ИНЖЕНЕРНЫЕ АСПЕКТЫ СОРМ В СЕТЯХ NGN

Б.С. ГОЛЬДШТЕЙН, заместитель директора ЛОНИИС, заведующий кафедрой СПбГУТ, доктор технических наук, А.А. ЗАРУБИН, доцент СПбГУТ, кандидат технических наук, А.В. ПИНЧУК, директор Научно-технического центра "Протей"

Не стремись слышать все, ибо услышишь, как твой раб злословит тебя.
Екклезиаст

Как уже обсуждалось в [1], когда при сегодняшних терактах, человеческая жизнь ценится дешевле, чем во времена написания строк, взятых в качестве эпиграфа, стремление спецслужб не только слышать, но и видеть, читать и получать любую передаваемую по сетям связи мультимедийную информацию с целью предотвратить преступление является вполне оправданным. В результате конвергенции сетей и услуг связи эта информация начинает концентрироваться в сетях связи следующего поколения NGN (Next Generation Network). Среди услуг NGN мы выделим важные в контексте реализации СОРМ:

- речевое соединение (двустороннее или в режиме конференцсвязи) между пользователями сетей с коммутацией каналов (TDM-сетей) и сетей IP-телефонии;
- услуги Интеллектуальной сети – переадресация, бесплатный вызов, телеголосование, вызов по карте и пр.;
- доступ пользователей к IP-сети, предполагающий, в частности, обмен сообщениями электронной почты (e-mail), использование систем интерактивного обмена текстовыми сообщениями (chat), обмен HTTP-трафиком, обмен данными FTP и т. д.;
- в перспективе – видеосвязь между пользователями.

На начальных этапах развертывания NGN основной услугой будет оставаться голосовое соединение между пользователями сети с использованием аналоговых и цифровых (ISDN) телефонных аппаратов, подключаемых к NGN через универсальные устройства доступа.

Однако организация этого соединения в NGN имеет принципиальные отличия от его установления в традиционных телефонных сетях с коммутацией каналов. Это связано с тем, что медиатрафик (речь) и сигнальная информация для управления обслуживанием вызова в NGN передаются по различным маршрутам и обрабатываются разными сетевыми устройствами, а не единым узлом коммутации (АТС).

Медиатрафик проходит, как правило, непосредственно между шлюзами доступа (например, мультисервисными абонентскими концентраторами – МАК) или транспортными шлюзами. Сигнализация управления обслуживанием вызова проходит

через программные коммутаторы Softswitch [2], а в более простых случаях – через прокси-серверы SIP или привратники H.323, но всегда не там, где медиашлюзы и медиатрафик.

Аналогичная проблема наблюдается также при предоставлении услуги сеансового доступа пользователя к сети IP, когда узел сети, отвечающий за идентификацию пользователя, не участвует в передаче пользовательской информации.

Отсюда – невозможность получения пользовательской информации для СОРМ от единого устройства управления, определяющего параметры соединения по номерам вызывающего или вызываемого пользователя. Новый элемент NGN – пограничный контроллер сессий SBC (Session Border Controller), где естественным образом сходятся маршруты медиатрафика и сигнализации, – позволяет решить эту задачу в частных случаях. Но необходимость полного охвата СОРМ в сети связи требует общего решения для всех возможных вариантов архитектуры NGN. Это решение вынуждает реализовать функции СОРМ одновременно в нескольких сетевых устройствах, в том числе:

- в устройстве управления сетью (Softswitch, привратник, SIP-прокси) с целью постановки на контроль пользователя сети и получения относящейся к его вызову служебной информации;
- в устройстве сети, отвечающем за перенос пользовательской информации, с целью ее получения в интересах правоохранительных органов.

В [1] упоминалось, что требования к организации функций СОРМ для отечественных NGN будут оставаться весьма похожими на требования к законному перехвату сообщений ETSI и в некоторой степени на IETF и CALEA, согласно приведенной там табл. 2. Единственным отличием, скорее всего, будет организация взаимодействия между правоохранительными органами, в европейских стандартах именуемыми LEA (Law Enforcement Agency), и оператором/провайдером NWO/AP/SvP (NetWork Operator/ Access Provider/Service Provider) через интерфейс HI1.

Это отличие не оказывает существенного влияния на рассматриваемые здесь инженерные аспекты СОРМ, затрагивающие преимущественно интерфейсы HI2 и HI3 из стандартов ETSI. Реализацию этих интерфейсов, т. е. взаимодействие между пунктом управления ПУ СОРМ, в европейских спецификациях именуемым LEMF (Law Enforcement Monitoring Facility), и оборудованием оператора NWO/AP/SvP, предлагается производить путем использования специального устройства – Посредник

СОРМ (SORM Mediation). Оно, в свою очередь, связано с устройствами управления NGN – Softswitch, медиашлюзами, абонентским доступом, а также с маршрутизаторами сети IP.

Посредник СОРМ в данном случае будет исполнять роль конвертера сигнализации, аналогичного известным в отечественных сетях разработкам Протей или Малвин, а также конвертера (шлюза) медиапотоков для доставки пользовательской информации к ПУ СОРМ.

Такая архитектура представлена на рис.1. Здесь ПУ СОРМ – это пункт управления, применяющийся в существующих традиционных сетях с коммутацией каналов и связанный через интерфейсы 1 с Посредником СОРМ. Интерфейс 1 является стандартным интерфейсом команд и ответов СОРМ, аналогичным применяющимся в существующих сетях ТОМ.

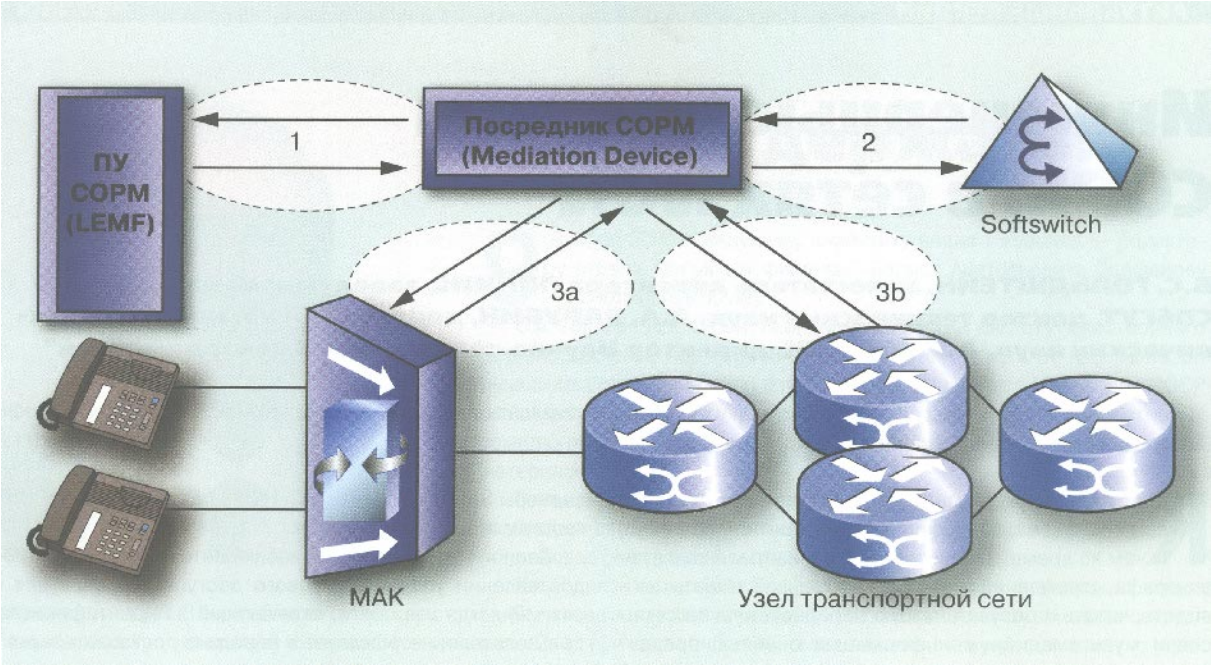

Рис. СОРМ в NGN

Интерфейс 2, используемый для взаимодействия Посредника СОРМ и устройства управления сетью с целью поставить пользователей на контроль, получать уведомления об их действиях в сети и пр., может быть не стандартным, а предлагаемым разработчиком интерфейсом. Согласование интерфейсов 1 и 3 обеспечивается Посредником, тем самым достигается независимость функций СОРМ от оборудования разных производителей.

Интерфейс 3 между Посредником и медиашлюзами (устройствами доступа или оборудованием транспортного уровня) предназначен для получения пользовательской

информации и тоже может настраиваться на определенный тип оборудования. Указанная схема близка к предложениям об обеспечении функций СОРМ, разработанным ETSI, что будет показано ниже.

Но прежде рассмотрим процесс проведения оперативно-розыскных мероприятий в NGN. Он будет выглядеть следующим образом. От ПУ СОРМ к Посреднику поступает стандартная команда поставить на контроль пользователя с некоторым идентификатором (интерфейс 1). Посредник обеспечивает установку триггерной точки для этого пользователя в устройстве управления Softswitch (интерфейс 2), для чего может быть применен нестандартный протокол, предлагаемый разработчиком.

При активизации триггерной точки Softswitch передает информацию об этом событии через интерфейс 2 к Посреднику, а далее эта информация поступает в ПУ СОРМ. Если необходимо произвести съем пользовательской информации, то по соответствующей команде от ПУ СОРМ Посредник через интерфейс 3 настраивает оборудование доступа или транспортного уровня на копирование пользовательского потока данных и передачу его к Посреднику. Затем эта информация передается в приемлемой форме к ПУ СОРМ.

Заметим, что такой подход соответствует документам ETSI [3 – 6] и комитета IETF [7] в области стандартизации решений СОРМ для NGN, разумеется, с учетом вышеупомянутых отличий российской СОРМ от законного перехвата сообщений по ETSI [1].

В концепциях, предлагаемых указанными организациями, основой СОРМ тоже является вышеупомянутый Посредник или Mediation Device (MD) – устройство, принимающее от пункта управления СОРМ запросы съема информации и определяющее посредством взаимодействия с сетевым устройством управления элемент сети, который обеспечивает транзит пользовательской информации. Съем и передачу в ПУ СОРМ пользовательской информации также производит этот Посредник.

Съем информации может производиться по нескольким сценариям, приведенным на рис. 1. В первом из них для копирования информации используется интерфейс 3a между Посредником и устройством доступа (например, мультисервисным абонентским концентратором), во втором сценарии съем пользовательской информации производится с одного из маршрутизаторов транспортного уровня NGN через интерфейс 3b.

Реализация интерфейса 3b между Посредником COPM и узлом транспортной сети (маршрутизатором) или специализированным устройством транзита медиапотоков (например, RTP-прокси) удобна в случае применения IP-телефонов, подключаемых к NGN без участия устройства доступа, такого как MAK. При этом для всех подобных терминалов сети или терминалов и идентификаторов пользователей, поставленных на контроль, может быть предусмотрен единый узел, в котором и будет производиться съем информации.

Кроме того, при использовании в сети таких терминалов необходимо предусмотреть механизмы принудительной маршрутизации к устройству управления сетью относящейся к ним сигнальной информации и данных.

Рассмотрим более детально процесс съема пользовательской информации. Сразу же отметим, что предлагаемая авторами архитектура близка к принципам, изложенным в документах IETF [7] и ETSI [3 – 6].

На рис. 2 представлена предлагаемая в документах IETF и ETSI архитектура, а на рис. 3 – архитектура для COPM, реализованная авторами.

На рис. 2 показаны следующие элементы архитектуры законного перехвата сообщений в NGN. Это LI AF (Llawful Intercept Admin Function) – функция, обеспечивающая передачу в приемлемом для сети виде запроса от LEA к Посреднику COPM поставить на контроль того или иного пользователя. Нужное преобразование и отправка запроса к Посреднику COPM может производиться с участием уполномоченного человека.

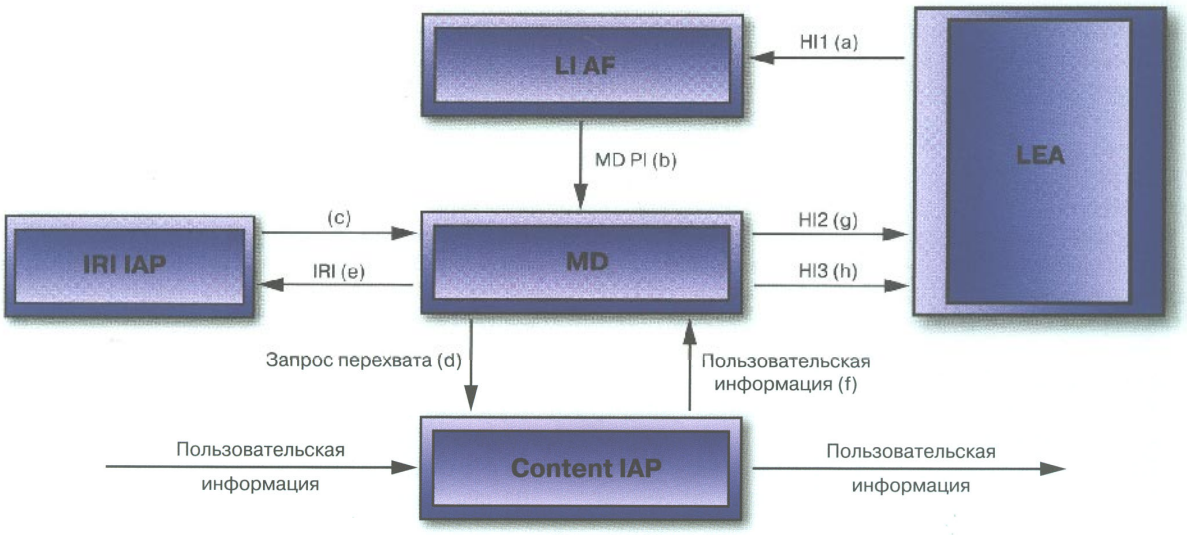

Рис. 2. Архитектура законного перехвата по IETF и ETSI

Сам Посредник COPM, названный Mediation Device (MD), – устройство, взаимодействующее с другими сетевыми устройствами с целью контроля действий пользователя в сети и съема пользовательской информации, которое конвертирует перехваченный трафик в требуемый LEA формат. Если несколько LEA контролируют одного и того же пользователя, MD должен создавать и отправлять копии перехваченной информации к каждому LEA. Действующие параллельно правоохранительные органы не имеют при этом информации друг о друге.

IAP (Intercept Access Point) – устройство, предоставляющее MD информацию о действиях пользователя в сети, или устройство, с которого производится съем пользовательской информации. Существуют два типа IAP:

IRI IAP (Intercept Related Information IAP) определяет устройство доступа, обслуживающее пользователя, или маршрутизатор, обрабатывающий поток пользовательских данных. Функции IRI IAP *в* NGN выполняет, например, Softswitch или сервер аутентификации и авторизации.

Content IAP – устройство, через которое проходит пользовательская информация и которое обеспечивает съем этой информации и передачу ее к MD.

Между элементами рассматриваемой архитектуры COPM действует следующий набор интерфейсов:

- НИ – Handover Interface 1, административный интерфейс, через который LEA передает к LI AF запрос поставить на контроль пользователя (имя, паспортные данные и т. п.);
- MD PI (MD Provisioning Interface) – интерфейс, управляющий Посредником MD, который переносит такие параметры, как идентификатор абонента, время, в течение которого будет вестись контроль, параметры контроля пользователя и т. д.;
- IRI IAP Provisioning Interface – интерфейс с IRI IAP для запроса данных о действиях пользователя в сети и данных, необходимых для съема пользовательской информации;
- Content Intercept Provisioning Interface – интерфейс, посредством которого Content IAP получает команду начать съем пользовательской информации; например, для маршрутизаторов Cisco – это команды протокола SNMPv.3;
- IRI to MD – интерфейс между IRI IAP и MD, с помощью которого доставляются данные о действиях пользователя в сети и данные, необходимые для съема пользовательской информации;
- Content to MD – интерфейс между Content IAP и MD для доставки перехваченной информации к MD;
- HI2 – интерфейс между MD и LEA для доставки данных о действиях пользователя;

- HI3 – интерфейс между MD и LEA для доставки пользовательской информации.

Возвращаясь от рассмотренной архитектуры IETF/ETSI к российским требованиям СОРМ, рассмотрим схему на рис. 3, являющуюся, по сути, результатом объединения рис. 1 и 2. В ней отсутствует интерфейс НИ, функции которого частично делегированы HI2; функции прочих интерфейсов практически не изменяются. Для большей наглядности на рис. 3 в скобках указаны также обозначения рис. 2.

Рис. 3. Архитектура для СОРМ для NGN

Представленная на рис. 3 архитектура апробирована в мультисервисном коммутаторе доступа Протей-МКД, являющемся первым и пока единственным отечественным Softswitch класса 5, в котором полностью реализованы и сертифицированы функции СОРМ.

Далее, чтобы не злоупотребить вниманием читателей, описывая собственную разработку вместо СОРМ в МКД, рассмотрим пример весьма близкой реализации законного перехвата в маршрутизаторах компании Cisco [8]. В терминах рассмотренной концепции рис. 2 и 3 они являются Content IAP или транзитными узлами пользовательской информации, соответственно, и обладают следующими возможностями:

- позволяют нескольким правоохранительным органам независимо и незаметно вести перехват пользовательской информации;
- используют протокол SNMP v.3 в интерфейсе (d), для чего оборудование поддерживает работу со специализированной базой MIB (Management Information Base), так называемой CISCO-TAP-MIB;
- ведя перехват пользовательской информации, инкапсулируют ее в UDP-пакеты и передают их на указанный сетевой адрес;

- перехваченная информация скрывается ото всех, кроме авторизованных пользователей СОРМ.

Выбор протокола SNMP для управления перехватом информации между Посредником СОРМ сети NGN и узлом, обрабатывающим поток данных контролируемого пользователя, представляется очень удобным с точки зрения реализации интерфейса как на стороне MD, так и на стороне оборудования, переносящего пользовательские данные. Этим достигается определенный уровень стандартизации интерфейса и в то же время его гибкость по отношению к разнотипному оборудованию многочисленных компаний-разработчиков за счет применения индивидуальных для каждого оборудования MIB. Принимая во внимание разнообразие услуг NGN и узлов, их предоставляющих, такой подход может оказаться единственным технически приемлемым.

Заключение

На основании вышеизложенного можно сформулировать характеристики СОРМ для сетей следующего поколения:

- при использовании Посредника СОРМ (MD) достижим порядок взаимодействия ПУ СОРМ с оборудованием сети NGN, не отличающийся от установленных правил взаимодействия ПУ СОРМ с оборудованием традиционных телефонных сетей;
- взаимодействие ПУ СОРМ с узлами NGN при посредничестве специализированного устройства MD позволит обеспечить независимость функций СОРМ от оборудования разных производителей, устанавливаемого BNGN;
- операции постановки пользователя на контроль, получения относящейся к его связи информации и т. п. реализуются Посредником MD при взаимодействии с Softswitch;
- операции съема пользовательской информации (прослушивания речи) могут производиться в устройствах сети доступа (например, мультисервисных абонентских концентраторах или медиашлюзах); возможен также съем пользовательской информации с узлов транспортной сети;
- интерфейс между Посредником и устройством управления сетью NGN сегодня не стандартизирован, что требует адаптации Посредника к различным интерфейсам с Softswitch;
- интерфейс между Посредником и устройствами уровня доступа или транспортного уровня также не стандартизирован, а наиболее удобной представляется его реализация средствами протокола SNMP.

Литература

1. Б. С. Гольдштейн, Ю. А. Крюков, И. П. Хегай. Инженерные аспекты СОРМ/ Вестник связи. - 2005. № 9.
2. Б.С. Гольдштейн. Системы коммутации. Учебник для ВУЗов. 2-е издание, доп. и испр.//СПб.: BHV-2004.
3. ETSI TR 101 943 V2.1.1 (2004-10). Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture.
4. ETSI TS 101 878 V4.1.1 (2003-11). Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Service Capability Definition; Service Capabilities for TIPHON Release 4.
5. ETSI TS 102 227 V4.1.1 (2004-05). Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception.
6. ETSI TS 102 232 V1.3.1 (2004-10). Lawful Interception (LI); Handover specification for IP delivery.
7. Baker F., Foster B., Sharp C. Cisco Architecture for Lawful Intercept in IP Networks. IETF RFC 3924, October 2004.
8. Cisco 10000 Series Router. Lawful Intercept Configuration Guide. Version I 1.0. August 2004.