньев В. Д.* Истина, достоверность и обоснованность в следствии и судебных актах // *Вопр. теории судебной экспертизы: Сб. науч. тр. ВНИИСЭ.* Вып. 39. М., 1979; *Белкин Р. С.* Собираение, исследование и оценка доказательств. М., 1966; *Эйсман А. А.* Некоторые вопросы исследования вещественных доказательств // *Вопр. криминалистики.* 1962. № 5; *Горских Г. Ф.* Проблемы доказательства в советском уголовном процессе / *Горских Г. Ф., Кокорев Л. Д., Элькин П. С.* Воронеж, 1978; *Давлетов А. А.* Основы уголовно-процессуального познания. Свердловск, 1991; и др.

³³ См. также: *Банин В. А.* К вопросу о предмете и пределах доказывания в советском уголовном процессе // *Проблемы доказательственной деятельности по уголовным делам.* Красноярск, 1987; *Гущин А. Н.* Проблемы использования результатов оперативно-розыскной деятельности в доказывании по уголовному делу / *Гущин А. Н., Николаиченко В. В., Громов Н. А.* Пенза, 1998; *Кузнецов Н. П.* Доказывание в стадии возбуждения уголовного дела. Воронеж, 1983; *Лупинская П. А.* Допустимость доказательств: пора обеспечить единство судебной практики // *Рос. юстиция.* 1998. № 11; *Михеенко М. М.* К вопросу о правовой регламентации оценки доказательств и их источников в советском уголовном процессе // *Актуальные проблемы доказывания в советском уголовном процессе.* М., 1981; и др.

магнитным системам единой сети электросвязи РФ, кроме сети почтовой связи, и не содержащие человеческого голоса³⁴.

Поскольку мы живем в век цифровой техники, при оценке следователем полученной или представленной информации в цифровом виде закономерно возникнет вопрос о ее достоверности. На наш взгляд, нельзя полностью согласиться с мнением Д. Г. Румянцева и Л. Ф. Монастырского, утверждающих, что при переносе информации в память компьютера неизбежно теряются индивидуальные особенности исходной природы данных — остаются только смыслы, стоящие за ними. Определив порог, при определении которого изменения физической величины будут наречены нами единицей, мы тем самым определяем величину информационных потерь и уничтожаем изначально присущую аналоговым данным индивидуальность³⁵. Более адекватный подход состоит в том, что информация в цифровом виде может с любой заранее заданной точностью отражать соответствующую аналоговую информацию.

Отсутствие в настоящее время реальных методик определения подлинности и авторства цифровых сообщений является едва ли не основной проблемой преобразования в доказательства соответствующих данных, полученных в процессе электронного наблюдения.

Важнейшими фактами, которые должны быть выяснены в ходе судебной проверки материалов электронного наблюдения, полученных с использованием специальных технических средств, должны стать участники событий, место, дата и время получения соответствующей информации, а также подлинность данных, зафиксированных на представленных носителях информации, — другими словами, отсутствие умышленных и неумышленных искажений.

Современный уровень развития информатики делает реальной возможность удостоверения подлинности информации, содержащейся на материальном носителе в цифровом виде, полученной с помощью специальных технических средств. Встраивание в названные средства специализированных крипточипов с уникальными секрет-

³⁴ Таким образом, сюда следует отнести пейджинговые, факсимильные сообщения, информацию, продуцируемую персональными компьютерами или переданную в любом стандартном формате по сетям документальной электросвязи (в т. ч. Интернету), видеофайлы, электронную почту, IP-телефонию и т. д.

³⁵ См.: Румянцев Д. Г., Монастырский Л. Ф. Путь программиста. М., 2000.

ными неизменяемыми ключами для каждого устройства при соответствующей нормативной и организационной поддержке принципиально решает проблему обеспечения и проверки подлинности материалов, полученных в ходе электронного наблюдения на современных телекоммуникационных системах передачи информации. Можно прибегнуть к уже хорошо известному в юридической практике понятию электронной цифровой подписи, смысл от этого останется неизменным. При этом предполагается, что для защиты от умышленных искажений данных электронная цифровая подпись формируется на основе двухключевой криптографической системы и соответствующие секретные ключи неизвестны пользователям специальных технических средств³⁶. Дешифрование данных может быть произведено с помощью открытых ключей, значениями которых должен располагать следователь (если он поручал проведение электронного наблюдения субъектам оперативно-розыскной деятельности) или судья. Отметим, что такая технология не решит всех проблем, но позволит гарантированно подтвердить отсутствие модификации сформированного снифером³⁷ сообщения в процессе его регистрации, передачи и представления полученных материалов следователю и в суд.

Если написанные от руки записи различаются, как правило, почерком, то цифровая информация на машинном носителе состоит из длинной цепочки нулей и единиц, которые не указывают на личность автора. Эта проблема присутствует при общении через Интернет, сохраняя авторам электронных писем анонимность. Например, Интернет-технологии гарантируют пользователям анонимность сообщений по электронной почте, а Интернет-чат-каналы позволяют абонентам общаться, не называя своих настоящих имен. Если следователь предъявит подобные материалы обвиняемому, подозреваемому или другому лицу в качестве доказательств, то названные лица, естественно, оспорят названные материалы на предмет их достоверности.

³⁶ Ими могут быть сотрудники оперативно-технических или оперативно-поисковых подразделений субъектов оперативно-розыскной деятельности, специалист или непосредственно следователь (дознатель) при проведении электронного наблюдения.

³⁷ *Снифер* — прибор контроля информации.

Косвенные доказательства обычно могут предоставить ключ к установлению авторства анонимного сообщения, а также подлинности компьютерной записи.

В качестве примера хотелось бы привести дело Simpson, рассмотренное одним из федеральных судов США³⁸. Обвинитель по этому делу стремился показать, что ответчик общался с агентом Федерального бюро расследования, работающим под прикрытием, по Интернет-чату и темой переписки была детская порнография. Сотрудники правоприменительных органов предоставили распечатку данного разговора, происходившего в Интернет-чате между агентом и лицом, которое было идентифицировано как Stavron, и хотели доказать, что Stavron — это и есть ответчик. Окружной суд принял эту распечатку в качестве доказательства. В апелляции, последовавшей за обвинительным приговором, Simpson оспорил этот момент: поскольку правительственные сотрудники не могли доказать, что сообщения были написаны его почерком или записаны его голосом, то данная распечатка не является подлинной и ее нужно исключить из списка представленных доказательств.

Десятая выездная сессия Окружного суда отклонила этот аргумент, отметив значимость косвенных доказательств в том, что Stavron является ответчиком. Так, Stavron сообщил агенту под прикрытием, что его настоящее имя — это В. Simpson. Он также назвал данному агенту свой домашний адрес, который соответствовал адресу Simpson's и, как оказалось в ходе дальнейшего расследования, получал доступ в Интернет со счета, зарегистрированного на Simpson. Далее полиция обнаружила записи в доме Simpson's, в которых были указаны имя, адрес и телефонный номер, которые агент, работающий под прикрытием, послал Stavron. Суд признал, что сотрудники правоприменительных органов, расследовавших данное дело, предоставили достаточные доказательства для подтверждения того, что ответчиком является Stavron и что распечатка была подлинной³⁹.

³⁸ USA, v. Simpson, 152 F.3d 1241 (10th Cir. 1998).

³⁹ См. также: USA, v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000), где делается вывод, что Окружной суд надлежащим образом принял к рассмотрению распечатку из Интернет-чата при обстоятельствах, сходных с теми, которые были приведены в деле Simpson; USA, v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000), где было вынесено решение, что сообщения по электронной почте были должным образом удостоверены, когда они включали электронный адрес ответчика, его псевдоним и время, когда он после получения данных сообщений перезванивал по указанному в сообщении адресу.

В Российской Федерации пока подобной судебной практики нет. Представляется, что проведение электронного наблюдения на современных средствах связи в рамках предлагаемого следственного действия стимулирует законодателя к разрешению обозначенных проблем в области цифровой информации.

С точки зрения теории доказательств основными вопросами, требующими своего осмысления в русле данной проблемы, являются следующие:

— К какому виду доказательств может быть отнесена информация в электронном виде?

— Каким процессуальным способом может быть введена такая информация в уголовное дело?

Ответ уже приводился выше:

— В качестве вещественных доказательств и иных документов.

— Способом проведения электронного наблюдения в рамках предлагаемого следственного действия.

Разграничение этих двух видов доказательств требует учета специфики электронного документа. На сегодня понятие электронного документа в российском уголовном (и не только) процессе отсутствует (или нечетко определено), что приводит к необходимости его разработки (уточнения)⁴⁰. Названный документ, как правило, имеет ряд характерных черт, не позволяющих рассматривать его как аналог бумажного документа. В подтверждение этому можно привести несколько тезисов, перечисляющих особенности электронного документа:

- отсутствие жесткой привязки к носителю, точнее говоря, один и тот же документ может существовать на разных носителях, оставаясь при этом аутентичным;

- к нему неприменимо сочетание таких терминов, как оригинал и копия: если мы согласимся с тем, что электронный документ —

⁴⁰ По всей вероятности, первым юридическим актом в нашей стране, который регулировал вопросы использования электронного документа в судебном разбирательстве, были Инструктивные указания Государственного арбитража СССР от 29 июня 1979 года № И-1-4 «Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронной вычислительной техники» // Сб. инструктив. указаний Гос. арбитража СССР. 1983. С. 92—94.

это файл, состоящий из набора «0» и «1», то и копия будет состоять точно из такого же порядкового набора цифровых символов; таким образом, понятие оригинала электронного документа столь же некорректное, как и масса мыслительного образа;

- аутентичность, достоверность документа может быть подтверждена криптографическим кодом, который ничего общего не имеет с последовательностью символов, соответствующих изображениям печати или визирования.

Электронный документ как вещественное доказательство может характеризоваться следующими параметрами:

- с какого именно компьютера была изготовлена и передана задокументированная информация, полученная в ходе проведения электронного наблюдения: его местонахождение⁴¹, принадлежность, круг лиц, имеющих к нему доступ;

- какие программные средства установлены на данном компьютере и использованы для формирования и передачи интересующей нас информации (операционные системы, программное обеспечение и т. п.);

- включен ли рассматриваемый компьютер в какую-либо сеть (локальную, региональную, федеральную, трансконтинентальную) или работает в автономном режиме;

- в каком формате изготовлена и передана информация, полученная в ходе электронного наблюдения;

- в каком файле, каталоге, диске компьютера хранится переданное электронное сообщение (документ) (точнее, каков путь к этому файлу: сеть — компьютер — диск — каталог — файл), наименование всех этих компонентов, присвоенных ему пользователем;

- дата создания переданного файла и внесения в него изменений;

- характеристика указанного файла (обычный, скрытый, архивный, только для чтения, закрытый паролем от несанкционированного доступа к нему) и т. д.

Как полагает А. С. Золотарев, «...если хотя бы один из названных параметров значим для дела, то этот электронный документ

⁴¹ Как правило, определяется по присвоенному компьютеру IP-адресу.

должен быть признан вещественным доказательством»⁴². Его мнение, на наш взгляд, заслуживает внимания.

Вопрос об отграничении документов — вещественных доказательств от иных документов является самостоятельной научной проблемой.

Интересно мнение К. Б. Калиновского и Т. Ю. Маркеловой, утверждающих, что для признания электронного или бумажного документа вещественным доказательством необходимо выполнение двух условий. Во-первых, зафиксированная в документе информация должна указывать на преступление как «главный факт» в предмете доказывания (а не на причины и условия, способствовавшие совершению преступления, характеристику личности обвиняемого, размер ущерба, подлежащего возмещению). Во-вторых, информация в документе — вещественном доказательстве должна быть объективной, т. е. такой, которая напрямую отражает преступление.

Другими словами, информация не должна быть следствием восприятия из памяти: сознание человека не должно быть промежуточным носителем информации. Например, заведомо ложное сообщение об акте терроризма, размещенное в Интернете, будучи приобщенным к уголовному делу в виде распечатки, магнитного носителя, фотографии или видеозаписи, станет вещественным доказательством.

В практике бывает недостаточно двух вышеназванных критериев для отграничения документов от вещественных доказательств. Поэтому неустранимые сомнения следует толковать в пользу вещественного доказательства, имеющего более строгую процессуальную форму.

Важно отметить, что первоисточником вещественного доказательства является сам предмет, отразивший искомое событие (факт сообщения об акте терроризма). Следовательно, для решения вопроса о допустимости электронного документа в качестве вещественного доказательства необязательно знать автора

⁴² Золотарев А. С. Процессуальные аспекты использования компьютерной информации в доказательственной деятельности // Информ. о-во: право и власть: Сб. науч. ст. Екатеринбург, 2001. С. 69.

документа. Установление автора будет целью дальнейшего процесса доказывания.

В отличие от вещественного доказательства иной документ имеет своим первоисточником сознание человека. Поэтому известность автора — это минимальное требование к иному документу⁴³.

Верховный суд ФРГ, например, под документом в смысле уголовно-процессуального права понимает любой предмет, на котором зафиксирована мысль посредством письменных знаков⁴⁴. Применительно к другим материалам электронного наблюдения можно утверждать, что задокументированная и истребованная или приобретенная дознавателем, следователем или прокурором информация, полученная в рамках предлагаемого следственного действия, может быть зафиксирована как в письменном, так и в ином виде (надо полагать, и в форме электронного документа). К «иному виду» можно отнести видеофайлы и другую информацию, не содержащую человеческого голоса, истребованную или полученную в названном порядке.

Письменный документ, запись или фотография признаются подлинными, если представлены их оригиналы. Как же быть с информацией, получаемой в цифровом виде? Если сделать распечатку данной информации, будет ли она считаться подлинной? Мы уже не раз говорили, что оригинал файла есть просто набор цифр 0 и 1; в отличие от этого распечатка является результатом манипуляций, проведенных с ним сложных серий электронных и механических процессов. На наш взгляд, на этот вопрос следует отвечать положительно. Строго говоря, оригиналом фотографии является негатив, а если пойти еще дальше, то непроявленный негатив. Мы же признаем в качестве оригинала позитивный отпечаток, и это ни у кого не вызывает возражений. Точно так же практические цели испол-

⁴³ См. об этом: *Калиновский К. Б., Маркелова Т. Ю.* Доказательственное значение «электронной» информации в российском уголовном процессе // *Рос. следователь.* 2001. № 6. С. 18—19.

⁴⁴ См.: *Громов Н. А., Гуцин А. Н.* Проблемы интерпретации оперативно-розыскных данных в качестве доказательств // *Профессионал: Науч.-прав. альманах МВД России.* 1999. № 5. С. 27—29.

зования согласуются с положением об оригинале в отношении любой распечатанной информации.

Роль и значение электронного наблюдения при ведении дел, связанных с организованной преступностью, вымогательством, незаконным изготовлением, приобретением, хранением, перевозкой, пересылкой либо сбытом наркотических средств или психотропных веществ, а также коррупцией среди государственных чиновников, невозможно переоценить. Приведенный американский опыт свидетельствует о том же.

Ю. К. Орлов полагает, что «...опыт далекой заокеанской страны (США) со своей историей, сложившейся и четко работающей правоохранительной и судебной системами, высококвалифицированными кадрами и, наконец, со своим менталитетом меньше всего подходит для российской действительности»⁴⁵. В какой-то степени это, безусловно, так. Но предлагаемое оперативно-техническое мероприятие и следственное действие и не пытаются его копировать. Они учитывают реальность сегодняшнего дня именно в России.

В настоящее время прослушивание и электронное наблюдение по уголовным делам узаконено во многих странах, что отнюдь не случайно: оно стало очень доступным в техническом отношении. И поэтому нельзя ставить правоприменительные органы в неравные условия по сравнению с преступниками. Нам представляется, что электронное наблюдение возможно в строго ограниченных законом рамках.

⁴⁵ *Орлов Ю. К.* Основы теории доказательств в уголовном процессе. М., 2000. С. 19.

ЗАКЛЮЧЕНИЕ

Понятие электронное наблюдение по своему содержанию намного шире, чем понятие системы технических средств по обеспечению оперативно-розыскных мероприятий, или отдельно взятых видов оперативно-розыскных мероприятий (прослушивание телефонных переговоров и снятие информации с технических каналов связи), контроля и записи переговоров как следственного действия. Оно их объединяет, консолидирует, учитывает все их нюансы и особенности на основе единой категории — информации.

Под электронным наблюдением следует понимать совокупность последовательно осуществляемых действий, выполняемых уполномоченным государственным органом в пределах своей компетенции на проведение следственных действий или/и оперативно-розыскной деятельности на основании судебного решения по снятию информации, передаваемой в форме любого излучения, передаче или приему знаков, сигналов, голосовой информации, письменного текста, изображений, звуков или сообщений любого рода по радиосистеме, проводной, оптической и другим электромагнитным системам.

Введение подобного понятия в УПК РФ существенно расширило бы возможности следователя или органа дознания на получение информации, имеющей значение для уголовного дела как на первоначальном, так и на последующих этапах расследования.

В Федеральном законе «Об оперативно-розыскной деятельности» данное определение реально отражало бы ту совокупность оперативно-розыскных мероприятий, которые охватываются в первую очередь системой технических средств по обеспечению оперативно-розыскных мероприятий, а также прослушиванием телефонных переговоров и снятием информации с технических каналов связи. Кроме того, создало бы правовую базу упомянутой системы на уровне федерального закона, исключив ведомственное нормотворчество.

Следует объединить прослушивание телефонных переговоров и контроль технических каналов связи в одно оперативно-техническое мероприятие с учетом имеющихся наработок в области системы технических средств по обеспечению оперативно-розыскных мероприятий. Для этого дополнить ст. 6 Федерального закона «Об оперативно-розыскной деятельности» новым оперативно-розыскным мероприятием «электронное наблюдение», исключив два вышеназванных.

Электронное наблюдение — комплексное оперативно-техническое мероприятие, проводимое на основании судебного решения и заключающееся в конспиративном получении оперативно-техническими подразделениями субъектов оперативно-розыскной деятельности фактической или оперативно-значимой информации с помощью специальных технических средств, фиксирующих и копирующих названную информацию во время ее передачи объектами оперативной заинтересованности через единые сети электросвязи Российской Федерации.

Предлагаемое содержание электронного наблюдения как нового вида оперативно-технического мероприятия позволит четче определить границы таких оперативно-технических мероприятий, предусмотренных Федеральным законом «Об оперативно-розыскной деятельности», как контроль почтовых отправлений, телеграфных и иных сообщений, а также наблюдение. Электронная составляющая наблюдения должна быть поглощена предлагаемым видом оперативно-технического мероприятия.

Предлагается закрепить в ч. 3 ст. 6 Федерального закона «Об оперативно-розыскной деятельности» общее определение системы технических средств по обеспечению оперативно-розыскных мероприятий как одной из составляющих предлагаемого оперативно-технического мероприятия «электронное наблюдение».

В связи с этим **часть 3 статьи 6** Федерального закона «Об оперативно-розыскной деятельности» необходимо изложить в следующей редакции:

В ходе проведения оперативно-розыскных мероприятий используются информационные системы, системы технических средств по обеспечению оперативно-розыскных мероприятий, видео- и аудио-запись, кино- и фотосъемка, а также другие технические и иные

средства, не наносящие ущерба жизни и здоровью людей и не причиняющие вреда окружающей среде.

Система технических средств по обеспечению оперативно-розыскных мероприятий является одной из составляющих электронного наблюдения и входит в состав аппаратных и программных средств дополнительного оборудования стационарной аппаратуры средств связи, независимо от их формы собственности и ведомственной принадлежности.

Статью 89 УПК РФ изложить в следующей редакции:

1. Результаты оперативно-розыскной деятельности являются источником фактических данных и могут быть приобщены к уголовному делу в качестве доказательств в соответствии с требованиями уголовно-процессуального закона.

2. Представление результатов оперативно-розыскной деятельности органу дознания, следователю, прокурору или в суд осуществляется на основании постановления руководителя органа, осуществляющего оперативно-розыскную деятельность, и означает передачу в установленном законодательством Российской Федерации порядке оперативно-служебных документов, предметов, которые могут быть приобщены к уголовному делу.

Инициатива в получении результатов оперативно-розыскной деятельности может исходить от органов предварительного расследования или суда.

3. Перед представлением материалов оперативно-розыскной деятельности сведения, содержащие государственную тайну, подлежат рассекречиванию на основании мотивированного постановления руководителя органа, осуществляющего оперативно-розыскную деятельность, либо представляются в порядке и в соответствии с законом.

4. Результаты оперативно-розыскной деятельности могут быть представлены следователю, прокурору или в суд в виде справки-меморандума, в которой излагается полученная информация в обоб-

щенном виде или в виде подлинников соответствующих оперативно-служебных документов.

Представляемые материалы должна сопровождать информация о времени, месте и обстоятельствах изъятия в ходе оперативно-розыскной деятельности предметов и документов, получения видео- и аудиозаписей, кино- и фотоматериалов, копий и слепков, должно быть приведено описание индивидуальных признаков указанных предметов и документов.

Предлагается предусмотреть в уголовно-процессуальном законе новое следственное действие, включающее в себя также контроль и запись переговоров, восполнив имеющиеся в законодательстве пробелы.

С этой целью следует изменить наименование **статьи 186 УПК РФ** и изложить ее в следующей редакции:

ПРОВЕДЕНИЕ ЭЛЕКТРОННОГО НАБЛЮДЕНИЯ

1. При наличии достаточных оснований полагать, что телефонные и устные переговоры подозреваемого, обвиняемого и других лиц, любая другая информация, передаваемая ими по сетям электро-связи общего пользования и присоединенным к названной сети выделенным или технологическим сетям связи, могут содержать сведения, имеющие значение для уголовного дела, ее документирование, фиксация на материальном носителе и оценка допускаются при производстве по уголовным делам средней тяжести, тяжким, особо тяжким преступлениям только на основании судебного решения, принимаемого в порядке, установленном ст. 165 настоящего Кодекса.

2. В случае возникновения угрозы жизни, здоровью, собственности потерпевшего, свидетеля или их близких родственников, родственников, близких лиц проведение электронного наблюдения допускается на основании постановления следователя, по заявлению или с согласия в письменной форме указанных лиц, с обязательным уведомлением судьи в течение 24 часов, а при отсутствии такого заявления — на основании судебного решения.

3. В ходатайстве следователя о проведении электронного наблюдения указывается:

— уголовное дело, при производстве которого необходимо применение данной меры;

— основания, по которым производится данное следственное действие;

— фамилия, имя, отчество лица, чьи телефонные, устные переговоры, любая другая информация документируются. Для уточнения круга лиц, подозреваемых в совершении преступления, допускается указание нумерации средства связи без приведения установочных данных пользующихся им лиц;

— срок проведения электронного наблюдения;

— наименование органа дознания и/или оператора связи, которому поручается техническое осуществление электронного наблюдения.

4. Постановление о проведении электронного наблюдения направляется следователем для исполнения в соответствующий орган дознания и/или оператору связи.

5. Оператор связи на основании судебного решения, а в случаях, указанных в части второй настоящей статьи, — на основании постановления прокурора, следователя или руководителя органа дознания обязан обеспечить содействие прокурору, следователю или дознавателю и не вправе разглашать информацию о факте проведения расследования абоненту или другому лицу.

Прокурор, следователь или дознаватель предупреждают оператора связи о недопустимости разглашения ставших известными ему данных предварительного расследования, о чем у него берется подписка с предупреждением об ответственности в соответствии со ст. 310 УК РФ.

На основании решения суда оператор связи должен незамедлительно предоставить следователю всю необходимую информацию, оборудование и техническую помощь в течение срока действия судебного решения.

Оператору связи, предоставляющему оборудование или техническую помощь следователю, в соответствии с данной статьей может быть предоставлена компенсация за обоснованные расходы, понесенные им при предоставлении этого оборудования или помощи.

6. Проведение электронного наблюдения может быть установлено на срок до 180 суток. Оно прекращается по постановлению следователя, если необходимость в данной мере отпадает, но не позднее окончания предварительного расследования по данному уголовному делу.

7. Следователь в течение всего срока проведения электронного наблюдения вправе в любое время истребовать от органа дознания или оператора связи, его осуществляющего, фонограмму или иную информацию для осмотра и прослушивания. Она передается следователю в печатанном виде с сопроводительным письмом, в котором должны быть указаны дата и время начала и окончания проведения электронного наблюдения и краткие характеристики использованных при этом технических средств.

8. О результатах осмотра и прослушивания фонограммы или иной информации, полученной в ходе проведения электронного наблюдения, следователь с участием понятых и, при необходимости, специалиста составляет протокол, в котором должна быть дословно изложена та часть фонограммы или иная информация, которые, по мнению следователя, имеют отношение к данному уголовному делу. Лица, участвующие в осмотре и прослушивании фонограммы, осмотре иной предоставленной информации, вправе в том же протоколе или отдельно изложить свои замечания к протоколу.

9. Фонограмма или иная информация в полном объеме приобщаются к материалам уголовного дела на основании постановления следователя в качестве вещественного доказательства или иного документа и хранятся в печатанном виде в условиях, исключающих возможность прослушивания и тиражирования указанных объектов посторонними лицами и обеспечивающих их сохранность и техни-

ческую пригодность для повторного прослушивания или предъявления, в том числе в судебном заседании.

Иная информация, полученная в ходе электронного наблюдения и обладающая признаками, указанными в части первой статьи 81 настоящего Кодекса, признается вещественным доказательством.

Необходимо внести соответствующие изменения в образцы процессуальных документов, приведенных в приложениях 89, 90, 91 ст. 476 и в приложении 11 ст. 477 УПК РФ, с учетом предлагаемого следственного действия.

Назрела необходимость дальнейшего совершенствования уголовно-процессуального и оперативно-розыскного законодательства и с точки зрения оптимизации процесса использования информации, полученной в ходе проведения электронного наблюдения.

Предстоит еще многое сделать, чтобы электронное наблюдение было поставлено в строгие рамки закона, не нарушая прав и свобод граждан ни при каких обстоятельствах. По словам директора уголовной полиции одной из земель ФРГ г-на Питржика, «тот, кто ожидает от следственных органов успехов, достижимых в принципе только конспиративными методами, должен быть готов отстаивать и требования их правовой оправданности даже в случае исчерпания определенных законами возможностей. В этой необходимости должны быть убеждены не только политики, но в первую очередь прокуроры и судьи»¹. Добавим от себя: без этого невозможна гуманизация норм процессуального права и обеспечение задач правосудия.

¹ Цит. по: Гесснер Р., Херцог У. За фасадом права: Методы новой тайной полиции. М., 1990. С. 51.

ПРИЛОЖЕНИЯ

Приложение 1

Проект приложения № 89 к ч. 6 ст. 476 УПК РФ

(Согласен, Не согласен)

Прокурор _____
(Наименование органа прокуратуры,

классный чин, фамилия, инициалы прокурора)

(Подпись)

«__» _____ Г.

ПОСТАНОВЛЕНИЕ О ВОЗБУЖДЕНИИ ПЕРЕД СУДОМ ХОДАТАЙСТВА О ПРОВЕДЕНИИ ЭЛЕКТРОННОГО НАБЛЮДЕНИЯ

«__» _____ Г.

(Место составления)

Следователь (дознатель)

(Наименование органа предварительного следствия или дознания,

классный чин или звание, фамилия, инициалы следователя (дознателя))

Рассмотрев материалы уголовного дела № _____,
установил:

(Излагаются основания проведения электронного наблюдения)

На основании изложенного и руководствуясь ст. 186 УПК РФ,
постановил:

1. Ходатайствовать перед судом _____ о проведении
(Наименование суда)
электронного наблюдения _____
(Фамилия, имя, отчество лица, в отношении которого проводится электронное наблюдение)
сроком на ____ суток

(Указать средство связи, подлежащее электронному наблюдению*)

2. Техническое осуществление электронного наблюдения поручить

(Наименование правоприменительного органа и/или оператора связи)

Следователь (дознатель) _____
(Подпись)

Приложение 2

Проект приложения № 90 к ч. 6 ст. 476 УПК РФ

ПОСТАНОВЛЕНИЕ О ПРЕКРАЩЕНИИ ЭЛЕКТРОННОГО НАБЛЮДЕНИЯ

_____ «__» _____ г.
(Место составления)

Следователь _____
(Наименование органа предварительного следствия или дознания,

_____,
классный чин или звание, фамилия, инициалы следователя)

Рассмотрев материалы уголовного дела № _____,
установил:

* Для уточнения круга лиц, подозреваемых в совершении преступления, или их сообщников допускается указание нумерации оконечного оборудования связи без приведения установочных данных пользующихся им лиц.

(Когда, на основании решения какого суда начато проведение электронного

наблюдения, причины его прекращения: *Отпала необходимость*

в данной мере, Оканчивается предварительное расследование)

На основании изложенного и руководствуясь ч. 6 ст. 186 УПК РФ,
постановил:

1. Прекратить проведение электронного наблюдения

(Фамилия, имя, отчество лица, в отношении которого проводилось электронное наблюдение)

2. Настоящее постановление направить для исполнения

(Наименование органа дознания и/или оператора связи)

Следователь _____
(Подпись)

Приложение 3

Проект приложения № 91 к ч. 6 ст. 476 УПК РФ

ПРОТОКОЛ ОСМОТРА, ПРОСЛУШИВАНИЯ ФОНОГРАММЫ ИЛИ ИНОЙ ИНФОРМАЦИИ, ПОЛУЧЕННОЙ В ХОДЕ ПРОВЕДЕНИЯ ЭЛЕКТРОННОГО НАБЛЮДЕНИЯ

_____ «__» _____ г.
(Место составления)

Осмотр и прослушивание начаты в ____ ч ____ мин
Осмотр и прослушивание окончены в ____ ч ____ мин

Следователь (дознатель)

(Наименование органа предварительного следствия или дознания,

_____,
классный чин или звание, фамилия, инициалы следователя/дознателя)

в присутствии понятых:

1. _____
(Фамилия, имя, отчество и место жительства понятого)

2. _____
(Фамилия, имя, отчество и место жительства понятого)

с участием _____
(Процессуальное положение, фамилия, имя, отчество,

а при необходимости — адрес и иные данные о личности каждого из участвующих лиц)

в соответствии с ч. 8 ст. 186 УПК РФ в помещении _____

(Каком именно)

произвел осмотр и/или прослушивание _____
(Чего именно)

Перед началом осмотра и прослушивания фонограммы или иной информации, полученной в ходе проведения электронного наблюдения, участвующим лицам разъяснены их права, ответственность, а также порядок производства осмотра и прослушивания фонограммы или иной информации.

Понятым до начала осмотра и прослушивания фонограммы или иной информации, полученной в ходе проведения электронного наблюдения, разъяснены их права, обязанности и ответственность, предусмотренные ст. 60 УПК РФ.

(Подпись первого понятого)

(Подпись второго понятого)

Специалисту (эксперту) _____
(Фамилия, имя, отчество)

разъяснены его права, обязанности и ответственность, предусмотренные ст. 58 (57) УПК РФ.

(Подпись специалиста/эксперта)

Иные участвующие лица: _____
(Подпись)

(Подпись)

Участвующим лицам также объявлено о применении технических средств _____
(Каких именно, кем именно)

Осмотр и прослушивание фонограммы или иной информации производились в условиях _____
(Освещенность, звукоизоляционные характеристики помещения,

в котором производится осмотр и прослушивание фонограммы или иной информации,

аппаратура, на которой прослушивалась фонограмма или осматривалась иная информация)

Осмотром и прослушиванием фонограммы или иной информации установлено:

(Отмечается наличие и целостность упаковки и печатей,

указываются индивидуальные признаки осматриваемой фонограммы или иной информации,

кроме того, дословно излагается полностью или та часть фонограммы или иной информации,

которая, по мнению следователя, имеет отношение к данному уголовному делу)

В ходе осмотра проводилась _____
(Видео-, аудиозапись и т. п.)

По окончании осмотра и прослушивания фонограмма или иная информация _____
(Какая)

опечатана _____
(Какой печатью)

К протоколу осмотра прилагаются _____
(Схемы, фототаблицы и другие аудио- и видеоматериалы)

Перед началом, в ходе, либо по окончании осмотра и прослушивания фонограммы или иной информации от участвующих лиц

(Процессуальное положение, фамилии, инициалы)

заявления _____.
(Поступили, Не поступили)

Содержание заявления _____

Проект приложения № 11
к ч. 6 ст. 477 УПК РФ

ПОСТАНОВЛЕНИЕ
О РАЗРЕШЕНИИ ПРОВЕДЕНИЯ ЭЛЕКТРОННОГО НАБЛЮДЕНИЯ

«__» _____ г.

(Место составления)

Судья _____
(Наименование суда, фамилия, инициалы судьи)

с участием прокурора _____
(Наименование органа прокуратуры, фамилия, инициалы прокурора)

при секретаре _____,
(Фамилия, инициалы)

а также _____
(Процессуальное положение, фамилии, инициалы иных участников)

рассмотрел постановление прокурора, следователя (дознавателя)

(Наименование органа прокуратуры, органа предварительного следствия
или дознания; фамилии, инициалы)

о возбуждении ходатайства о проведение электронного наблюдения

(Фамилия, имя, отчество)

по уголовному делу № _____.

Проверив представленные материалы, заслушав мнение прокурора _____, следователя (дознавателя) _____,
(Фамилия, инициалы) (Фамилия, инициалы)

установил:

(Излагаются суть ходатайства прокурора, следователя (дознавателя),

а также основания принимаемого судебного решения)

На основании изложенного и руководствуясь ст. 165 и 186 УПК РФ, **постановил:**

1. _____

(Разрешить, Отказать в удовлетворении ходатайства о проведение электронного наблюдения)

Поняты: _____
(Подпись)

(Подпись)

Специалист (эксперт) _____
(Подпись)

Иные участвующие лица: _____
(Подпись)

(Подпись)

Протокол прочитан лично или вслух следователем (дознавателем).

Замечания к протоколу _____
(Содержание замечаний, указание на желание лица,

участвующего в осмотре и прослушивании фонограммы или иной информации,

изложить свои замечания к протоколу отдельно, отсутствие замечаний)

Поняты: _____
(Подпись)

(Подпись)

Специалист (эксперт) _____
(Подпись)

Иные участвующие лица: _____
(Подпись)

(Подпись)

Настоящий протокол составлен в соответствии со ст. 166, 167 и 186 УПК РФ.

Следователь _____
(Подпись)

СПИСОК ЛИТЕРАТУРЫ

_____*.
(Фамилия, имя, отчество лица, в отношении которого проводится электронное наблюдение)

(Указать средство связи**, подлежащее электронному наблюдению)
сроком на ____ суток, начиная с « ____ » ____ г. по « ____ » ____ г.
2. Техническое осуществление электронного наблюдения воз-
ложить на _____.
(Наименование органа дознания и/или оператора связи)

Настоящее постановление может быть обжаловано
в _____
(Наименование вышестоящего суда)

в течение 10 суток со дня его вынесения.

Судья _____
(Подпись)

* Для уточнения круга лиц, подозреваемых в совершении преступления, или их сообщников допускается указание нумерации оконечного оборудования связи без приведения установочных данных пользующихся им лиц.

** Данная графа заполняется в случае принятия судебного решения о разрешении проведения электронного наблюдения.

Нормативно-правовые акты и документы Российской Федерации

Закон Российской Федерации от 21 июля 1993 года № 5473-1 «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы» // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1993. № 33. Ст. 1316.

Закон Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне» // Рос. газ. 1993. 21 сент.

Закон Российской Федерации от 5 марта 1992 года № 2446-1 «О безопасности» // Рос. газ. 1992. 6 мая.

Закон РСФСР от 18 апреля 1991 года «О милиции» № 1026-1 // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1991. № 16. Ст. 503.

Инструкция «О порядке предоставления результатов оперативно-розыскной деятельности органу дознания, следователю, прокурору или в суд». Утв. Приказом Федеральной службы налоговой полиции России, Федеральной службы безопасности России, Министерства внутренних дел России, Федеральной службы охраны России, Федеральной пограничной стражи России, Государственного таможенного комитета России, Службы внешней разведки России от 13 мая 1998 года № 175/226/336/201/410/56 // Бюл. норматив. актов федеральных органов исполнительной власти. 1998. № 23. С. 86—92.

Конституция Российской Федерации // Рос. газета. 1993. 25 дек.

Концепция судебной реформы в Российской Федерации. М., 1992.

Основы уголовного судопроизводства Союза ССР и союзных республик // Ведомости Съезда народных депутатов СССР и Верховного Совета СССР. 1990. № 26. Ст. 495.

Перечень сведений конфиденциального характера. Утв. Указом Президента Российской Федерации от 6 марта 1997 года № 188 // Рос. газ. 1997. 14 марта.

Письмо первого заместителя Минсвязи РФ руководителям организаций и операторам связи от 30 апреля 1996 года № 2259 «О взаимодействии с органами, осуществляющими оперативно-розыскную деятельность» (официально не опубликовано).

Постановление правительства Москвы от 28 января 2003 года № 51-ПП «Об итогах реализации программы “Мой двор, мой подъезд” в 2002 году и задачах на 2003 год» [Электрон. ресурс]. Режим доступа: <http://www.uvao.ru/news>.

Постановление Правительства РФ от 15 сентября 1999 года № 1040 «О мерах по противодействию терроризму» // Собр. законодательства РФ. 1999. № 38. Ст. 4550.

Постановление Совета Федерации Федерального собрания РФ от 4 сентября 1998 года № 392-СФ «Об информации и. о. министра внутренних дел РФ и директора Федеральной службы безопасности России о криминогенной обстановке в Российской Федерации, принимаемых мерах по укреплению законности, пресечению фактов коррупции и проникновения криминальных элементов в органы государственной власти» // Собр. законодательства РФ. 1998. № 37. Ст. 4553.

Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность. Утв. Постановлением Правительства РФ от 27 августа 2005 года № 538 // Рос. газ. 2005. 2 сент.

Приказ Госкомсвязи РФ от 20 апреля 1999 года № 70 «О технических требованиях к системе технических средств для обеспечения функции оперативно-розыскных мероприятий на сетях электросвязи РФ». Прил.: 1. Технические требования к системе по обеспечению функции оперативно-розыскных мероприятий на сетях подвижной радиотелефонной связи; 2. Технические требования к системе технических средств по обеспечению функции оперативно-розыскных мероприятий на сетях персонального радиовызова общего пользования; 3. Технические требования к каналам обмена информацией между системой технических средств по обеспечению оперативно-розыскных мероприятий и пультом управления для сетей подвижной радиотелефонной связи; 4. Технические требования к системе технических средств по обеспечению функции оперативно-розыскных мероприятий на электронных телефонных станциях; 5. Технические требования к каналам обмена информацией между системой технических средств по обеспечению оперативно-розыскных мероприятий и пультом управления на электронных телефонных станциях // Связь-информ. 1999. № 6.

Приказ МВД России от 28 декабря 1994 года № 437 «Об утверждении Инструкции о порядке использования полиграфа при опросе граждан» // Бюл. текущего законодательства МВД. Вып. 13. М., 1995. С. 46—49.

Приказ Министерства РФ по связи и информатизации от 25 июля 2000 года № 130 «О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования» // Рос. газ. 2000. 29 авг.

Приказ Минсвязи России от 24 июня 1992 года № 226 «Об использовании средств связи для обеспечения оперативно-розыскных мероприятий Министерства безопасности РФ» [Электрон. ресурс]. Режим доступа: <http://www.svscons.ru/normdok>.

Приказ Минфина России от 30 ноября 2001 года № 103-н «Об утверждении Положения о порядке финансирования за счет средств федерального бюджета оперативно-розыскных мероприятий» // Рос. газ. 2002. 12 янв.

Распоряжение префекта Юго-Восточного административного округа г. Москвы от 28 февраля 2003 года № 364 «Об итогах реализации программы “Мой двор, мой подъезд” на территории юго-восточного административного округа в 2002 году и задачах на 2003 год» [Электрон. ресурс]. Режим доступа: <http://www.uvao.ru/news>.

Решение Государственной комиссии по электросвязи при Государственном комитете РФ по телекоммуникациям от 29 сентября 1999 года № 63 (официально не опубликовано).

Уголовно-исполнительный кодекс Российской Федерации // Собр. законодательства РФ. 1997. № 2. Ст. 198.

Уголовно-процессуальный кодекс Российской Федерации // Собр. законодательства РФ. 2001. № 52. Ст. 4921.

Уголовный кодекс Российской Федерации // Собр. законодательства РФ. 1996. № 25. Ст. 2954.

Указ Президента РФ от 1 сентября 1995 года № 891 «Об упорядочении организации и проведения ОРМ с использованием технических средств» // Собр. законодательства РФ. 1999. № 24. Ст. 2954.

Указ Президента РФ от 18 апреля 1996 года № 567 «О координации деятельности правоохранительных органов по борьбе с преступностью» // Собр. законодательства РФ. 1996. № 17. Ст. 1958.

Указ Президента РФ от 30 ноября 1995 года № 1203 «Перечень сведений составляющих государственную тайну» // Собр. законодательства РФ. 1995. № 49. Ст. 4775.

Федеральный закон от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности» // Рос. газ. 1995. 18 авг.

Федеральный закон от 17 июля 1999 года № 176-ФЗ «О почтовой связи» // Собр. законодательства РФ. 1997. № 35. Ст. 4136.

Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» // Собр. законодательства РФ. 1995. № 8. Ст. 609.

Федеральный закон от 27 мая 1996 года № 57-ФЗ «О государственной охране» // Собр. законодательства РФ. 1996. № 22. Ст. 2594.

Федеральный закон от 29 декабря 1994 года № 77-ФЗ «Об обязательном экземпляре документов» // Рос. газ. 1995. 17 янв.

Федеральный закон от 29 декабря 1994 года № 78-ФЗ «О библиотечном деле» // Собр. законодательства РФ. 1995. № 1. Ст. 2.

Федеральный закон от 3 апреля 1995 года № 40-ФЗ «Об органах федеральной службы безопасности в Российской Федерации» // Рос. газ. 1995. 12 апр.

Федеральный закон от 4 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене» // Собр. законодательства РФ. 1996. № 28. Ст. 3347.

Федеральный закон от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» // Рос. газ. 2001. 9 авг.

Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи» // Рос. газ. 2003. 10 июля.

Федеральный закон от 8 января 1998 года № 3-ФЗ «О наркотических средствах и психотропных веществах» // Соб. законодательства РФ. 1998. № 2. Ст. 219.

Федеральный конституционный закон от 23 июня 1999 года № 1-ФКЗ «О военных судах РФ» // Собр. законодательства РФ. 1999. № 26. Ст. 3170.

Судебные решения

Инструктивные Указания Государственного Арбитража СССР от 29 июня 1979 года № И-1-4 «Об использовании в качестве доказательств по арбитражным делам документов, подготовленных с помощью электронной-вычислительной техники» // Сб. инструктив. указаний Государственного арбитража СССР. 1983. С. 92—94.

Определение Конституционного Суда РФ от 02 октября 2003 года № 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”» // Рос. газ. 2003. 10 дек.

Определение Конституционного суда РФ от 14 июля 1998 года «По делу о проверке конституционности отдельных положений Федерального закона “Об оперативно-розыскной деятельности” по жалобе гражданки И. Г. Черновой» // Собр. законодательства РФ. 1998. № 34. Ст. 4368.

Определение Конституционного суда РФ от 21 декабря 2000 года № 290-О «Об отказе в принятии к рассмотрению жалобы гражданина Идалова Тимура Саид-Магомедовича на нарушение его конституционных прав рядом статей УПК РСФСР и частью 2 статьи 8 ФЗ “Об оперативно-розыскной деятельности”» // Собр. законодательства РФ. 2001. № 11. Ст. 1069.

Определение Конституционного суда РФ от 4 февраля 1999 года № 18-О «По жалобе граждан М. Б. Никольской и М. И. Сапронова на нарушение их конституционных прав отдельными положениями Федерального закона “Об оперативно-розыскной деятельности”» // Вестн. Конституционного суда РФ. 1999. № 3. С. 23—25.

Определение Судебной коллегии по уголовным делам Верховного суда РФ от 09 декабря 1993 года и от 17 ноября 1994 года // Бюл. Верховного суда РФ. 1994. № 11. С. 47; 1995. № 5. С. 49.

Постановление Пленума Верховного Суда РФ от 24 декабря 1993 года № 13 «О некоторых вопросах, связанных с применением статей 23 и 25 Конституции РФ» // Бюл. Верховного суда РФ. 1994. № 3. С. 51—53.

Решение Верховного суда Российской Федерации от 25 сентября 2000 года № ГКПИ 00-1064 // Бюл. Верховного суда РФ. 2001. № 4. С. 84.

Уголовное дело № 1301 (Прокуратура Ленинского района г. Екатеринбург, 2004).

Уголовное дело № 2-131/03 (архив Свердловского областного суда, 2003).

Уголовное дело № 2-25/03 (архив Свердловского областного суда, 2003).

Уголовное дело № 232-96 (архив Уральского окружного военного суда, 1996).

Уголовное дело № 2-75/03 (архив Свердловского областного суда, 2003).

Уголовное дело № 309-97 (архив Уральского окружного военного суда, 1997).

Уголовное дело № 34805 (архив Железнодорожного суда г. Екатеринбург, 1998).

Уголовное дело № 864501 (архив Ленинского суда г. Екатеринбург, 1992).

Уголовное дело № 945802 (архив Свердловского областного суда, 1997).

Зарубежные нормативно-правовые акты и судебные прецеденты

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Criminal Division United States Department of Justice July 2002.

18 U.S.C., параграфы 2510—2522.

18 U.S.C., параграфы 3121—3127.

Criminal Procedure Law // N. Y. Criminal Stat. and Rules. LexisNexis. 2002. P. 452.

S. Rep. No. 99-541, at 12 (1986), reprinted in 1986 U.S.C.A.N.3555; United States v. Torres, 751 F. 2dd 875, 885—86 (7th Cir. 1984).

USA, v. Simpson, 152 F.3d 1241 (10th Cir. 1998).

USA, v. Tank, 200 F.3d 627, 630-31 (9th Cir. 2000).

USA, v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000).

Исследования и учебные пособия

Аверьянова Т. В. Криминалистика: Учеб. для вузов / Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г. и др.; Под ред. Р. С. Белкина. М., 2001.

Алексеев Н. С. Очерк развития науки советского уголовного процесса / Алексеев Н. С., Даев В. Г., Кокорев Л. Д. Воронеж, 1980.

Арсеньев В. Д. Истина, достоверность и обоснованность в следствии и судебных актах // Вопр. теории судебной экспертизы: Сб. науч. тр. ВНИИСЭ. Вып. 39. М., 1979.

Балакишин В. С. Доказательства в российском уголовном процессе: понятие, сущность, классификация. Екатеринбург, 2002.

Банин В. А. К вопросу о предмете и пределах доказывания в советском уголовном процессе // Проблемы доказательственной деятельности по уголовным делам. Красноярск, 1987.

Бедняков Д. И. Непроцессуальная информация и расследование преступлений. М., 1991.

Бедняков Д. И. О реализации оперативно-розыскной информации в процессе доказывания и особенности ее оценки // Проблемы надежности доказывания в советском уголовном процессе. М., 1984.

Безлепкин Б. Т. Комментарий к Уголовно-процессуальному кодексу Российской Федерации (постатейный). 4-е изд., перераб. и доп. М., 2004.

Безлепкин Б. Т. Проблемы уголовно-процессуального доказывания // Сов. государство и право. 1991. № 8. С. 100—102.

Белкин А. Р. Теория доказывания. М., 1999.

Белкин Р. С. Криминалистика: проблемы, тенденции, перспективы: Общие и частные теории. М., 1987.

Белкин Р. С. Собираение, исследование и оценка доказательств: Сущность и методы. М., 1966.

Белкин Р. С., Винберг А. И. Криминалистика и доказывание. М., 1969.

Быков В. М., Тренбак В. М. Основания и критерии признания доказательств недопустимыми // Следователь. 1998. № 9. С. 36—39.

Варфоломеева Т. В. Производные вещественные доказательства. М., 1980.

Винберг А. И. Криминалистика: Введение в криминалистику. Вып. 1. М., 1950.

Винер Н. Кибернетика, или Управление и связь в животном и машине / Пер. с англ. И. В. Соловьева; Под ред. Г. Н. Поварова. М., 1958.

Власова Н. А. Уголовный процесс: Курс лекций. М., 2001.

Вольтер Ф. М. Философские сочинения / Пер. с франц. С. Я. Шейман-Топштейн; Под ред. В. Н. Кузнецова. М., 1988.

Гаврилин Ю. В., Дубоносов Е. С. Использование контроля и записи телефонных и иных переговоров в раскрытии и расследовании преступлений: Учеб. пособие. М., 2003.

Гесснер Р., Херцог У. За фасадом права: Методы новой тайной полиции. М., 1990.

Голубев В. В. Интернет и оперативно-розыскная деятельность // Законодательство. 1999. № 11. С. 71—78.

Горских Г. Ф. Проблемы доказательств в советском уголовном процессе / Горских Г. Ф., Кокорев Л. Д., Элькинд П. С. Воронеж, 1978.

Горских Г. Ф. Судебная этика / Горских Г. Ф., Кокорев Л. Д., Котов Д. П. Воронеж, 1973.

Гушин А. И. Использование результатов оперативно-розыскной деятельности в доказывании // Проблемы реализации судебной реформы в России. Вып. 1. Саратов, 1998.

Громов Н. А. Доказательства, доказывание и использование результатов оперативно-розыскной деятельности / Громов Н. А., Пономаренков В. А., Гушин А. Н и др. М., 2001.

Громов Н. А. Доказательства, доказывание и использование результатов оперативно-розыскной деятельности / Громов Н. А., Гушин А. Н., Луговец Н. В. и др. М., 2006.

Громов Н. А. Новое в расследовании преступлений / Громов Н. А., Францифоров Ю. В., Николайченко В. В. // Следователь. 1998. № 2. С. 31—32.

Громов Н. А. Понятие доказательств в уголовном судопроизводстве // Государство и право. 1998. № 3. С. 48—52

Громов Н. А., Гушин А. Н. Проблемы интерпретации оперативно-розыскных данных в качестве доказательств // Проффессионал: Науч.-прав. альманах МВД России. 1999. № 5. С. 27—29.

Громов Н. А., Пономаренков В. А. Доказательства и доказывание в уголовном процессе. Самара, 1999.

Гушин А. Н. Оперативно-розыскная деятельность: совершенствование форм вхождения ее результатов в уголовный процесс: Учеб.-практ. пособие / Гушин А. Н., Громов Н. А., Царева Н. П. М., 2003.

Гушин А. Н. Проблемы использования результатов оперативно-розыскной деятельности в доказывании по уголовному делу / Гушин А. Н., Николайченко В. В., Громов Н. А. Пенза, 1998.

Давлетов А. А. Основы уголовно-процессуального познания. Свердловск, 1991.

Данилюк С. Как прослушать телефонный разговор / Данилюк С., Виноградов С., Щерба С. // Социалист. законность. 1991. № 2. С. 32—33.

Деларю Ж. История гестапо / Пер. с фр. Ю. А. Немешаева и др. Смоленск, 1998.

Доля Е. А. Использование в доказывании результатов оперативно-розыскной деятельности. М., 1996.

Доля Е. А. Использование результатов оперативно-розыскной деятельности в доказывании // Рос. юстиция. 1995. № 5. С. 41—42.

Доля Е. А. Новая Конституция и уголовно-процессуальная деятельность // Рос. юстиция. 1994. № 4. С. 19—21.

Доля Е. А. Прослушивание телефонных и иных переговоров — следственное ли это действие? // Сов. юстиция. 1992. № 19—20. С. 2.

Ермолович В. Ф., Ермолович М. В. Построение и проверка версий / Под ред. И. И. Басецкого. Минск, 2000.

Жук О. Д. Организованная преступность в современной России: Раскрытие и расследование преступлений, совершаемых организованными преступными формированиями. Томск, 1998.

Зажичкий В. И. Закон об оперативно-розыскной деятельности не идеален // Сов. юстиция. 1993. № 5. С. 20—22.

Зажичкий В. И. Правовая регламентация деятельности по обнаружению признаков преступления // Правоведение. 1992. № 4. С. 104, 105.

Зажичкий В. И. Связь оперативно-розыскной деятельности и уголовного процесса // Государство и право. 1995. № 6. С. 57—59.

Зинченко И. А. Использование в уголовно-процессуальном доказывании фотоснимков, кинолент и видеограмм. Ташкент, 1988.

Золотарев А. С. Процессуальные аспекты использования компьютерной информации в доказательственной деятельности // Информ. о-во: право и власть: Сб. науч. ст. Екатеринбург, 2001. С. 69, 70.

Золотых В. В. Проверка допустимости доказательств в уголовном процессе. М.; Ростов н/Д, 1999.

Из уха в ухо // Моск. комсомолец — Урал. 2000. 31 авг.

Иконникова О. А. Права человека: СОПМ-2 — новый электронный колпак // Юрист. 1999. № 2. С. 27, 28.

Ищенко Е. П. Использование современных научно-технических средств при расследовании уголовных дел. Свердловск, 1985.

Ищенко Е. П. Проблемы первоначального этапа расследования преступлений. Красноярск, 1987.

Калиновский К. Б., Маркелова Т. Ю. Доказательственное значение «электронной» информации в российском уголовном процессе // Рос. следователь. 2001. № 6. С. 18—19.

Кальницкий В. В. Следственные действия: Учеб. пособие. 2-е изд., перераб. и доп. Омск, 2003.

Карнеева Л. М. Доказательства и доказывание в уголовном процессе. М., 1995.

Китнис Н. М. Допустимость доказательств в уголовном судопроизводстве. М., 1995.

Козусев А. Законность прослушивания телефонных переговоров // Законность. 1993. № 2. С. 9—11.

Козырев Г. Документирование прослушивания и звукозапись телефонных и иных переговоров // Законность. 1993. № 4. С. 32—36.

Кокорев Л. Д., Кузнецов Н. П. Уголовный процесс: доказательства и доказывание. Воронеж, 1995.

Комлев В. О порядке прослушивания телефонных переговоров // Социалист. законность. 1991. № 7. С. 54—55.

Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Под общ. ред. В. П. Верина, В. В. Морзякова. М., 2004.

Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Под общ. ред. В. И. Радченко. 2-е изд. перераб. и доп. М., 2004.

Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Отв. ред. В. И. Радченко; Науч. ред. В. Т. Томин, М. П. Поляков. М., 2004.

Комментарий к Уголовно-процессуальному кодексу Российской Федерации / Под общ. и науч. ред. А. Я. Сухарева. 2-е изд. перераб. и доп. М., 2004.

Комментарий к Федеральному закону «Об оперативно-розыскной деятельности» / Д. В. Ривман. СПб., 2003.

Комментарий к Федеральному закону «Об оперативно-розыскной деятельности»: С постатейным приложением нормативных актов и документов / Авт.-сост. д-р юрид. наук, проф. А. Ю. Шумилов. 5-е изд., испр. и доп. М., 2003.

Комментарий оперативно-розыскного законодательства РФ и зарубежных стран: Учеб. пособие / М. П. Смирнов. М., 2003.

Корневский Ю. В., Токарева М. Е. Использование результатов оперативно-розыскной деятельности в доказывании по уголовным делам: Метод. пособие. М., 2000.

Кузнецов Н. П. Доказывание в стадии возбуждения уголовного дела. Воронеж, 1983.

Ларин А. М. Работа следователя с доказательствами. М., 1966.

Ленин В. И. Заключительное слово по докладу об очередных задачах Советской власти // Полн. собр. соч.: В 42 т. 4-е изд. Т. 36. М., 1962.

Лушинская П. А. Допустимость доказательств: пора обеспечить единство судебной практики // Рос. юстиция. 1998. № 11. С. 23—25.

Лушинская П. А. Основания и порядок принятия решений о недопустимости доказательств // Рос. юстиция. 1994. № 11. С. 3—4.

Лушинская П. А. Проблемы допустимости доказательств при рассмотрении дел судом присяжных // Рассмотрение дел судом присяжных. Варшава, 1997.

Малинова И. П. Регулирование информационной стихии как проблема современной культуры // Информ. о-во: право и власть: Сб. науч. ст. Екатеринбург, 2001. С. 4, 5.

Мингалин Н. Н. Контроль и запись переговоров в системе следственных действий // Следователь. 2003. № 12. С. 28—30.

Митрофанов Е. А., Каретников М. К. Некоторые проблемы нормативно-регулирующего применения и оборота специальных технических средств // Состояние, проблемы применения и совершенствования законодательства о борьбе с организованной преступностью и коррупцией. М., 2001.

Михайлов В. И. Контролируемая поставка как оперативно-розыскная операция / Под ред. А. Ю. Шумилова. М., 1998.

Михеенко М. М. К вопросу о правовой регламентации оценки доказательств и их источников в советском уголовном процессе // Актуальные проблемы доказывания в советском уголовном процессе. М., 1981.

Моисеев Н. Н. Универсум, информация, общество. М., 2001.

Овчинский А. С. Информация и оперативно-розыскная деятельность. М., 2002.

Овчинский С. С. Значение уголовно-правовых и уголовно-процессуальных институтов для оперативно-розыскной деятельности в борьбе с организованной преступностью // Следователь. 1999. № 9. С. 31—33.

Ожегов С. И. Словарь русского языка. М., 1978.

Орлов Ю. К. Основы теории доказательств в уголовном процессе. М., 2000.

Основы оперативно-розыскной деятельности: Учеб. / Под ред. В. Б. Рушайло. СПб., 2000.

Панченко М., Колпакиди А. Уши Лубянки // Версия. 2001. 22—28 мая. С. 11.
Пашин С. А. Допустимость доказательств (информация) // Рос. юстиция. 1994. № 7. С. 27—28.

Петрухин И. Л. Частная жизнь (правовые аспекты) // Государство и право. 1999. № 1. С. 68—70.

Пешиков М. А. Прослушивание и электронное наблюдение в уголовном процессе США // Рос. юстиция. № 4. 1997. С. 29—31.

Поляков М. П. Уголовно-процессуальное использование результатов оперативно-розыскной деятельности / Поляков М. П., Попов А. П., Попов Н. М. Пятигорск, 1998.

Рапинов А. Р. Вопросы следственного мышления в свете теории информации // Вопр. кибернетики и права. М., 1967.

Рапинов А. Р. Судебная психология для следователей. М., 1967.

Румянцев Д. Г., Монастырский Л. Ф. Путь программиста. М., 2000.

Семенцов В. А. Следственные действия: Учеб. пособие. Екатеринбург, 2003.

Сетров М. И. Информационные процессы в биологических системах. Л., 1975.

Словарь иностранных слов / Под ред. И. В. Лехина. 6-е изд, перераб. и доп. М., 1964.

Советский уголовный процесс: Учеб. / Под ред. Л. М. Карнеевой, П. А. Лупинской, И. В. Тыричева. М., 1980.

Соловьев А. Б. О психологических приемах допроса // Проблемы предварительного следствия в уголовном судопроизводстве. М., 1980.

Соловьев А. Б. Прокурорский надзор за всесторонностью, полнотой и объективностью расследования преступлений / Соловьев А. Б., Багатулин Ф. Н., Филиппов М. Н. М., 1996.

Соловьев А. Б. Следственные действия на первоначальном этапе расследования преступлений. М., 1994.

Степанов В. В., Денежкин Б. А. Проблемы развития средств доказывания в уголовном судопроизводстве // Вестн. Сарат. гос. академии права. 1995. № 3. С. 27, 28.

Строгович М. С. Избранные труды: В 3 т. Т. 1. М., 1990.

Трусов А. И. О допустимости и относимости доказательств // Сов. юстиция. 1990. № 14. С. 14—15.

Трусов А. И. Судебное доказывание в свете идей кибернетики // Вопр. кибернетики и права. М., 1967.

Управление Федеральной службы безопасности Российской Федерации по Свердловской области 1918—2003: К 85-летию образования Управления Федеральной службы безопасности России по Свердловской области. Екатеринбург, 2003.

Фаткуллин Ф. Н. Общие проблемы процессуального доказывания. 2-е изд. Казань, 1976.

Чечетин А. Е. Оперативно-розыскные мероприятия // Федеральный закон «Об оперативно-розыскной деятельности»: Науч.-практ. comment. / Под ред. В. В. Николюка, В. В. Кальницкого, А. Е. Чечетина. Омск, 1999.

Шейфер С. А. Доказательственное значение Закона об оперативно-розыскной деятельности // Государство и право. 1994. № 1. С. 94—97.

Шейфер С. А. Доказательственные аспекты Закона об оперативно-розыскной деятельности // Государство и право. 1991. № 1. С. 98—100.

Шейфер С. А. Использование непроцессуальных познавательных мероприятий // Государство и право. 1997. № 9. С. 47—49.

Шейфер С. А. Проблемы развития системы следственных действий в УПК РФ // Уголов. право. 2002. № 3. С. 90—91.

Шейфер С. А. Следственные действия: Система и процессуальная форма. М., 1981.

Шейфер С. А. Собираение доказательств в советском уголовном процессе: методологические и правовые проблемы. Саратов, 1986.

Шейфер С. А. Сущность и способы собирания доказательств в советском уголовном процессе. М., 1972.

Эйсман А. А. Некоторые вопросы исследования вещественных доказательств // Вопр. криминалистики. 1962. № 5. С. 31—33.

Авторефераты диссертаций

Диденко В. И. Использование следователем фактических данных, полученных в результате применения в оперативно-розыскной деятельности аудио- и видеозаписи, фото- и киносъемки: Автореф. дис. ... канд. юрид. наук. М., 1996.

Орлов Ю. К. Заключение эксперта как источник выводного знания в судебном доказывании: Автореф. дис. ... канд. юрид. наук. М., 1985.

Пономаренков В. А. Проблемы представления и использования доказательств в уголовном процессе: Автореф. дис. ... канд. юрид. наук. Саратов, 1998.

Электронные ресурсы

Адрес сайта газ. «Московские новости»: <http://www.mn.ru>.

Приказ Российской Военной Социалистической Республики от 23 декабря 1918 года № 346 // Положение о военной цензуре. Прил.: Перечень сведений, подлежащих предварительному просмотру военной цензурой, «Перечень сведений, не подлежащих распространению путем почтово-телеграфных сообщений, Штаты военно-цензурных отделений [Электрон. ресурс]. Режим доступа: <http://www.vif2.ru/users/offtopic/vio/VIO/IST16.htm>.

Фонд «Социум». Отношение жителей г. Екатеринбурга к камерам видеонаблюдения в магазинах и других общественных местах: Опрос фонда «Социум» [Электрон. ресурс]. Режим доступа: www.socium.ur.ru.

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations / Criminal Division United States Department of Justice. July, 2002 [Electronic resource]. [Http://www.cybercrime.gov](http://www.cybercrime.gov).

Научное издание

Соколов Юрий Николаевич

ЭЛЕКТРОННОЕ НАБЛЮДЕНИЕ
В УГОЛОВНОМ СУДОПРОИЗВОДСТВЕ
И ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ

Редактор и корректор
Компьютерная верстка

Р. Н. Кислых
Н. В. Комариной

Подписано в печать 24.10.2006. Формат 60×84 1/16.
Бумага для множительных аппаратов. Гарнитура Times.
Уч.-изд. л. 9,2. Усл. печ. л. 9,53. Тираж 100 экз. Заказ .

Издательство ООО «Оптима Проф». 620014, Екатеринбург, ул. 8 Марта, 32г.

Отпечатано в ООО «Корпорация типографий “Циркон”».
Свердловская обл., г. Реж, ул. Ломоносова, 6.