Новая парадигма законного перехвата сообщений в NGN/IMS

Б. ГОЛЬДШТЕЙН, заведующий кафедрой СПбГУТ, доктор технических наук, профессор, В. ЕЛАГИН, научный сотрудник НТЦ «Протей», Ю. КРЮКОВ, научный сотрудник ЛОНИИС, Ю. СЕМЕНОВ, директор ООО «Протей-Спецтехника»

Написав очередную (седьмую) книгу из серии «Телекоммуникационные протоколы», посвященную СОРМ [1], и подборку статей о разных инженерных аспектах законного перехвата (ЗП) сообщений в нескольких номерах журнала «Вестник связи», авторы понадеялись, что этого будет достаточно, что исчезло еще одно белое пятно на карте современных телекоммуникационных протоколов. Что благодаря затраченным усилиям (книга писалась нелегко и к тому же была неоднозначно встречена отдельными читателями, полагавшими, что важнее засекретить инженерную проблему, чем найти ее решение) удалось относительно подробно обсудить инженерные аспекты интерфейсов СОРМ в сетях подвижной и фиксированной телефонной связи, в том числе и при переходе к NGN. Но эти усилия оказались недостаточными, темпы революционных перемен в инфокоммуникациях опередили самые смелые прогнозы. Неизмеримо усложнилась и проблематика ЗП сообщений, что наглядно продемонстрировала прошедшая в Праге 2 – 6 июня 2009 г. Международная конференция ISS World Europe-2009 (Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering). Активное участие в этом международном форуме приняли четыре отечественные компании, что вселяет надежду на активное участие российских программистов в этой важной области современного телекоммуникационного рынка.

СОРМ в TDM-сетях

Основная обсуждавшаяся в [1] схема подключения оборудования СОРМ к узлу коммутации в телефонной сети общего пользования (ТфОП) и в сетях подвижной связи (СПС) приведена на рис. 1.

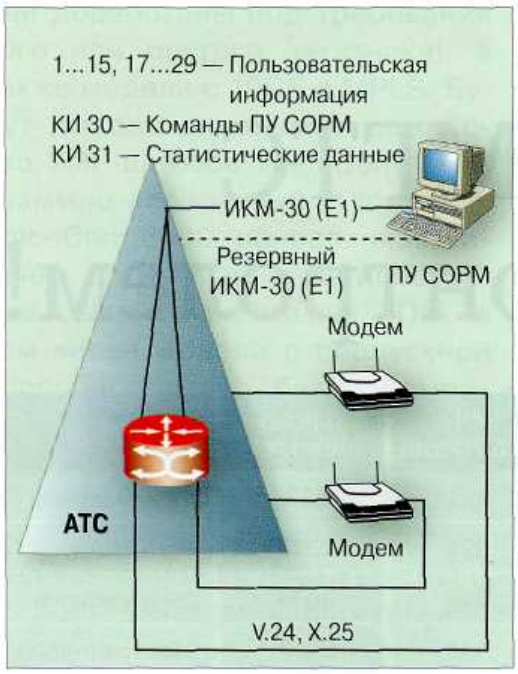

Рис. 1. Схема подключения оборудования СОРМ в традиционной ТфОП

Принятая в РФ архитектура построения СОРМ предусматривает наличие специального административного канала для передачи управляющих сообщений. Данный интерфейс носит название канал 1 и может быть отдельным модемным каналом, либо организуется в 30-канальном интервале тракта ИКМ-30/32, как это показано на рис. 1. При помощи данного канала пульт управления (ПУ) управляет работой модуля СОРМ на станции и самостоятельно передает команды об установке пользователя на контроль, снятии его с контроля, запрос на передачу статистической информации и т. д.

Протоколом обмена данными между СОРМ и ПУ первоначально был выбран протокол X.25, а в качестве физического уровня используется интерфейс V.24 (V.35). Осуществляемый сегодня переход от протокола передачи X.25 к протоколу TCP/IP позволяет упростить и ускорить создание федеральной сети СОРМ. Так или иначе, СОРМ представляет собой процесс получения статистической информации о вызовах и/или перехват информации (речевых переговоров, текстовых, мультимедийных сообщений и т. д.) поставленного на контроль пользователя. Эти две категории носят названия: статистический контроль – данные о вызове и данные по зарегистрированному терминалу (идентификаторы абонента и терминала, время, длительность вызова, категория абонента, ФИО и т. п.) и полный: контроль – данные статистического контроля, запись переговоров, перехват пользовательской информации.

Инженерная проблематика СОРМ в TDM-сетях характеризуется следующими факторами:

- одна и та же сеть для сигнализации и передачи контента;
- один коммутируемый канал на соединение;
- ограниченность управления установлением соединения и самого установления соединения границами одного и того же региона;
- взаимно-однозначное соответствие между сервисом и предоставляющей этот сервис сетью;
- универсальная точка доступа для СОРМ (обычно АТС для ТфОП, MSC для СПС);
- ограниченность границами региона;
- универсальный интерфейс для стационарного подключения оборудования СОРМ.

С позиций сегодняшних проблем видно, насколько вышеприведенные факторы облегчают реализацию статистического и полного контроля для организации ЗП сообщений.

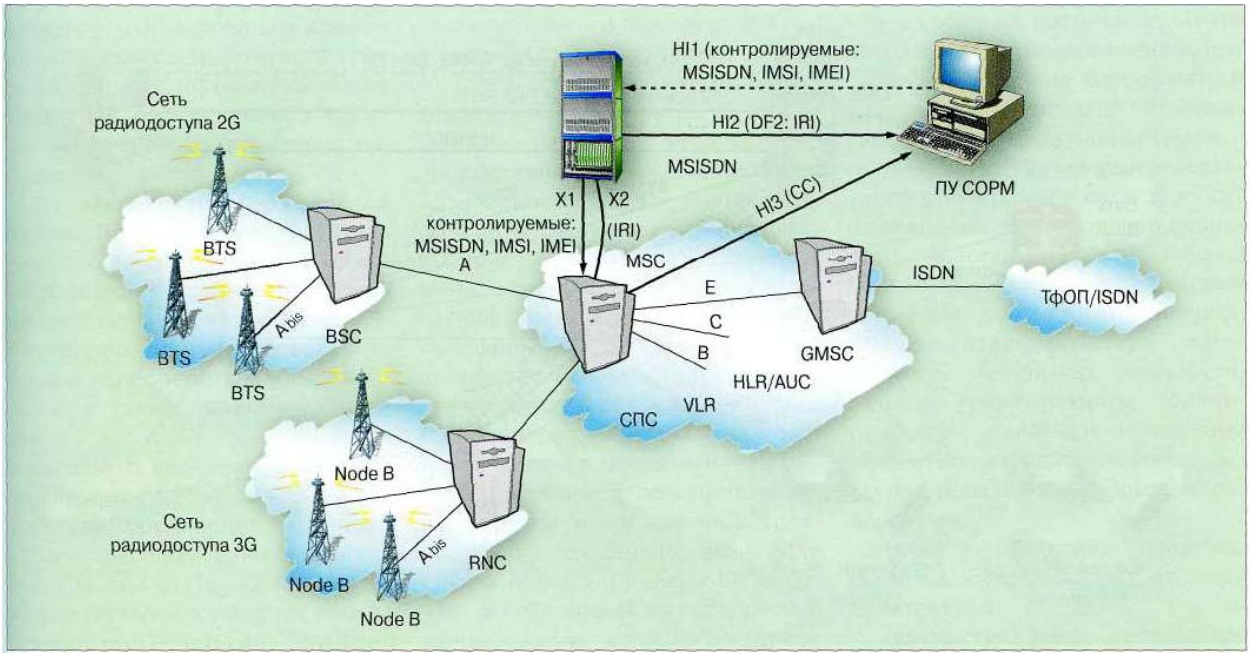

Рис.2. Реализация СОРМ в традиционной СПС поколений 2 и 3G

Новые проблемы в современных мультисервисных сетях

Современный этап конвергенции сетей фиксированной и мобильной связи и построения конвергентной мультисервисной сети характеризуется новыми факторами, весьма существенными в контексте проблематики ЗП сообщений. Это независимость услуг (речь, e-mail, SMS) и средств доступа к ним (рис. 3), т. е. разные сервисы могут быть доступны с одной и той же точки доступа, а один и тот же сервис – с разных, а также независимость сигнализации и поставки контента, т. е. сигнализация и поставка контента обрабатываются разными провайдерами (что существенным образом усложняет процесс реализации ЗП, рис. 3), причем обрабатывающий сигнализацию провайдер не имеет доступа к контенту, а контент-провайдер обычно ничего не знает о сессии, которая должна быть под контролем. Эти факторы требуют обязательной кооперации между контент-провайдером и оператором, обрабатывающим сигнализацию.

Таким образом, для подключения оборудования различных сетей требуются разнообразные устройства взаимодействия – медиаторы (Mediation Device), которые позволили бы передавать различные виды информации (голос, видео, e-mail и т. д.) на единый ПУ СОРМ. Сегодня специализированные компании предлагают отдельные устройства сопряжения или целые системы СОРМ, которые позволяют обеспечить полноценный комплекс мероприятий ЗП сообщений в мультисервисных сетях.

Новыми, общими для всех этих решений проблемами являются отделение доступа к услугам от самих услуг, отделение сигнализации от контента, отсутствие у провайдера услуг информации о выбранном доступе к этим услугам, различные провайдеры доступа, сигнализации и услуг, например, в архитектуре IMS. Отсюда следует необходимость постановки на контроль самого факта доступа к услуге для заданного пользователя, а также всех остальных возможных для него способов доступа к этой услуге в реальном времени. В противном случае задача СОРМ может считаться не выполненной.

Практическая реализация законного перехвата

Рассмотрим организацию архитектуры ЗП на сети оператора связи/провайдера доступа и услуг на основе IETF RFC 3924, который идентичен общеевропейским стандартам [3]. Общее описание архитектуры ЗП с детализацией используемого на стороне оператора связи/провайдера доступа и услуг оборудования представлено на рис. 4.

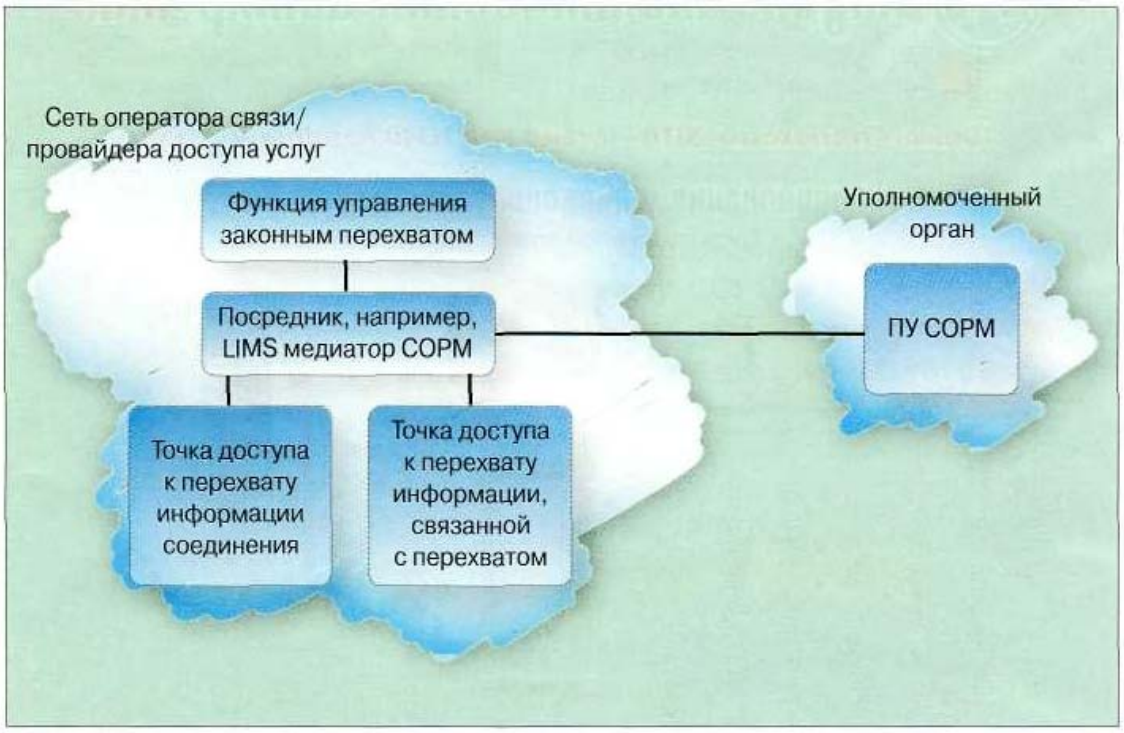

Рис. 4. Архитектура ЗП с детализацией используемого на стороне
оператора связи/провайдера доступа и услуг оборудования

Функция управления перехватом используется оператором связи/провайдером доступа и услуг для обеспечения ЗП информации через взаимодействие с сетевыми компонентами. Задачами этой функции являются обеспечение формирования сетевых точек перехвата, а также контроль и поддержка получения информации перехвата.

В дополнение к этому функция управления ЗП отвечает за безопасность и целостность осуществляемого перехвата путем постоянного мониторинга активных логов на предмет обеспечения исключительно санкционированного перехвата в соответствии с целевыми критериями объекта наблюдения. Формирование сетевых точек перехвата заключается в посылке соответствующим сетевым элементам определенного перечня настроечных характеристик, позволяющих осуществить ЗП.

Посредник поддерживается NWO/AP/SvP, являясь центром процессов обеспечения ЗП. Задачей посредника является отправка соответствующих команд различным точкам доступа к перехвату для его непосредственной реализации, а также прием информации перехвата (IRI – информации, связанной с перехватом – Intercept Related Information и CC – информации соединения – Content of Communication) с последующей ее доставкой на ПУ СОРМ. В литературе термину посредник иногда соответствует термин "функция доставки" (delivery function). В некоторых случаях посредник осуществляет фильтрацию получаемой информации.

Кроме обозначенных задач, одной из основных функций посредника является конвертация получаемой от сетевых элементов информации в информацию, определенную национальной нормативной базой, для ее последующей передачи на ПУ. Посредники производства НТЦ «Протей» осуществляют и определенную стандартами возможность по конвертации специфических внутрифирменных протоколов в определенные национальной нормативной базой форматы.

В целом для российского рынка, а также стран, использующих российский СОРМ, создание универсального посредника, способного преобразовывать данные, получаемые в формате ETSI, в данные формата СОРМ и обратно, является экономически оправданным, так как позволит существенно упростить процедуру сертификации и использования оборудования иностранного производства на отечественных сетях.

Для производителей инфоком-муникационного оборудования характерна ситуация, когда функция управления перехватом, посредник и ПУ не относятся к нему непосредственно и являются оборудованием третьей стороны.

Точка доступа к перехвату информации, связанной с перехватом, является устройством, предоставляющим посреднику идентификационную информацию. Для речевых коммуникаций IRI может представлять собой номера вызывающего и вызываемого пользователей, а также IP-адреса и время соединения. Также IRI описывает и все остальные действия целевого объекта, связанные с перенаправлением вызовов или вовлечением в соединение третьих лиц, например, переадресацию вызова или использование трехсторонней конференцсвязи. Для случая передачи данных IRI включает в себя время установления и конца сессии, а также IP-адреса отправителя и получателя. Для ЗП речевых коммуникаций IRI определяется, например, на SIP-прокси или H.323-шлюзе, а для трафика данных – на сервере аутентификации, авторизации и учета.

Точка доступа к перехвату информации соединения является устройством, на котором осуществляется непосредственный перехват пользовательского контента целевого объекта, копирование этого контента и его последующая переадресация посреднику. Точка доступа для перехвата информации соединения должна располагаться максимально близко к пользовательскому оборудованию целевого объекта, чтобы минимизировать число обращений к себе для осуществления перехвата, что позволит осуществить гарантированный перехват информации. Сетевые элементы, с которыми непосредственно взаимодействует пользователь, например, маршрутизаторы, концентраторы, мультиплексоры, являются примерами эффективного выбора точки доступа к перехвату информации соединения.

Ниже перечислены основные преимущества рассматриваемой архитектуры:
- архитектура унифицирована для перехвата речи, видео и данных;
- управление процессами ЗП осуществляется посредником, а не оборудованием управления сеансами связи;
- управление процедурой ЗП отделено от процедур управления сеансами связи;
- общий интерфейс к посреднику и устройству управления сеансами связи;
- модульная архитектура легко адаптируема к национальным и региональным требованиям за счет возможности быстрой конфигурации посредника.

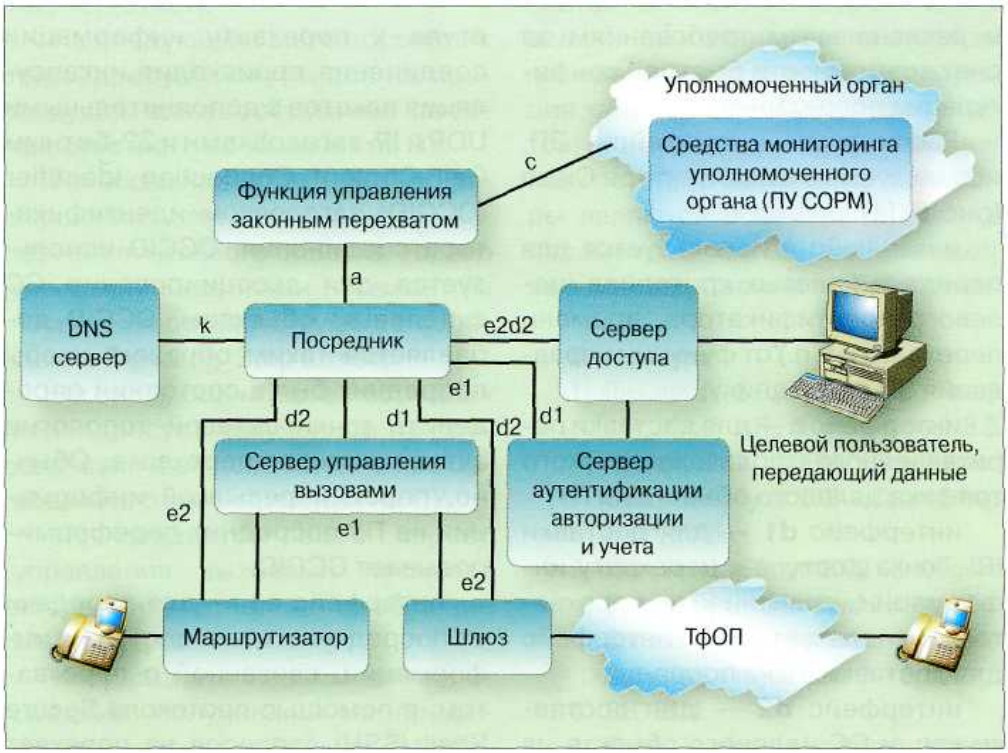

Рис. 5. Интерфейсы ЗП голосовой информации

Рассмотрим интерфейсы ЗП, используемые в архитектуре Cisco (рис. 5) [4]:

- интерфейс **a** используется для передачи целевых критериев (целевого идентификатора, времени перехвата и т. п.) от функции управления ЗП посреднику;
- интерфейс **c** – для доставки перехваченного пользовательского трафика целевого объекта на ПУ;
- интерфейс **d1** – для доставки IRI. Точка доступа к перехвату информации, связанной с перехватом, использует этот интерфейс для доставки IRI на посредник;
- интерфейс **d2** – для доставки копии СС целевого объекта на посредник. При этом в точке доступа к перехвату информации соединения происходит инкапсуляция пакетов с дополнительными UDP и IP-заголовками и 32-битным Call Content Connection Identifier (CCCID) заголовком идентификатора соединения. CCCID используется для ассоциирования СС с целевым объектом. CCCID добавляется таким образом, чтобы посредник был в состоянии определить точки сетевой топологии актуальные для перехвата. Обычно, перед пересылкой информации на ПУ посредник переформировывает CCCID;
- интерфейс **e1** – для передачи от посредника точке доступа к информации, связанной с перехватом, с помощью протокола Secure Shell (SSH) запросов на перехват (конфигурационных команд);
- интерфейс **e2** – для передачи от посредника точке доступа к перехвату информации соединения с помощью протокола Simple Network Management Protocol версия 3 (SNMPv3) запросов на передачу СС целевого объекта;
- через интерфейс **k** посредник запрашивает сервер доменных имен (Domain Name Server – DNS) полное доменное имя точки доступа к перехвату информации соединения.

На рис. 6 проиллюстрирован пример реализации процедуры ЗП применительно к архитектуре рис. 5 с использованием сообщений североамериканского стандарта CALEA, более подробно описанного, например, в [1] (показана процедура взаимодействия сетевых компонентов для перехвата речевой информации на шлюзе или пограничном маршрутизаторе) [4].

Использование сообщений CALEA позволяет проиллюстрировать универсальность архитектуры ЗП с применением посредника, позволяющего адаптироваться под национальные и региональные стандарты.

Опишем гипотетический процесс реализации ЗП согласно рис. 6.

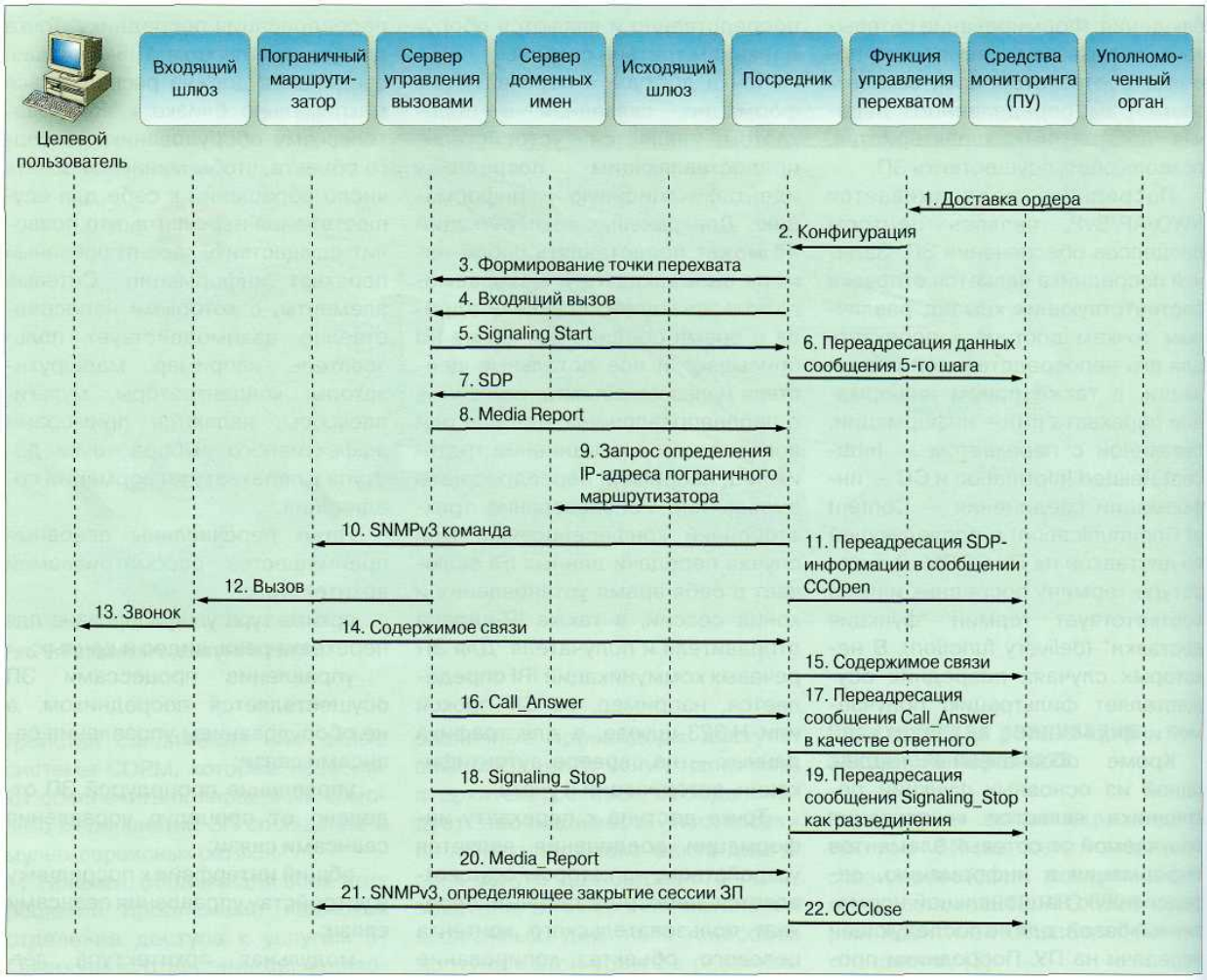

Рис. 6. Пример реализации процедуры ЗП

На первом шаге происходит физическая доставка ордера санкционирующего ЗП от уполномоченного органа администратору NWO/AP/SvP, отвечающему за функцию управления перехватом.

На втором шаге происходит конфигурация процедуры ЗП для целевого пользователя на основе полученного ордера путем определения точек перехвата функцией управления перехватом.

С использованием полученной конфигурации посредник на третьем шаге посылает непосредственные конфигурационные команды серверу управления вызовами для организации ЗП (запрос).

Целевому объекту поступает входящий вызов – шаг четыре.

На пятом шаге сервер управления вызовами посылает посреднику сообщение Signaling Start – совокупность IRI (отчет).

На шестом шаге происходит передача от посредника на ПУ соответствующего событию сообщения, содержащего полученную на пятом шаге информацию (в соответствии с возможностями используемого посредника формат этого сообщения может определяться национальными и региональными требованиями).

На седьмом шаге исходящий шлюз посылает серверу управления вызовами информацию Session Definition Protocol (SDP).

На восьмом шаге сервер управления вызовами посылает посреднику сообщение Media_Report – совокупность IRI, содержащее SDP-данные седьмого шага (отчет).

На следующем шаге посредник обращается к серверу доменных имен с целью определения IP-адреса пограничного маршрутизато ра (базируясь на IP-адресе целевого шлюза) – запрос.

На десятом шаге посредник инициирует перехват на пограничном маршрутизаторе или сетевом сервере доступа с использованием информации протокола SNMPv3 (запрос).

На одиннадцатом шаге посредник пересылает SDP-информацию, полученную на предыдущих шагах, на LEMF в сообщении ССОреп.

На двенадцатом шаге входящее соединение устанавливается от сервера управления вызовами до входящего шлюза.

На тринадцатом шаге входящий шлюз посылает вызывной сигнал на терминальное оборудование целевого объекта.

На четырнадцатом шаге устанавливается пользовательское соединение из конца в конец. Пограничный маршрутизатор или сетевой сервер доступа перехватывает информацию пользовательского соединения и пересылает все голосовые пакеты, соответствующие этому целевому соединению, посреднику (отчет).

На пятнадцатом шаге посредник пересылает СС целевого объекта на ПУ.

На шестнадцатом шаге сервер управления вызовами посылает посреднику сообщение Call_Answer (отчет).

На следующем шаге посредник переадресует полученное на предыдущем шаге сообщение в качестве ответного сообщения на ПУ.

На восемнадцатом шаге, по завершении пользовательского соединения целевого объекта, сервер управления вызовами посылает на посредник соответствующее сообщение Signaling Stop (отчет).

На следующем шаге посредник переадресует полученное на предыдущем шаге сообщение как сообщение о разъединении на ПУ.

На двадцатом шаге сервер управления вызовами посылает посреднику отчет – сообщение MediaReport.

На двадцать первом шаге посредник, получивший на предыдущем шаге сообщение Media_ Report, посылает пограничному маршрутизатору или сетевому серверу доступа сообщение SNMPv3, определяющее закрытие сессии ЗП. При этом регламентирована посылка трех сообщений о закрытии сессии ЗП: по одному для каждого пользовательского потока СС участника соединения и одного для посредника.

На двадцать втором шаге посредник посылает на ПУ сообщение CCCIose.

Исследовательские аспекты СОРМ

При проектировании систем ЗП особое внимание необходимо уделить временным характеристикам мероприятия. В текущих требованиях к СОРМ конкретно прописаны граничные значения основных характеристик, например, канал передачи данных должен обеспечивать коэффициент ошибок по битам не более 10 , при коэффициенте ошибок по битам в линии связи не более 10 и соотношении сигнала/шум плюс 12 дБ; время реакции СОРМ (с момента регистрации события на станции до момента записи информации о данном событии в порт передачи) при ее работе в реальном масштабе времени должно быть не более 200 мс.

Если коэффициент потерь является достаточно субъективной величиной и зависит от технологии передачи информации (коммутация каналов или коммутация пакетов) и не может быть единым для всех сетей, то временные параметры являются объективно важным параметром при ЗП, который должен соблюдаться на любой сети.

Литература

1. Гольдштейн Б.С., Крюков Ю.С., Пинчук А.В., Хегай И.П., Шляпоберский В.Э., «Интерфейсы СОРМ. Справочник», Санкт-Петербург, «БХВ - Санкт-Петер бург», 2006.
2. ISS World Europe-2009 (Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering). Prague, June 2-6, 2009.
3. RFC 3924.
4. Cisco Service Independent Intercept Architecture Version 3.0.