УДК 056+002:004.056

Противодействие преступлениям, связанным с нарушением тайны телефонных переговоров

А. А. Маринов, Е. Г. Усов, В. В. Загайнов

В современных условиях сотрудникам оперативных подразделений зачастую приходится сталкиваться с преступлениями, посягающими на конституционные права граждан, в том числе с нарушением тайны телефонных переговоров. Документирование указанных преступлений предполагает наличие у оперативника специальных познаний в сфере компьютерных технологий. При документировании преступных действий необходимо учитывать особенности рассматриваемого вида преступлений, о которых идет речь в данной статье.

Ключевые слова: противодействие преступлениям, нарушение тайны телефонных переговоров, нормативно-правовые акты, российские стандарты, нарушение тайны переписки.

1. Введение

Процесс научно-технического развития современного общества не только открывает новые возможности правоохранительных органов по документированию преступной деятельности, но также зачастую способствует анонимизации преступников. Следует согласиться с Ю. А. Серединой [9], которая утверждает, что «в связи с техническим прогрессом и постоянным расширением технических возможностей в настоящее время криминальными структурами с целью проведения определенных преступных операций активно используются самые различные электронные средства коммуникаций: телефон, телеграф, радиосвязь, пейджер, телефакс и другие устройства. Поэтому возникает необходимость создания особой системы защиты в этой области, а точнее системы мер по предотвращению преступлений и борьбы с ними с использованием научно-технических достижений». Наряду с вышеописанными одним из наиболее актуальных средств коммуникации в последние годы являются мессенджеры – программное обеспечение, предназначенное для обмена информацией между пользователями.

2. Построение и организация деятельности правозащитного механизма российского государства

Использование специальных познаний в сфере связи и компьютерной техники позволяет лицам, совершающим преступления, избегать привлечения к уголовной ответственности и безнаказанно совершать посягательства на конституционные права и свободы человека и гражданина. В постиндустриальном обществе особую актуальность приобретают преступные посягательства на тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (тайну связи). Государство в лице правоохранительных органов обязано обеспечивать информационную безопасность, одним из элементов которой является обеспечение вышеуказанных прав.

Статья 2 Конституция Российской Федерации гласит: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение

этого права допускается только на основании судебного решения» [1]. Из этого следует, что тайна телефонных переговоров является особо охраняемым видом тайны, для доступа к которой даже в интересах государства (например, в процессе осуществления оперативно-розыскной деятельности) требуется получение судебного разрешения.

Согласно определению Конституционного Суда Российской Федерации тайну телефонных переговоров составляют любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи [4]. Таким образом, анализируя позицию Конституционного Суда Российской Федерации, можно прийти к выводу, что сведения о детализации телефонных переговоров в той же степени составляют тайну телефонных переговоров, что и аудиальная и текстовая информация, передаваемая посредством телефонной связи. Кроме того, следует отметить, что содержание сообщений, передаваемых посредством мессенджеров (например, Viber, WhatsApp, Telegram и др.), голосовые сообщения и информация, передаваемые посредством звонков через мессенджеры, составляют тайну переписки и тайну телефонных переговоров.

Специализированным подразделением Министерства внутренних дел, в чьи функции входит выявление, предупреждение, пресечение и раскрытие преступлений, связанных с нарушением тайны телефонных переговоров, является Управление «К» БСТМ МВД России и входящие в его состав подразделения. В задачи указанных оперативных подразделений входит также оказание оперативного сопровождения по уголовным делам, возбужденным по ст. 138 УК РФ.

Расследованием уголовных дел по рассматриваемой статье согласно ст. 151 УПК РФ занимаются следователи Следственного комитета Российской Федерации.

Уголовная ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений закреплена в ст. 138 УК РФ. Посредством реализации данной нормы осуществляется уголовно-правовое регулирование вопросов обеспечения тайны телефонных переговоров.

Условно указанные нарушения можно разделить на три группы: нарушение тайны телефонных переговоров, совершенное с использованием возможностей правоохранительных органов; нарушение тайны телефонных переговоров, совершенное с использованием возможностей организаций, оказывающих услуги в сфере связи; нарушение тайны телефонных переговоров, совершенное лицом самостоятельно, без использования возможностей правоохранительных органов и операторов сотовой связи (в том числе с использованием вредоносного программного обеспечения и специальных технических средств, предназначенных для негласного получения информации).

Рассматривая первую группу нарушений, следует отметить, что правоохранительные органы в целях решения задач оперативно-розыскной деятельности имеют право на получение информации ограниченного доступа, в том числе сведений, составляющих тайну телефонных переговоров. При этом действующим законодательством проведение оперативно-розыскных мероприятий сотрудниками оперативно-розыскных органов в иных целях (в том числе личных) не допускается. Однако не во всех случаях указанные правовые предписания строго исполняются. Так, приговором Октябрьского районного суда г. Владимира был осужден начальник полиции УМВД России по Владимирской области [5], являющийся должностным лицом в государственном органе, который, действуя из иной личной заинтересованности, обусловленной желанием осуществления негласного контроля за служебной деятельностью руководящего состава подразделений, в отсутствие судебного решения, позволяющего осуществлять прослушивание телефонных переговоров, находясь в своем служебном кабинете, дал противоправное указание начальнику центра информационных технологий (ИТ), связи и защиты информации по Владимирской области о необходимости негласной записи телефонных переговоров со стационарных аппаратов связи, с использованием специальных технических средств.

3. Доступ к сведениям, составляющим тайну телефонных переговоров

Сотрудники организаций, оказывающих услуги в сфере связи, зачастую тоже привлекаются для совершения преступлений, связанных с нарушением тайны телефонных переговоров. В качестве примера второй группы нарушений можно рассмотреть приговор в отношении гражданина Н. Согласно материалам уголовного дела указанный гражданин, будучи коммерческим представителем компании, в дневное время суток, находясь на своем рабочем месте – в офисе продаж, используя свое служебное положение, персональный идентификатор, пароль и логин, полученные в ходе выполняемой им трудовой деятельности, а также предоставленные права и полномочия, предусмотренные трудовым договором, совершил доступ к компьютерной информации о персональных данных клиентов, содержащей в том числе входящие и исходящие данные биллинговой системы (в электронном виде) абонентов сотовой связи. В результате своих преступных действий гражданин Н. незаконно получил и передал третьим лицам сведения, составляющие тайну телефонных переговоров потерпевшей, тем самым нарушив конституционное право потерпевшей на неприкосновенность тайны телефонных переговоров [6], предусмотренное ст. 23 Конституции Российской Федерации.

Использование служебного положения, например, должностными лицами органов, уполномоченных на осуществление оперативно-розыскной деятельности, работниками почты, узлов связи и др., является квалифицированным составом преступления и предполагает более строгое наказание [8].

Следует отметить, что нарушение тайны телефонных переговоров не во всех случаях сопряжено с использованием возможностей правоохранительных органов или организаций, предоставляющих услуги в сфере связи. В ряде случаев рассматриваемые преступления совершаются лицом путем доступа к личным кабинетам абонентов сотовой связи [7]. Все без исключения операторы сотовой связи предоставляют своим абонентам возможность доступа к личному кабинету – информационному порталу, позволяющему контролировать расходы на сотовую связь, подключать и отключать дополнительные услуги и в том числе получать детализацию телефонных переговоров за определенный период времени. Получение детализации через личный кабинет осуществляется путем направления файла в формате PDF на электронную почту, указанную пользователем. Во время каждого входа в личный кабинет автоматически фиксируется IP-адрес, знание которого может позволить оперативнику установить местонахождение абонента, совершившего доступ.

В рамках указанной группы преступлений необходимо также рассмотреть нарушения тайны телефонных переговоров, совершенные с использованием вредоносного программного обеспечения. Указанный способ предполагает «заражение» устройства различными программами-вирусами. Заражение происходит различными способами: контактным, при котором осуществляется загрузка вредоносной программы с физического носителя (карта памяти, оптический диск и др.), и бесконтактным – например, при переходе пользователя по ссылке или установке им вируса под видом приложения. В случае заражения устройства вредоносным программным обеспечением доступ к нему могут получить третьи лица, инициировавшие заражение. В данном случае у указанных лиц появляется возможность ознакамливаться с информацией, находящейся на устройстве, осуществлять отправку либо блокирование СМС-сообщений, осуществлять запись переговоров, ведущихся с устройства, и получать детализацию звонков. Обстоятельствами, свидетельствующими о заражении устройства вредоносным программным обеспечением, являются: не обусловленное объективными факторами снижение производительности устройства, самопроизвольная смена заданных параметров и настроек, самопроизвольное отправление СМС-сообщений и/или совершение звонков. Вместе с тем с достаточной точностью утверждать, что устройство заражено вредоносным программным обеспечением, может лишь после проведения компьютерной экспертизы (исследования).

4. Использование специальных технических устройств для совершения преступления

Немаловажную роль в негласном получении информации отводится специальным техническим устройствам. Постановлением Правительства Российской Федерации[1] утвержден перечень из десяти категорий специальной техники. При этом одна из категорий – «специальные технические средства, предназначенные для негласного прослушивания телефонных переговоров» – функционально предназначена именно для получения информации, передаваемой по телефонным каналам связи. К указанной категории специальных технических устройств, предназначенных для негласного получения информации, в частности, относится так называемая ложная базовая станция – комплекс приемопередающей аппаратуры, которая перехватывает сигналы сотовой связи в определенном радиусе.

Следует отметить, что использование вредоносного программного обеспечения и специальных технических устройств, предназначенных для негласного получения информации в целях нарушения тайны телефонных переговоров, встречаются достаточно редко, так как эти способы сопряжены с приобретением дорогостоящего программного обеспечения или аппаратного оборудования.

Преступления, предусмотренные ст. 138 УК РФ, обладают достаточно высокой естественной латентностью, которая обусловлена, с одной стороны, нежеланием потерпевших обращаться в правоохранительные органы, а с другой – сложностью документирования следов преступления, требующей наличия специальных познаний. В этой связи следует рассмотреть некоторые аспекты получения и проверки первичной информации по делам данной категории.

Одним из важнейших способов получения первичной информации является анализ поступивших сообщений о преступлениях и обращений граждан. Как было указано выше, работа по рассматриваемой категории преступлений предполагает наличие особых познаний в сфере компьютерных технологий, которые имеются, например, у сотрудников подразделений «К». Однако в ряде случаев сообщения о преступлениях и обращения граждан, содержащие информацию о нарушении тайны телефонных переговоров, рассматриваются сотрудниками, не обладающими специальными познаниями, либо сотрудниками, не являющимися субъектами оперативно-розыскной деятельности (например, участковыми уполномоченными полиции). Это препятствует успешному документированию преступных деяний и зачастую влечет принятие незаконных и необоснованных решений об отказе в возбуждении уголовного дела либо направлении ответа гражданину без принятия соответствующего решения о проверке. С целью организации качественной проверки информации видится целесообразным вести инициативную работу по выявлению фактов обращения граждан по вопросам нарушения тайны телефонных переговоров сотрудникам профильных оперативных подразделений (подразделений «К»). Это позволит надлежащим образом квалифицировать факты, указанные в обращении, и в случае необходимости оказывать практическую помощь территориальным органам внутренних дел. При этом следует отметить, что уголовные дела о преступлениях, предусмотренных частью 1 ст. 138 УК РФ, согласно ст. 20 УПК РФ относятся к уголовным делам частно-публичного обвинения и возбуждаются не иначе как по заявлению потерпевшего или его законного представителя. Таким образом, в случае установления факта нарушения тайны телефонных переговоров обязательной процедурой является уведомление

[1] Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности: постановление Правительства Российской Федерации от 01.07.1996 г. № 770 // Собрание законодательства Российской Федерации. 1996. № 28. Ст. 3382.

лица, право которого было нарушено. В случае если указанное лицо желает обратиться в правоохранительные органы, обязательно требуется принять его заявление, так как оно будет являться поводом для возбуждения уголовного дела.

Для анализа сообщений о преступлениях представляется оптимальным использование ведомственного программного обеспечения АРМ «ДЧ Факт», которое позволяет в короткие сроки по заданным поисковым признакам осуществить выборку материалов, зарегистрированных в книгах учета сообщений о происшествиях (далее – КУСП). Учет обращений граждан ведется в подразделениях делопроизводства и режима, во взаимодействии с которыми оперативные сотрудники могут получать информацию о незарегистрированных в КУСП обращениях граждан по фактам нарушения тайны телефонных переговоров.

5. Проверка первичной оперативно-значимой информации

Наряду с анализом сообщений о преступлениях и обращений граждан важным источником оперативно значимой информации является использование содействия граждан. Как правило, к лицам, осведомленным о подобных фактах, относятся сотрудники служб безопасности операторов сотовой связи. Зачастую корпоративная политика компаний считает приоритетной задачей не доведение до сведения правоохранительных органов информации о преступлениях, а выявление среди своих работников лиц, занимающихся противоправной деятельностью, и их скорейшее увольнение под угрозой обращения в полицию. В связи с этим оперуполномоченным целесообразно проводить разъяснительную работу с сотрудниками служб безопасности вышеуказанных организаций, доводя до их сведения необходимость передачи информации о любых фактах нарушения тайны телефонных переговоров.

Для проверки первичной оперативно значимой информации необходимо установление механизма совершения преступления. Как указывалось выше, нарушения тайны телефонных переговоров могут быть совершены с использованием возможностей правоохранительных органов, организаций, оказывающих услуги в сфере связи, либо лицом самостоятельно.

Для того чтобы оперуполномоченному установить либо опровергнуть факт использования для совершения преступления возможностей органов, уполномоченных на осуществление оперативно-розыскной деятельности, необходимо в установленном порядке обратиться в подразделение, осуществляющее оперативно-технические мероприятия. В системе МВД России ими являются подразделения специальных технических мероприятий. Для получения информации об указанных мероприятиях необходимо провести оперативно-розыскное мероприятие «наведение справок», сопряженное с обращением в установленном порядке в оперативно-техническое подразделение, порядок получения указанной информации определяется Наставлением об основах организации оперативно-служебной деятельности подразделений специальных технических мероприятий органов внутренних дел Российской Федерации и взаимодействия с оперативными подразделениями системы МВД России, правомочными осуществлять оперативно-розыскную деятельность [3].

Схожим образом путем проведения оперативно-розыскного мероприятия «наведение справок» следует проверить версию о том, использовались ли для совершения преступлений возможности компаний, представляющих услуги связи. Во всех соответствующих компаниях ведется учет доступа к детализации абонентов, а также хранятся сведения о должностных лицах, которым она была передана в установленном порядке. Сведения об обращении к карточке абонента, об обращении к детализации конкретного абонента, а также о выдаче/отправлении детализации могут быть получены в соответствующих организациях по запросу. Для истребования указанной информации получение судебного решения сотрудником полиции не требуется [3], в запросе достаточно указать соответствующее основание, предусмотренное Федеральным законом «Об оперативно-розыскной деятельности».

Также следует рассмотреть вопрос документирования преступных действий лиц, совершивших преступление путем доступа к личным кабинетам абонентов сотовой связи.

Выше было указано, что все абоненты сотовой связи обладают возможностью получить на электронную почту детализацию по своему номеру путем доступа через интернет к личному кабинету. Личный кабинет абонента, как правило, предполагает возможность входа в него путем получения абонентом сообщения с кодом подтверждения. В этой связи завладение телефоном потерпевшего позволяет преступнику получить информацию о соединениях абонента втайне от ее обладателя. В указанных случаях оперативному сотруднику необходимо путем проведения оперативно-розыскного мероприятия «исследование предметов и документов» с согласия потерпевшего осуществить вход в личный кабинет потерпевшего с целью фиксации признаков преступления – IP-адресов входа в личный кабинет, привязанного к личному кабинету электронного почтового ящика, сведений о смене пароля и прочих. Указанная информация содержится в меню личного кабинета во вкладках под названием «история активности», «безопасность», «приватность» и других. При проведении данного оперативно-розыскного мероприятия следует проводить фотофиксацию, что позволит избежать утраты информации, потенциально имеющей доказательственное значение. Материалы, собранные в процессе оперативно-розыскной деятельности, после передачи в установленном порядке в органы предварительного расследования могут быть использованы в доказывании по уголовным делам.

Положительный опыт реализации оперативной разработки лица, нарушившего тайну телефонных переговоров граждан, следует рассмотреть на примере деятельности отдела «К» ГУ МВД России по Иркутской области.

В 2016 году в указанное подразделение поступила информация о том, что гражданин «В», являющийся частным детективом, осуществляет продажу информации о детализации абонентов [5]. С целью проверки указанной информации было проведено оперативно-розыскное мероприятие «проверочная закупка», в ходе которого осуществлено затратное приобретение детализации абонента сотовой компании ООО «Т2 Мобайл» гражданки «С», которая дала свое добровольное согласие на участие в оперативно-розыскных мероприятиях. В ходе проведения указанного оперативно-розыскного мероприятия было установлено, что гражданин «В» действительно предоставляет актуальную информацию о входящих и исходящих соединениях абонента [5]. Путем проведения оперативно-розыскного мероприятия «наведение справок» было установлено, что детализация гражданки «С» за рассматриваемый период была получена в одном из дилерских центров компании ООО «Т2 Мобайл» в городе Санкт-Петербурге.

Результаты оперативно-розыскной деятельности в 2017 году [8] были предоставлены в органы Следственного комитета Российской Федерации по Иркутской области, по факту нарушения тайны телефонных переговоров было принято решение о возбуждении уголовного дела по ст. 138 УК РФ.

6. Заключение

Подведя итог вышеизложенному, стоит отметить, что нарушение тайны телефонных переговоров является преступлением, которое обладает высокой латентностью и предъявляет высокие требования к уровню специальных знаний у сотрудников. Выявление информации о фактах нарушения тайны телефонных переговоров предполагает изучение поступивших сообщений о преступлениях и обращений граждан, а также использование содействия граждан. Преступления, предусмотренные ст. 138 УК РФ по механизму совершения условно можно разделить на три группы, каждая из которых имеет свои особенности. Учет особенностей данных преступлений позволит повысить эффективность правоохранительной деятельности, связанной с решением задач оперативно-розыскной деятельности применительно к нарушениям тайны телефонных переговоров.

Литература

1. Конституция Российской Федерации от 12.12.1993 // Собрание законодательства Российской Федерации. 2009. № 4. Ст. 445 (с послед. изм. и доп.).
2. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ (в ред. ФЗ от 19 февраля 2018 г. № 35-ФЗ) // СЗ РФ. 1996. № 25. Ст. 2954.
3. Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» // Собрание законодательства Российской Федерации. 1995. № 33. Ст. 3349.
4. Определение Конституционного Суда Российской Федерации от 02 октября 2003 г. № 345-О «Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 «О связи».
5. Приговор Октябрьского районного суда г. Владимир (Владимирская область) от 20 декабря 2017 г. по делу 1-427/2017 URL: http://sudact.ru/regular/doc/9YyJp2EVsPVL/ (дата обращения: 10.09.2021).
6. Приговор Кировского районного суда г. Астрахани (Астраханская область) № 1-523/2017 от 30 октября 2017 г. по делу 1-523/2017 URL: http://sudact.ru/regular/doc/ORwv1AJz1yUK/ (дата обращения: 10.09.2021).
7. Приговор Калужского районного суда (Калужская область) № 1-878/1/2017от 15 декабря 2017 г. по делу 1-878/1/2017 URL: http://sudact.ru/regular/doc/1KmWTdMX4qHo/ (дата обращения: 10.09.2021).
8. *Олефиренко С. П.* Уголовно-правовое исследование состояния морального вреда в преступлениях, предусмотренных ст. 138, 138.1 УК РФ // Вестник ЧелГУ. 2013. № 5. С. 91.
9. *Середина Ю. А.* Прослушивание телефонных переговоров, контроль и запись переговоров, сравнительная характеристика // Материалы МНПК «Актуальные проблемы борьбы с преступностью», 16–17 дек. 2011 г., Челябинск. 2012. С. 123.

Статья поступила в редакцию 29.10.2021.

Маринов Александр Андреевич
к.э.н., доцент центра компетенций по кибербезопасности института информационных технологий и анализа данных ИрНИТУ, e-mail: am-irk@yandex.ru.

Усов Евгений Геннадьевич
к.ю.н., доцент кафедры государственно-правовых дисциплин Восточно-Сибирского института МВД России, e-mail: usov.evgeniy@list.ru.

Загайнов Владимир Владимирович
к.ю.н., доцент кафедры уголовного права Всероссийского государственного университета юстиции (РПА Минюста России), e-mail: vladzagain@mail.ru.

Countering crimes related to the violation of the telephone conversation secrecy

A. Marinov, E. Usov, V. Zagainov

In today's circumstances, operational personnel often face crimes violating the constitutional rights of citizens, including violation of the telephone conversation secrecy. Documentation of these crimes implies that field investigator has special knowledge in the sphere of computer technology. When documenting criminal actions, it is necessary to take into account the type of crime characteristics mentioned in this article.

Keywords: countering crimes, violation of the secrecy of telephone conversations, regulatory acts, Russian standards, violation of the secrecy of correspondence.