**Инженерные аспекты СОРМ**

Б.С. ГОЛЬДШТЕЙН, заведующий кафедрой СПбГУТ, заместитель директора ЛОНИИС, доктор технических наук, профессор, Ю.А. КРЮКОВ, научный сотрудник, И.П. ХЕГАЙ, директор ГК "Экран"

"Все телефоны не подслушаешь,

Все разговоры не запишешь.

И люди пьют, едят и кушают,

И люди понемногу дышат,

И понемногу разгибаются,

И даже тихо улыбаются."

Б. Слуцкий

**Понятие СОРМ**

Относительная важность тех или иных функциональных возможностей коммутационных узлов и станций меняется во времени. Передача факсов, конференцсвязь, dial-up доступ в Интернет и другие экзотические дополнительные услуги телефонных сетей общего пользования (ТфОП) превратились в неотъемлемые функции современных систем коммутации. По независящим от связистов обстоятельствам к таким же обязательным и важным функциям отнесли поддержку АТС законного перехвата сообщений или, по-русски, систему оперативно-розыскных мероприятий (СОРМ).

За годы, прошедшие с тех пор как были написаны строки, выбранные в качестве эпиграфа к этой статье, к большому сожалению, обстановка в мире превратила СОРМ из весьма сомнительного требования в бесспорную и абсолютно необходимую функцию узлов коммутации современных сетей связи.

Под СОРМ в ТфОП понимается юридически санкционированный доступ правоохранительных организаций к частным телефонным разговорам. Этим уполномоченным организациям, именуемым в международных стандартах LEA (Law Enforcement Agency), принадлежат так называемые пункты управления ПУ (в российской терминологии) или, согласно терминологии ETSI, средства мониторинга, принадлежащие правоохранительному органу LEMF (Law Enforcement Monitoring Facility), обсуждение которых выходит за рамки этих статей.

Основное внимание мы уделим требованиям, предъявляемым СОРМ к узлам коммутации и сводящимся к необходимости организовать канал для прослушивания в ПУ контролируемого разговорного тракта, а также канал передачи от ПУ к станции специальных команд управления и от станции к ПУ сообщений о фазах контролируемых соединений. По этому же каналу передачи данных оператор ПУ имеет возможность взаимодействовать с программным обеспечением узла коммутации с помощью команд и сообщений, а станция — транслировать к ПУ аварийные сообщения о тех событиях, которые могут влиять на работу СОРМ.

Реализация этих требований является отнюдь не тривиальной инженерной задачей для АТС сети коммутации каналов [2], а для гибких коммутаторов Softswitch сетей NGN (о чем следующая статья [6] этого цикла) становится еще сложнее и интереснее. Но сначала — о сути проблемы.

Законный перехват сообщений

Функция СОРМ в терминах концепции ETSI называется законным перехватом сообщений LI (Lawful Interception) и, по мнению авторов, достаточно точно отражает суть дела. Имеются некоторые различия в практике применения этих двух терминов. СОРМ в странах СНГ до последнего времени предназначалась преимущественно для традиционной телефонии, в то время как международные стандарты LI разрабатывались более комплексно, без разделения на способы связи и методы коммутации, ориентируясь исключительно на контент [3, 4].

Кроме того, имеется некоторое отличие в начальной организации процедуры взаимодействия ПУ и LEA с оператором связи, о чем будет сказано ниже. С учетом этих двух нюансов, законный перехват сообщений LI используется в этой статье как синоним СОРМ.

Участники процесса законного перехвата сообщений и их роли

Таблица 1

|  |  |
| --- | --- |
| Участник | Роль |
| Уполномоченный орган (суд) | Судебный или административный орган выдает LEA законное разрешение — ордер на перехват сообщений |
| Правоохранительный орган (LEA) | LEA обращается к NWO/AP/SvP для перехвата информации согласно ордеру и получает результаты перехвата (СС и IRI), касающиеся определенного объекта. Несколько LEA могут в одно и то же время запросить перехват информации соединений одного и того же объекта |
| Сетевой оператор (NWO) | Оператор NWO эксплуатирует сеть связи и отвечает за обеспечение перехвата информации и ее передачи в LEA через HI. Несколько NWO могут использоваться для перехвата информации соединения одним и тем же LEA |
| Провайдер услуг (SvP) | Провайдер услуг SvP предоставляет пользователям услуги в дополнение к существующим на сети и отвечает за поддержку организации перехвата сообщений в NWO |
| Провайдер доступа (АР) | Провайдер доступа АР обеспечивает доступ пользовательского терминала к сети связи |
| Объект наблюдения | Объект наблюдения, который является пользователем услугами NWO/AP/SvP, соответствует идентификатору перехвата. Под идентификатором перехвата понимается технический параметр, например, списочный номер объекта наблюдения, причем один объект наблюдения может иметь несколько идентификаторов перехвата. Ни объект наблюдения, ни другие стороны, вовлеченные им в связь, не должны быть способны обнаружить факт перехвата |
| Производители телекоммуникационного оборудования | Производители обеспечивают реализацию соответствующих элементов архитектуры законного перехвата в производимом оборудовании, которое развернуто и используется NWO/AP/SvP. Функциональные возможности оборудования разных производителей должны обладать возможностью объединения в общей телекоммуникационной инфраструктуре |

Законный перехват сообщений определен ETSI как процесс обеспечения общественной безопасности, в котором оператор сети, провайдер доступа/провайдер услуг (NWO/AP/SvP — NetWork Operator/Access Provider/Service Provider) предоставляет официальным уполномоченным лицам доступ к частной информации, например, к телефонным разговорам или сообщениям электронной почты какого-либо лица или организации.

Это определение охватывает системы СОРМ в разных странах, внедряющих соответствующее оборудование законного перехвата, разрабатывающих регламентирующие его использование законодательные акты и инженерные решения, создающих международные рабочие группы стандартизации спецификаций СОРМ.

Распространение сетей разных типов за пределы национальных границ, происходящее на фоне конвергенции телекоммуникационных технологий и услуг, заставляет иначе взглянуть на процедуры СОРМ в рамках национальных стандартов, выдвигая на первый план концепцию стандартов ETSI.

К тому же в ней, помимо охвата традиционной и сотовой телефонии, предполагается реализация процедур LI для услуг Интернета, таких как: web-серфинг, e-mail, чат, ICQ, IP-телефония, ftp, telnet и др. Исследуются проблемы зашифрованного трафика: безопасной e-mail (PGP, S/MIME), безопасного серфинга с использованием HTTPS (SSL, TLS),

VPN (IPSec), зашифрованной IP-телефонии (pgp-phone, Nautilus) и т. д., для решения которых рассматриваются два пути — дешифрование информации перед ее передачей к средствам мониторинга, принадлежащим правоохранительным органам, или обеспечение этим органам доступа к ключам шифрования.

Европейские стандарты

Общеевропейские стандарты законного перехвата сообщений стремятся гармонизировать национальные документы, опираются на них и, в конечном итоге, призваны их заменить. Схема законного перехвата сообщений согласно общеевропейской концепции показана на рис. 1.

Правоохранительный орган LEA (Law Enforcement Agency) при намерении организовать процедуру законного перехвата сообщений подает через уполномоченный орган, например, суд, заявку на получение ордера, представляемого затем в NWO/AP/SvP через административный интерфейс НИ.

Когда ордер получен, средства мониторинга, принадлежащие правоохранительному органу LEMF (Law Enforcement Monitoring Facility), получают через порты интерфейса HI2 и HI3 информацию соединения СС (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. п.

Ордер может описывать IRI и СС для конкретного случая перехвата, период действия и предмет перехвата, адрес 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. Общеевропейские же спецификации содержатся в двух основных стандартах ETSI.

Первый из них, ETSI TS 101 671 "Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic" [3], определяет интерфейс взаимодействия с техническими средствами правоохранительных органов, ведущими мониторинг, и является в определенном смысле рамочным, предполагающим возможность выбора элементов спецификации интерфейса для того, чтобы соответствовать национальному законодательству, национальным требованиям и правилам конкретного правоохранительного органа.

В стандарте ETSI ES 201 158 "Telecommunications security; Lawful Interception (LI); Requirements for network functions" [4] определяются требования к сетевым функциям и детализируется обобщенная структура реализации законного перехвата сообщения, причем для каждой страны возможна ее трансформация в соответствии с национальным законодательством.

В определяемой этими стандартами концепции ETSI упоминаются участники процесса СОРМ, приведенные в табл. 1 вместе с их ролями.

Механизмы организации СОРМ в концепции ETSI

Рассмотрим алгоритм организации законного перехвата сообщений в рамках концепции ETSI. Базируясь на приведенном в табл. 1 перечне, рассмотрим действия участников процесса законного перехвата в упрощенном виде:

Шаг 1. LEA запрашивает у уполномоченного органа разрешение на ведение законного перехвата.

Шаг 2. Уполномоченный орган выдает LEA ордер на ведение законного перехвата

Шаг 3. LEA передает законное разрешение NWO/AP/ SvP, который, в свою очередь, определяет объекты наблюдения и контрольные идентификаторы, соответствующие полученному ордеру.

Шаг 4. NWO/AP/SvP организует перехват сообщений для/от определенных объектов наблюдения.

Шаг 5. NWO/AP/SvP сообщает LEA о готовности к законному перехвату сообщений конкретного объекта наблюдения.

Шаг 6. NWO/AP/SvP получает сведения об IRI и СС контролируемого объекта.

Шаг 7. Данные об IRI и СС контролируемого объекта передаются от NWO/AP/SvP к LEMF/LEA.

Шаг 8. По запросу LEA или по истечении периода действия законного разрешения на перехват NWO/AP/SvP прекращает процедуру перехвата.

Шаг 9. NWO/AP/SvP объявляет LEA о прекращении процедуры законного перехвата.

Для специальных команд, реализующих перехват, как правило, требуются следующие параметры:

идентификатор перехвата; идентификатор объекта—параметр, определяемый в ордере, например, указанный номер;

адрес средств ведения мониторинга правоохранительным органом (ПУ) для передачи СС;

адрес средств ведения мониторинга правоохранительным органом для передачи IRI;

адресные параметры для средств ведения мониторинга правоохранительным органом (например, для аутентификации и безопасности);

резервный маршрут;

идентификаторы NWO/AP/SvP.

Синтаксис необходимых команд может различаться в национальных применениях. В отечественных системах СОРМ, например, он определяется выбранным протоколом Х.25.

В условиях современной телекоммуникационной сети объект наблюдения может подписаться на услуги, предлагаемые несколькими провайдерами SvP, и имеет возможность выбрать один или более доступов АР (двухпроводная абонентская линия, ADSL-модем и др.) и операторов сети связи NWO (местная телефонная сеть, оператор междугородной связи и др.). Такая ситуация требует сотрудничества между операторами и провайдерами услуг при реализации СОРМ.

Если SvP использует среду нескольких АР и NWO, необходима организация их взаимодействия для реализации законного перехвата. Для выполнения процедуры перехвата требуется предоставление всей необходимой (но не более) эксплуатационной информации от АР и/или от NWO, касающейся объекта наблюдения и используемых им услуг.

**Список литературы**

Журнал «Вестник связи» №9, 2005 г.