своей территории лицу, у которого существуют вполне обоснованные опасения столкнуться с угрозой жизни, здоровью, правам и свободам в государстве гражданской принадлежности или постоянного места жительства. В узком смысле под правом убежища следует понимать право лица искать, просить и пользоваться убежищем. В свою очередь, совокупность правовых норм, регулирующих общественные отношения в сфере предоставления убежища лицам, его ищущим, образуют конституционно-правовой институт права убежища.

Библиографические ссылки

1. Антипов, А.Н. Право убежища в системе обеспечения безопасности государства / А.Н. Антипов // Тр. Акад. упр. МВД России. 2007. № 4.
2. Галенская, Л.Н. Право политического убежища / Л.Н. Галенская. М., 1968.
3. Лукашук, И.И. Международное право. Общая часть : учеб. для студентов юрид. фак. и вузов / И.И. Лукашук. 3-е изд., перераб. и доп. М., 2005.
4. Матузов, Н.И. Теория государства и права : учебник / Н.И. Матузов, А.В. Малько. М., 2004.
5. Международное право : учеб. для вузов / отв. ред. Г.В. Игнатенко, О.И. Тиунов. М., 1999.
6. Международное публичное право : учебник / Л.П. Ануфриева [и др.] ; отв. ред. К.А. Бекяшев. 4-е изд., перераб. и доп. М., 2005.
7. Мокринский, С.П. Политическое преступление в международных договорах о выдаче преступников / С.П. Мокринский // Междунар. жизнь. 1924. № 2–3.
8. О беженцах : федер. закон Рос. Федерации, 19 февр. 1993 г., № 4528-ФЗ // КонсультантПлюс : РФ. Технология ПРОФ [Электронный ресурс]. Минск, 2012.
9. О предоставлении иностранным гражданам и лицам без гражданства статуса беженца, дополнительной и временной защиты : закон Респ. Беларусь, 23 июня 2008 г., № 354 : в ред. закона Респ. Беларусь от 03.07.2011 // КонсультантПлюс : Беларусь. Технология ПРОФ [Электронный ресурс] / ООО «ЮрСпектр». Минск, 2012.
10. Ушаков, Н.А. Право убежища : дис. … канд. юрид. наук : 12.00.10 / Н.А. Ушаков. М., 1950.
11. Червонюк, В.И. Конституционное право России / В.И. Червонюк. М., 2004.
12. Шаргородский, М.Д. Выдача преступников и право убежища в международном праве / М.Д. Шаргородский // Вестн. Ленинград. ун-та. 1947. № 5.
13. Шибаева, Е.А. Проблемы права убежища в международном права : дис. … канд. юрид. наук : 12.00.10 / Е.А. Шибаева. М., 1953.

Дата поступления в редакцию: 31.08.2012

УДК 343

С.И. Семилетов, *кандидат юридических наук, старший научный сотрудник Института государства и права Российской академии наук*

МОДЕЛИ ПРАВОВОЙ ОРГАНИЗАЦИИ ОПЕРАТИВНО-РОЗЫСКНЫХ МЕРОПРИЯТИЙ В СЕТЯХ СВЯЗИ

Анализируются действующие модели законного перехвата коммуникаций на каналах и сетях связи на основе подходов по американскому стандарту CALEA и европейскому стандарту ETSI и российской действующей модели СОРМ. Дается сравнительный анализ моделей законного перехвата коммуникаций на каналах и сетях связи и отличия модели СОРМ от моделей на основе подходов по стандартам CALEA и ETSI в части их соответствия требованиям норм международного права.

The article provides an analysis of existing models of legal interception of communications on the channels and networks of communication based approaches to the American standard CALEA and ETSI European standard and Russian working model of SORM. The article presents a comparative analysis of the models on the lawful interception of communications channels and networks of communication and differences SORM model of models based on sets of CALEA and ETSI standards in terms of their compliance with the requirements of international law.

Федеральный закон «О содействии телекоммуникационных компаний правоохранительным органам» (CALEA) [2] содержит и описывает установленные законом обязательства телекоммуникационных компаний по части оказания содействия в выполнении слежки, наблюдения и перехвата переписки и иных сообщений на телекоммуникационных сетях с использованием радиоэлектронных средств в соответствии и на основании постановления суда или иных законных предписаний.

Цель CALEA состоит в том, чтобы в условиях ускоренного развития телекоммуникационных технологий и в рамках обеспечения прав человека и гражданина в соответствии с требованиями норм международного права и Конституции:

обеспечить на законной основе правоохранительные органы возможностью и способностью проводить наблюдение, отслеживание и перехват сообщений и иных данных с использо-

ванием радиоэлектронных средств, при этом сохраняя и охраняя общественную безопасность и право на частную жизнь;

сохранить конкурентоспособность в сфере телекоммуникационных услуг;

обеспечить контроль законности и правомерности проводимых мероприятий по наблюдению, отслеживанию и перехвату переписки и иных сообщений и получению сопутствующей конфиденциальной информации.

Требования к стандартам по перехвату сообщений в США и порядок перехвата, отвечающие требованиям CALEA определяются независимой Федеральной комиссией по связи (FCC) [1].

В разд. 229 закона CALEA установлены полномочия FCC. Федеральная комиссия связи играет важную роль в реализации положений CALEA [2]. Комиссия устанавливает политику взаимодействия, правила и процедуры взаимодействия коммуникационных компаний и поставщиков услуг с правоохранительными органами, которые должны обеспечивать выполнение требований закона CALEA, проверяет и утверждает сметы расходов за услуги и на необходимое оборудование средств перехвата поставщику услуг, которые подлежат компенсации из госбюджета. FCC также предотвращает попытки должностных лиц правоохранительных органов осуществить перехват без представления соответствующего разрешения (санкции) и подает ходатайства для привлечения их к ответственности и устанавливает порядок документирования действий должностных лиц правоохранительных органов по перехвату или доступу к идентифицирующей запрос информации с представлением соответствующего разрешения или без.

При этом сами стандарты в США разрабатываются некоммерческими организациями, в частности Ассоциацией по отраслевым решениям в сфере телекоммуникаций (ATIS) и Ассоциацией телекоммуникационной промышленности (TIA).

Основным документом, описывающим организацию законного перехвата, у CALEA является J-STD-025-A ‘Lawfully Authorized Electronic Surveillance’.

Концепция законного перехвата сообщений по модели CALEA представлена на рис. 1.

Рис. 1. Функциональная схема модели организации законного перехвата, реализующая подход CALEA

Генеральный прокурор (прокурор штата):

отчитывается перед конгрессом и делает доступным общественности отчет относительно затрат, уплаченных во время предыдущего бюджетного года поставщикам услуг;

утверждает список конкретных должностных лиц, которые уполномочены инициировать мероприятия по проведению законного перехвата, получать данные перехвата и идентифицирующей информации;

утверждает должностных лиц, которые в особых случаях, не терпящих отлагательства, имеют право без судебного ордера на основании ведомственного постановления инициировать перехват с последующим оформлением и предоставлением в течении 48 ч санкции суда.

Коммуникационная компания – поставщик услуг в лице своего уполномоченного на то представителя в праве и обязана [6]:

идентифицировать представителя правоохранительных органов, проверить его полномочия и полномочия ответственных лиц суда или иных лиц, подписавших ордер или иное законное разрешение на перехват;

документировать свои действия посредством внесения их в учетную запись вместе с контактной информацией, необходимой для связи с указанными лицами;

по представленному судом ордеру технически инициализировать перехват, доступ к информации, идентифицирующей звонок, задокументировать, хранить и поддерживать защищенную (от несанкционированного доступа) и точную запись каждого перехвата коммуникаций или доступа к идентифицирующей запрос информации в форме единственной легальной записи с указанием срока, установленного судьей, но не менее 10 лет (§ 2518 (8) (a) Chap. 119 Tit. 18 United States Code);

односторонне прекратить перехват в случаях истечения срока действия судебного ордера или непредставления правоохранительным органом судебного ордера в установленный срок;

документировать все случаи незаконного перехвата коммуникаций и письменно информировать о таких случаях незаконного перехвата органы прокуратуры и суда.

Правоохранительные органы (LEA) и их уполномоченные на то должностные лица:

юридически инициируют мероприятия по проведению законного перехвата и получают данные перехвата и идентифицирующую его информацию, оформляют каждую заявку (аффидевит) в суд и обращаются под присягу в суд;

не вправе самостоятельно устанавливать свои аппаратные средства и самостоятельно проводить перехват коммуникаций (за исключением некоторых случаев индивидуального перехвата устных сообщений средствами специального оборудования) и вправе лишь присутствовать и контролировать действия уполномоченных на то лиц поставщика коммуникационных услуг.

В функцию и полномочия судьи входит:

незамедлительное рассмотрение поступившей заявки на перехват (аффидевит) и приложенных материалов от уполномоченного на то лица правоохранительных органов на применение перехвата и получение судебного ордера;

проверка формальных требований, полномочий лиц правоохранительных органов, представивших заявку и подписавших постановление на проведение перехвата;

проверка мотивировки и обоснованности применения перехвата, в том числе и по квалификационным признакам статей уголовных преступлений, допускающих применение перехвата, указанных в § 2516 Chap. 119 Tit. 18 United States Code;

право требования дополнительных доказательств или обоснований в поддержку применения перехвата;

разрешать применение и выдавать судебный ордер на применение перехвата поставщику услуг на основании представленных фактов и обстоятельств (на которые ссылается правоохранительный орган) и своей убежденности в их необходимости;

обусловливать выдачу судебного ордера и вписывать в судебный ордер условие представления отчета должностного лица правоохранительного органа, инициализировавшего перехват, об результатах и эффективности полученных данных перехвата в получении сведений необходимых доказательств преступления;

в случае отказа выдать ордер правоохранительному органу на применение уже инициализированного им перехвата, подать уведомление лицам, указанные в запросе, о фактах перехвата их коммуникации (§ 2518 (8) (d) Chap. 119 Tit. 18 United States Code);

после получения ходатайства от лица, в отношении которого правоохранительный орган провел незаконный перехват, может по своему усмотрению дать доступ такому лицу или его адвокату относительно осмотра частей перехваченных коммуникаций применений и ордеров, касающихся такого лица;

получение экземпляра легализованной записи перехвата по каждому выданному судьей ордеру, доступа к нему и обязанность определения порядка и места долговременного хранения такой легализации.

Лица, в отношении которых проводился перехват, вправе:

подавать ходатайство на ознакомление с содержанием незаконных перехватов их коммуникаций или на уничтожение записей таких перехватов;

получать копии содержания перехватов любой проводной, устной или электронной коммуникации, перехваченной в соответствии с установленным порядком или доказательством, полученным из них, вместе с копиями судебного ордера или иными разрешающими и сопровождающими перехват документами не менее чем за 10 дней до судебного процесса или другого процесса в любом суде, слушании или другом процессе в федеральном суде или суде штата, где это содержание или доказательства, вытекающие из них, будут представлены (§ 2518 (10) (a) Chap. 119 Tit. 18 United States Code).

Страны ЕС ориентируются на стандарт, разработанные Европейским институтом стандартов связи (ETSI) для проводной связи, интернета, беспроводной связи и кабельных систем. ETSI официально признан ЕС. ETSI объединяет более 70 членов-организаций из 62 стран мира, а среди них объединяет производителей, операторов сетей, национальные правительства, провайдеров услуг, исследовательские институты, группы пользователей и консультантов.

Разработанные стандарты ETSI по законному перехвату сообщений играют важную роль и оказывают существенную помощь правоохранительным органам Европы в их борьбе с преступностью.

Модель организации законного перехвата, заложенная в стандарте ETSI, представлена на рис. 2.

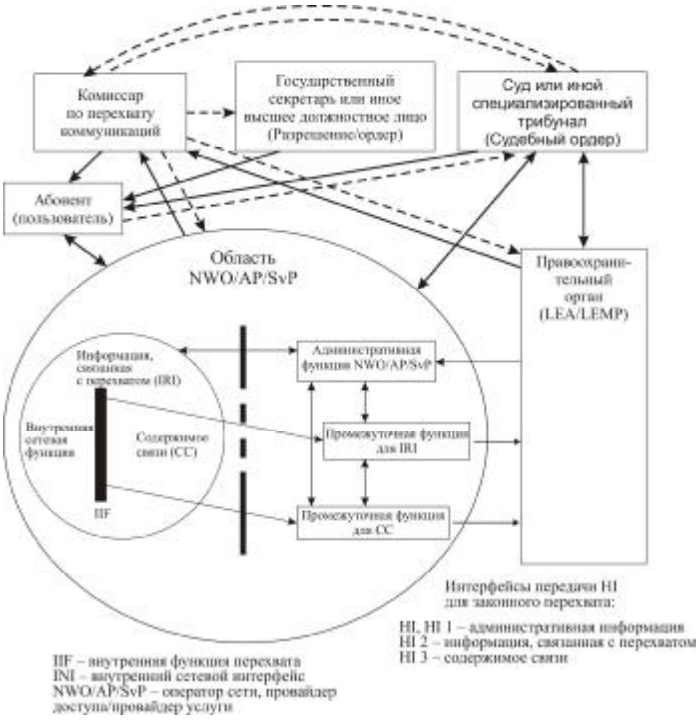

Рис. 2. Функциональная схема модели организации законного перехвата и интерфейсов передачи, реализующая подход по стандарту ETSI

Законный перехват общественных телекоммуникационных систем в каждой стране базируется на национальном законодательстве, но модель организации законного перехвата и взаимодействия сторон строится по стандартам ETSI. Цель стандартизации законного перехвата в ETSI состоит в том, чтобы облегчить реализацию законного перехвата таким образом, чтобы перехват соответствовал национальному законодательству и международным конвенциям и был эффективен и при этом экономичен.

Описание функциональной модели, ее характеристик, интерфейсов, передаваемых сообщений и других параметров представлено в документах ETSI TS 101 671 ‘Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommuni-

cations Traffic' (Телекоммуникационная безопасность; законный перехват (LI); интерфейс передачи для законного перехвата телекоммуникационного трафика) [5], ES 201 158 'Telecommunications Security; Lawful Interception (LI); Requirements for Network Functions' (Телекоммуникационная безопасность; законный перехват (LI); требования для функций сети) [3], а также ETSI TS 101 331 'Telecommunications Security; Lawful Interception (LI); Requirements of Law Enforcement Agencies' (Телекоммуникационная безопасность; законный перехват (LI); требования правоохранительных органов) [4].

Потребителями услуг по законному перехвату являются правоохранительные органы, агентства национальной безопасности. Структурно конфигурация системы реализует три блока действий:

инициализация, поиск и сбор, в котором из сети извлекаются только целевые вызовы, звонки, сообщения и иной целевой контент по идентификационным данным (информация, связанная с перехватом);

посредничество, где данные форматируются, чтобы соответствовать определенным форматам и стандартам;

передача данных и содержания правоохранительным органам.

Ордер может описывать связанную с перехватом информацию и информацию соединения для конкретного случая перехвата, период действия и предмет перехвата, адрес и иные индикационные данные пользователя (абонента), телекоммуникационные услуги и т. д. Для различных правоохранительных органов и разных случаев могут применяться разные ограничения, устанавливаемые национальными законодательствами и зависящие от абонентских услуг и сетей, которые используются для перехвата.

Когда ордер получен, оператор NWO/AP/SvP на основании ордера и его указаний ставит пользователя (абонента) на контроль и правоохранительный орган на свои средства мониторинга (LEMF – Law Enforcement Monitoring Facility), получают через порты интерфейса HI 2 и HI 3 информацию соединения (CC – Content of Communication), а также связанную с перехватом информацию (IRI – Intercept Related Information) о телекоммуникационных услугах, соединениях, включая неуспешные попытки вызовов, о местонахождении пользователя и т. д.

Представленная модель охватывает систематические и расширяемые средства, с помощью которых могут взаимодействовать операторы сети и правоохранительные органы, особенно с учетом того, что сети постоянно усложняются и растет количество услуг. Необходимо отметить, что такая конфигурация относится не только к традиционным проводным и беспроводным голосовым звонкам, но и к IP-сетям и вторичным сервисам и услугам на их основе, включая VoIP-телефонию (передача голоса по IP), электронную почту, мгновенную передачу сообщений и др.

Содержание звонка, или CC, – это поток данных, передающих контент сообщения звонка. Административная функция управления законным перехватом (LI) встроена в архитектуру и включает в себя инициализацию сеанса перехвата, прекращение и его удаление, планирование и целевую идентификацию. Связь между оператором сети и правоохранительными органами идет посредством интерфейса обмена (передачи) HI 1. Данные и содержание связи обычно передается от оператора сети правоохранительным органам в зашифрованном формате через виртуальные частные сети на основе IP-протокола по интерфейсам HI 2 и HI 3 соответственно. Важно отметить, что такая архитектура ETSI одинаково применима и к сервисам, реализуемым на IP-протоколах, в которых IRI зависят от параметров, связанных с пакетом передачи сообщения, которое необходимо перехватить.

Порт и интерфейс HI 1 предназначен для обмена административной информацией между LEA и оператором NWO/AP/SvP. Должно быть организовано полное разделение административного интерфейса HI 1 и технических HI 2 и HI 3 в самой сети оператора NWO/AP/SvP, чтобы обеспечить требуемую конфиденциальность информации об абонентах, находящихся под контролем. По концепции ETSI исключается любая возможность прямого контроля (управления) средств оператора NWO/AP/SvP средствами LEMF/LEA. Ручной интерфейс HI 1 обычно представлен в виде бумажного документооборота, где LEA на основании выданной лицензии по факсу или письмом отправляет запрос на предоставление услуг законного перехвата. Такая заявка поступает в административный центр. После ее обработки LEA информируется об активизации процедуры перехвата и по интерфейсу HI 2 и HI 3 в сторону LEA будет поступать информация, относящаяся к вызову (IRI) и содержимому (контенту) связи (CC). Имеется также

электронная реализация интерфейса HI 1 (альтернатива ручной), где используется электронный интерфейс, в котором обмен запросами и уведомлениями осуществляется в форме соответствующих электронных документов.

В целом основное отличие модели ETSI от CALEA заключается в том, что правоохранительный орган (LEA) самостоятельно предъявляет полученную санкцию суда (судебный ордер) на перехват оператору связи (поставщику услуг) (NWO/AP/SvP). При этом большинство стран по всему миру согласны с требованиями по LI применяемыми в странах Америки и в Европе, поддерживают их и идут по пути внедрения этих стандартов.

Таким образом, рассмотренные модели организации проведения оперативно-розыскных мероприятий, используемые в служебной деятельности правоохранительных органов зарубежных государств, и их опыт могут послужить для модернизации существующей системы оперативно-розыскных мероприятий Российской Федерации (СОРМ РФ).

Библиографические ссылки

1. Федеральная комиссия по связи (Federal Communications Commission – FCC) – независимое правительственное агентство Соединенных Штатов, созданное, управляемое и уполномоченное в соответствии с уставом Конгресса [Электронный ресурс]. 2012. Режим доступа: http://ru.wikipedia.org/wiki/Конгресс_США. Дата доступа: 20.09.2012.

2. Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified as amended in scattered sections of 18 U.S.C. and 47 U.S.C. §§ 229, 1001-1010, 1021. Mode of access: http://www. askcalea.net/docs/calea.pdf. Date of access: 20.09.2012.

3. ES 201 158 'Telecommunications Security; Lawful Interception (LI); Requirements for Network Functions'. 1998. Mode of access: http://cryptome.org/espy/ES201-158.pdf. Date of access: 20.09.2012.

4. ETSI TS 101 331 'Telecommunications Security; Lawful Interception (LI); Requirements of Law Enforcement Agencies'. Mode of access: http://www.gliif.org/LI_standards/ts_101331v010101p_lea-requirements.pdf. Date of access: 20.09.2012.

5. ETSI TS 101 671 'Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic'. Mode of access: http://www.gliif.org/LI_standards/ts_101671v020801p.pdf. Date of access: 20.09.2012.

6. FCC, Rules and Regulations, § 64.2104. Mode of access: http://www.gliif.org/LI_legal/47CFR-CALEA_parts.pdf. Date of access: 20.09.2012.

Дата поступления в редакцию: 04.10.2012

УДК 340.132

***А.А. Стремоухов**, кандидат юридических наук, доцент, начальник кафедры теории и истории государства и права Санкт-Петербургского военного института внутренних войск МВД России;*
***А.А. Дерюгин**, кандидат юридических наук, заместитель начальника кафедры теории и истории государства и права Санкт-Петербургского военного института внутренних войск МВД России*

ВОЙСКА ВНУТРЕННЕГО НАЗНАЧЕНИЯ В МЕХАНИЗМЕ ГОСУДАРСТВА (НА ПРИМЕРЕ ИСТОРИКО-ПРАВОВОГО ОПЫТА ФУНКЦИОНИРОВАНИЯ ВНУТРЕННИХ ВОЙСК МВД РОССИИ)

На основании анализа опыта выполнения внутренними войсками служебно-боевых задач рассматриваются правовые аспекты их функционирования в механизме государства на различных этапах истории России и в современных условиях.

In article on the basis of the analysis of experience of performance internal troops of office and fighting tasks consider legal aspects of their functioning in the state mechanism at various stages of history of Russia and in modern conditions.

Внутренние войска МВД России уже более 200 лет являются одной из составляющих системы обеспечения внутренней безопасности государства. Признанием заслуг внутренних войск МВД России в защите прав и свобод человека и гражданина от преступных и иных противоправных посягательств указом Президента Российской Федерации от 19 марта 1996 г. № 394 установлен День внутренних войск МВД России – 27 марта.

Необходимость рассмотрения функций внутренних войск (войск внутреннего назначения) в механизме государства через призму историко-правового опыта определяется следующими обстоятельствами.