Б.С. Гольдштейн, Ю.С. Крюков, А.В. Пинчук, И.П. Хегай, В.Э. Шляпоберский

СПРАВОЧНИК

ПО ТЕЛЕКОММУНИКАЦИОННЫМ ПРОТОКОЛАМ

Интерфейсы СОРМ

Б.С. Гольдштейн, Ю.С. Крюков, А.В. Пинчук, И.П. Хегай, В.Э. Шляпоберский

Серия справочников
«Телекоммуникационные протоколы ЕСЭ РФ»

Интерфейсы СОРМ

Справочник

Санкт-Петербург
«БХВ-Петербург»
2014

УДК 621.395
ББК 32.88
Г63

Гольдштейн, Б.С.

Интерфейсы СОРМ. Справочник / Б.С. Гольдштейн, Ю.С. Крюков, А.В. Пинчук, И.П. Хегай, В.Э. Шляпоберский. — СПб.: БХВ-Петербург, 2014. — 160 с.: ил.

ISBN 978-5-9775-2730-9

Рассматриваются интерфейсы коммутационных узлов и станций со средствами поддержки оперативно-розыскных мероприятий (СОРМ) в сетях связи, как традиционных, с коммутацией каналов и пакетов, так и перспективных сетях следующего поколения NGN. Излагаются задачи поддержки СОРМ в узлах коммутации и пути их решения в России и в других странах. Обсуждаются особенности решения этих задач в стационарных сетях – телефонных, передачи данных – и в сетях подвижной связи. Особое внимание уделяется протоколам СОРМ, их конвертированию и тестированию, а также сетевым аспектам пунктов управления СОРМ, их распределенной организации и архитектуре. Рассматриваются современные реализации оборудования СОРМ в коммутационных узлах и станциях и перспективы их развития.

Справочник

ISBN 978-5-9775-2730-9

Издательство «БХВ-Петербург», 190005, Санкт-Петербург, Измайловский пр., 29

Содержание

Предисловие 6

Глава 1. Законный перехват сообщений 9

1.1. Поддержка функции СОРМ в АТС 9
1.2. Понятие законного перехвата сообщений 10
1.3. Европейские стандарты 11
1.4. Механизм организации СОРМ в концепции ETSI 14
1.5. Интерфейсы законного перехвата ETSI 16
1.6. CALEA и другие стандарты СОРМ 20
1.7. Канал передачи данных к ПУ в российском СОРМ 25

Глава 2. СОРМ в телефонной сети общего пользования 29

2.1. Функции поддержки СОРМ для ТфОП 29
2.2. СОРМ в оконечных узлах 30
2.3. СОРМ в транзитных и оконечно-транзитных узлах 31
2.4. Команды из ПУ в оборудование СОРМ 32
2.5. Сообщения от оборудования СОРМ к ПУ по каналу 1 44
2.6. Информационные сообщения от оборудования СОРМ к ПУ по каналу 2 55
2.7. Дополнительные сообщения от оборудования СОРМ к ПУ по каналу 2 65
2.8. Методика проведения испытаний 66

Глава 3. СОРМ в сетях подвижнойсвязи 67

3.1. Организация СОРМ в сетях подвижной связи 67
3.2. Интерфейс между СОРМ ЦКП и ПУ 69
3.3. Команды из ПУ в СОРМ ЦКП 70
3.4. Сообщения от оборудования ЦКП к ПУ по каналу 1 74
3.5. Информационные сообщения от ЦКП к ПУ по каналу 2 77

3.6. Дополнительные сообщения от оборудования СОРМ к ПУ по каналу 2 79
3.7. Методика проведения испытаний....79

Глава 4. СОРМ в сетях передачи данных 81

4.1. Требования СОРМ-2....81
4.2. Возможности RADIUS 86
4.3. Возможности DIAMETER....89
4.4. MAC-адреса 94
4.5. Структура сообщений СОРМ-2 98
4.6. Команды СОРМ-2 99

Глава 5. Конвертирование протоколов СОРМ 101

5.1. Проблема преобразования интерфейсов 101
5.2. Конвертеры ТфОП 102
5.3. Платформа XSM 103
5.4. Медиатор СОРМ для сетей NGN 105
5.5. СОРМ в АТС малой емкости....106

Глава 6. СОРМ в сетях следующего поколения.... 108

6.1. Услуги NGN 108
6.2. Проблемы СОРМ 111
6.3. Медиатор СОРМ....113
6.4. Процесс СОРМ в NGN....114
6.5. Архитектура ETSI 116
6.6. Апробация СОРМ в NGN 118

Глава 7. Тестирование протоколов СОРМ 121

7.1. Проблема тестирования функции СОРМ 121
7.2. Сертификационные испытания СОРМ 122
7.3. Протокол-тестер СОРМ типа ТОР-4М 123
7.4. Имитатор ПУ типа ИМС-30 127

7.5. Зарубежные протокол-тестеры систем законного перехвата сообщений 128
7.6. Сравнение протокол-тестеров СОРМ 129

Глава 8. Сетевая организация ПУ 130

8.1. Требования к ПУ СОРМ 130
8.2. Структура ПУ СОРМ 131
8.3. Алгоритм обслуживания заявок 134
8.4. Распределенная сетевая архитектура СОРМ 135

Глава 9. Реализация оборудования СОРМ 138

9.1. Классификация оборудования СОРМ 138
9.2. Зарубежные варианты реализации 140
9.3. Система A8619 142
9.4. Российские платформы СОРМ 142

Глава 10. Quo Vadis? 144

Список сокращений 148

Литература 156

Предисловие

«Не стремись слышать все, ибо услышишь, как твой раб злословит тебя», – сказано у Экклезиаста. Но в сегодняшних условиях угроз терроризма и распространения наркотиков стремление спецслужб контролировать телефонные переговоры с целью предотвратить преступление представляется оправданным.

В нашей стране это стремление возникло практически сразу же после возникновения телефонной связи: первые упомянутые в литературе устройства для подслушивания телефонных переговоров в России были установлены в помещении IV Государственной думы в 1913 году. Сегодня организационные аспекты в этой области зафиксированы в федеральных законах об оперативно-розыскной деятельности и о связи. В редакции закона о связи №126-ФЗ от 07.07.2003 статья 64 об обязанностях Операторов связи и об ограничении прав пользователей услугами связи при проведении оперативно-розыскных мероприятий и следственных действий гласит:

«1. Операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность, информацию о пользователях услугами связи и об оказанных им услугах связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач, в случаях, установленных федеральными законами.

2. Операторы связи обязаны обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, требований к сетям и средствам связи для проведения оперативно-розыскных мероприятий, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий.

3. Приостановление оказания услуг связи юридическим и физическим лицам осуществляется Операторами связи на основании мотивированного решения в письменной форме одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, в соответствии с законодательством Российской Федерации об оперативно-розыскной деятельности. Операторы связи обязаны возобновить оказание услуг связи на основании решения суда или мотивированного решения в письменной форме одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, который принял решение о приостановлении оказания услуг связи.

4. Порядок взаимодействия Операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, устанавливается Правительством Российской Федерации.

5. При проведении уполномоченными государственными органами следственных действий Операторы связи обязаны оказывать этим органам содействие в соответствии с требованиями уголовно-процессуального законодательства.»

Еще раньше, на основании предыдущей редакции закона о связи №15-ФЗ от 16.02.95 (статья 14 которого предписывала Операторам связи, независимо от их ведомственной принадлежности и форм собственности, действующим на территории Российской Федерации, при разработке, создании и эксплуатации сетей связи оказывать содействие и предоставлять возможность проведения оперативно-розыскных мероприятий в этих сетях органам, осуществляющим оперативно-розыскную деятельность) был издан приказ № 135 Минсвязи России от 11.08.95 «О порядке внедрения системы технических средств по обеспечению оперативно-розыскных мероприятий на электронных АТС на территории Российской Федерации», который интенсифицировал разработку протоколов системы технических средств обеспечения оперативно-розыскных мероприятий (сокращенно СОРМ) и, соответственно, привел к написанию этой книги.

Сама книга несколько выбивается из общего справочного стиля книг серии «Телекоммуникационные протоколы», что обусловлено как относительно короткой историей разработки интерфейсов СОРМ, которая активизировалась только после печально известной даты 11 сентября 2001 года, так и весьма значительными инженерными сложностями реализации законного перехвата сообщений в активно разрабатывающихся сегодня сетях связи следующего поколения NGN (Next Generation Network).

Книга отражает сегодняшнее состояние российских и международных принципов организации и спецификаций протоколов СОРМ, а с теми новшествами в решении этой отнюдь не тривиальной инженерной задачи, которые будут появляться уже после выхода книги в свет, читатель сможет познакомиться в разделе СОРМ сайта http://www.niits.ru.

Еще один адрес в Интернет – http://portal.etsi.org/li/Summary.asp – принадлежит ETSI и тоже может оказаться полезным читателю.

Неоценимую помощь в написании книги авторам оказали стимулирующие дискуссии с А.А. Васильевым, А.М. Кузнецовым и В.И. Полянцевым, оригинальные разработки конвертеров СОРМ и протокол-тестеров ТОР-4М в научно-техническом центре ПРОТЕЙ, системные исследования, выполненные А.А. Зарубиным и В.С. Елагиным на кафедре систем коммутации СПбГУТ им. проф. М.А. Бонч-Бруевича, совместные сертификационные испытания СОРМ с коллегами из российской компании Малвин-сервис, из зарубежных компаний Сименс, Алкатель, Стром, Авайя, Лусент, Италтел, Эрикссон, Искрател, Нортел и др.

Глава 1. Законный перехват сообщений

Не бойтесь их: ибо нет ничего сокровенного, что не открылось бы, и тайного, что не было бы узнано.

От Матфея, глава 10, стих 24

1.1. Поддержка функции СОРМ в АТС

Относительная важность тех или иных функциональных возможностей АТС меняется во времени. Передача факсов, конференц-связь, dial-up доступ в Интернет из экзотических дополнительных услуг телефонных сетей общего пользования превратились со временем в неотъемлемые функции современных систем коммутации. Перечисленные в предисловии и не зависящие от связистов обстоятельства заставили причислить к таким же обязательным функциям АТС поддержку законного перехвата сообщений или, по-русски, с*истемы оперативно-розыскных мероприятий* (СОРМ).

Под СОРМ в телефонных сетях общего пользования (ТфОП) понимается *юридически санкционированный доступ правоохранительных организаций к частным телефонным переговорам*. Этим уполномоченным организациям, именуемым в международных стандартах *LEA (Law Enforcement Agency),* принадлежат так называемые *пункты управления ПУ* (в российской терминологии) или, согласно международной (европейской) терминологии, – *LEMF (Law Enforcement Monitoring Facility), – средства мониторинга, принадлежащие правоохранительному органу,* обсуждение которых выходят за рамки настоящей книги. Основное внимание

в ней уделено техническим требованиям, которые предъявляет СОРМ к узлам коммутации. Эти требования сводятся к необходимости организовать канал для *прослушивания* в ПУ контролируемого разговорного тракта, канал передачи специальных *команд управления* от ПУ к станции и *ответных сообщений* от станции, а также канал передачи *сообщений* о фазах контролируемых соединений от станции к ПУ. По этим каналам передачи данных оператор ПУ имеет возможность взаимодействовать с программным обеспечением АТС с помощью команд, а станция – транслировать к ПУ разные сообщения, в том числе и аварийные сообщения о тех событиях, которые могут влиять на работу СОРМ. Реализация этих требований является непростой инженерной задачей и для АТС сети коммутации каналов, а для гибких коммутаторов Softswitch сетей NGN (чему посвящена глава 4) становится еще сложнее и интереснее. Но сначала – о сути проблемы.

1.2. Понятие законного перехвата сообщений

Функция СОРМ в терминах стандартов Европейского института стандартизации в телекоммуникациях ETSI (European Telecommunications Standards Institute) называется *законным перехватом сообщений LI (Lawful Interception),* который весьма точно отражает суть дела. В качестве синонимов LI иногда используются термины *phone tapping* или *wiretapping*.

Имеются некоторые различия между российским СОРМ и стандартизованным ETSI законным перехватом сообщений, заключающиеся в организации взаимодействия LEA с Оператором связи. Согласно европейским стандартам LEA сообщает Оператору номера телефонов, назначенные для мониторинга, перекладывая на него управление процедурой СОРМ, а в российской версии управление процедурой СОРМ и информация о назначенных для мониторинга номерах телефонов сосредоточены исключительно в ПУ и на станции. Организация каналов для трансляции перехваченной информации также различна: коммутируемый канал в модели ETSI и полупостоянное соединение в российском СОРМ. С учетом этих нюансов законный перехват сообщений LI используется в книге как синоним СОРМ.

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 переговорам или к сообщениям электронной почты какого-либо лица или организации. Это определение охватывает системы СОРМ в разных странах, внедряющих соответствующее оборудование, разрабатывающих регламентирующие его использование законодательные акты и необходимые инженерные решения, создающих международные рабочие группы стандартизации спецификаций законного перехвата. 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 и выдвигает на первый план международные стандарты ETSI.

Базовый стандарт TS 101 331 «Requirements of Law Enforcement Agencies» определяет основные требования и кооперацию сетевых Операторов и сервис-провайдеров при законном перехвате сообщений. В других документах ETSI, помимо охвата услуг традиционной и сотовой телефонии, предполагается реализация процедур LI для услуг Интернет, таких как Web-серфинг, e-mail, чат, ICQ, IP-телефония, ftp, telnet и др. В рамках этой же концепции силами ETSI и 3GPP исследуется реализация СОРМ в NGN и 3G, а также другие вопросы, например, проблемы зашифрованного трафика – безопасной e-mail с PGP и S/MIME, безопасного серфинга с использованием HTTPS (SSL, TLS) и виртуальных частных сетей VPN (IPSec), зашифрованной IP-телефонии (pgp–phone, Nautilus), для решения которых рассматриваются два пути – дешифрование информации перед ее передачей к средствам мониторинга, принадлежащим правоохранительным органам, или доступность этим органам ключей шифрования.

Но прежде рассмотрим несколько подробнее базовые международные стандарты СОРМ.

1.3. Европейские стандарты

Общеевропейские стандарты законного перехвата сообщений стремятся унифицировать национальные документы СОРМ и, в конечном итоге, призваны их заменить.

История работы ETSI над проблематикой законного перехвата сообщений началась в 1991 году с создания группы ETSI/TC *STAG (Security Techniques Advisory Group)*. Затем эта группа была преобразована в ETSI/TC *SEC-WGLI (Security*

Working Group Lawful Interception) в 1997 году и, наконец, с октября 2002 года – в ETSI/TC *TC LI (Lawful Interception)*. Схема законного перехвата сообщений согласно общеевропейской концепции показана на рис. 1.1.

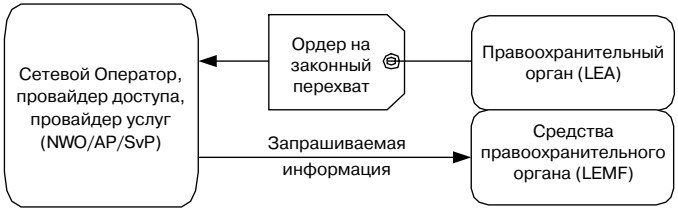


Рис. 1.1. Схема законного перехвата сообщений согласно общеевропейской концепции

Правоохранительный орган *LEA* при намерении организовать законный перехват сообщений подает через уполномоченный орган, например суд, заявку на получение законного ордера, представляемого затем в NWO/AP/SvP через административный интерфейс HI1. Когда ордер на законный перехват получен, средства мониторинга, принадлежащие правоохранительному органу *LEMF,* получают через порты интерфейса HI2 и HI3 информацию о содержимом связи *CC (Content of Communication),* а также связанную с перехватом информацию *IRI (Intercept Related Information)* о телекоммуникационных услугах, о соединениях, включая неуспешные попытки вызовов, о местонахождении пользователя и т.п. Ордер может описывать IRI и CC для конкретного случая перехвата, период действия ордера и предмет перехвата, адрес абонента, телекоммуникационные услуги и т.д. Для различных правоохранительных органов и для разных случаев могут применяться разные ограничения, устанавливаемые национальными законодательствами и зависящие от абонентских услуг и от сетей, в которых производится перехват. Общеевропейские же спецификации содержатся в двух основных стандартах ETSI.

Первый из них, стандарт ETSI ES 201 671 / ETSI TS 101 671 «Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic» определяет интерфейс взаимодействия с техническими средствами правоохранительных органов, ведущими мониторинг, и является, в определенной степени, рамочным. Рамочным в том смысле, что он оставляет возможность выбора элементов спецификации интерфейса для того, чтобы соответствовать национальному законодательству, национальным требованиям и правилам конкретного правоохранительного органа. Стандарт закрывает технологии

ТфОП, ISDN, GSM, GPRS, TETRA и оставляет для изучения стационарные сети NGN, включая эмуляцию ТфОП/ISDN в IMS (IP Multimedia Subsystem). Им же определен язык ASN.1 (Abstract Syntax Notation One) по рекомендации ITU-T X. 680 для интерфейса HI2, о чем речь ниже.

В другом стандарте ETSI ES 201 158 «Telecommunications security; Lawful Interception (LI); Requirements for network functions» определяются требования к сетевым функциям и детализируется обобщенная структура реализации законного перехвата сообщения, причем для каждой страны также возможна ее трансформация в соответствии с национальным законодательством. В определяемой этими стандартами концепции ETSI упоминаются участники процесса COPM, приведенные в табл. 1.1 вместе с их ролями.

Таблица 1.1. Участники процесса законного перехвата сообщений по ETSI и их роли

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 (CC и IRI), касающиеся определенного объекта. Несколько LEA могут в одно и тоже 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 HI2 – HI3. Один и тот же LEA может использовать для перехвата информации несколько NWO
Провайдер услуг (SvP)	Провайдер услуг SvP предоставляет пользователям услуги в дополнение к услугам, предоставляемым самой сетью, и отвечает за поддержку организации перехвата сообщений
Провайдер доступа (AP)	Провайдер доступа AP 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 содержать возможность объединения их в общей телекоммуникационной инфраструктуре

Отметим еще несколько связанных с СОРМ документов ETSI. Это ориентированный на законный перехват сообщений в сети ISDN документ TR 102 053 «Notes on ISDN LI functionalities», высокоуровневое описание сетевых принципов организации СОРМ в современных телекоммуникационных сетях в документе TR 101 943 «Concepts of Interception in a Generic Network Architecture» и непосредственно связанный с содержанием глав 4 и 5 книги документ TR 101 944 «Issues on IP Interception».

Проблематике СОРМ в IP-сетях посвящены и более поздние разработки ETSI, в частности, документ TS 102 232 «Delivery of IP based interception», описывающий общие аспекты интерфейсов HI2 и HI3, рассматриваемых ниже в параграфе 1.5 этой главы, для всех сетей, базирующихся на транспорте TCP/IP, а также заголовки, которые должны быть добавлены к IRI и CC, посылаемым через интерфейсы HI2 и HI3 и протоколы для IRI и CC. В эти новые заголовки, как правило, включаются идентификатор законного перехвата, код страны, код соединения, номер сообщения в последовательности сообщений, временная отметка, сведения о типе и направлении полезной нагрузки, о типе законного перехвата и о типах сообщений IRI (Begin, Continue, End, Report), тоже рассматриваемых в параграфе 1.5.

На IP-сети ориентированы также документ TS 102 233 «Service specific details for E-Mail Services», касающийся электронной почты и описывающий интерфейсы законного перехвата e-mail с участием протоколов SMTP и POP3, и документ TS 102 234 «Service specific details for Internet Access Services», посвященный вопросам СОРМ при доступе в Интернет, законному перехвату информации TCP/IP, протоколам DHCP и RADIUS, к обсуждению чего мы будем возвращаться в главах 3 и 4 данной книги. Кроме того, есть также стандарты LI, разработанные объединением 3GPP: TS 133 106 «Lawful interception requirements», TS 133 107 «Lawful interception architecture and functions» и TS 133 108 «Handover interface for Lawful Interception». Но прежде рассмотрим базовые механизмы.

1.4. Механизм организации СОРМ в концепции ETSI

Рассмотрим алгоритм организации законного перехвата сообщений в рамках концепции ETSI, несколько отличающийся, как уже упоминалось выше, от российского СОРМ. Базируясь на приведенном в табл. 1.1 перечне, рассмотрим действия участников процесса законного перехвата в следующем 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 CC контролируемого объекта.

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

Шаг 8. По запросу LEA, или когда истечет период действия ордера на законный 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 для передачи CC;
- 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.

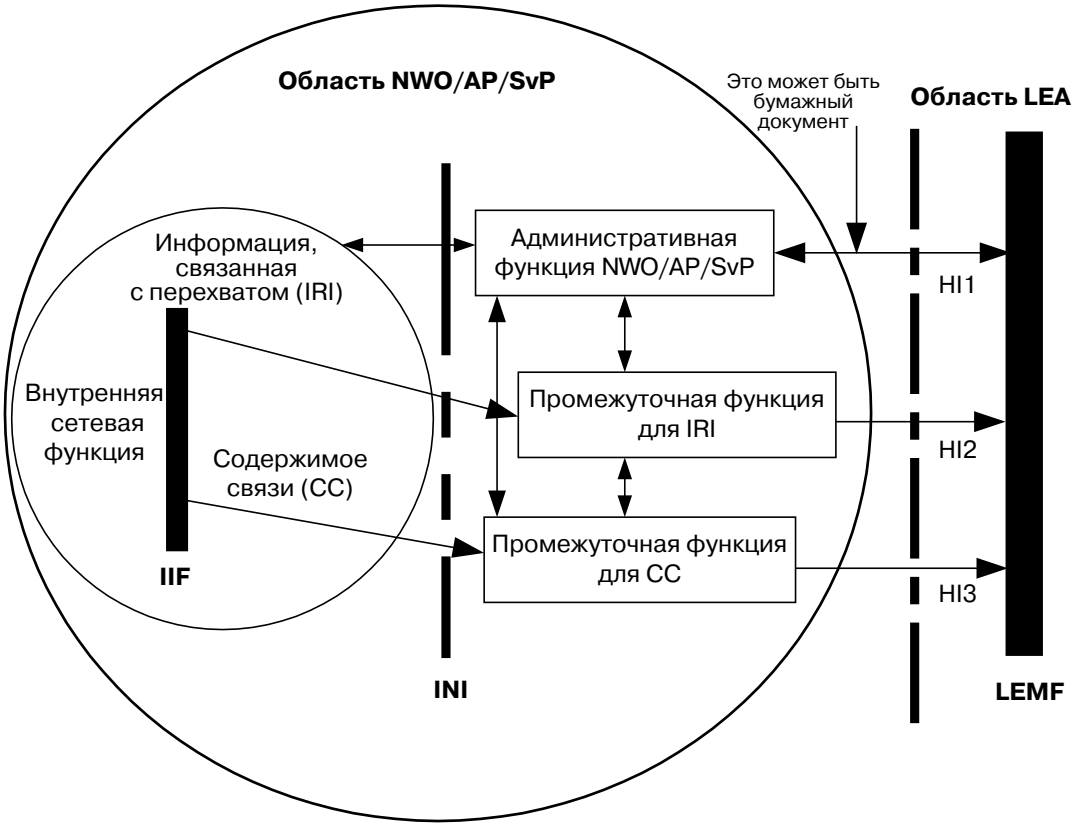
Синтаксис необходимых команд может различаться в национальных применениях. В отечественных системах СОРМ, например, он определяется выбранным протоколом X. 25 и подробно рассматривается в следующей главе.

В условиях современной телекоммуникационной сети объект наблюдения может подписаться на услуги, предлагаемые несколькими провайдерами SvP, и имеет возможность выбрать один или более доступов AP (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 AP и NWO, для реализации законного перехвата необходима организация их взаимодействия. Для выполнения процедуры перехвата необходимо предоставление всей необходимой (но не более того) эксплутационной информации от AP и/или от NWO, касающейся объекта наблюдения и используемых им услуг. В случае совместного предоставления услуг несколькими SvP, любому из них предоставляется сетевая эксплуатационная информация в объеме не большем, чем это необходимо для перехвата. Более того, *глобальная инфокоммуникационная инфраструктура GII (Global Infocommunication Infrastructure)* предусматривает, что в организацию перехвата вовлекаются национальные правоохранительные структуры разных государств, в связи с чем возможны сценарии, где в предоставлении услуги участвуют несколько SvP, расположенных в разных странах.

1.5. Интерфейсы законного перехвата ETSI

Хотя новые сетевые требования к законному перехвату сообщений, возникающие при переходе к NGN, могут привести к пересмотру описываемого ниже интерфейса, сегодня базовый интерфейс законного перехвата ETSI использует три разных порта таким образом, что административная информация, IRI и CC логически разделены между собой. Речь идет о портах HI1, HI2 и HI3 на рис.1.2, ориентированных на обмен информацией этих трех типов. Порт HI1 выполняет рассматриваемые ниже административные функции и работает обычно в режиме обмена бумажными носителями. Каналы и протоколы для HI2 и HI3 выбираются в

зависимости от используемых сетью технологий, например, временных каналов тракта E1 и протокола X. 25 в российских сетях связи.



INI - внутренний сетевой интерфейс
IIF - внутренняя функция перехвата
HI1,2,3 - интерфейсы для законного перехвата сообщений

Рис. 1.2. Функциональная архитектура COPM согласно концепции ETSI

Первый из рассматриваемых интерфейсов – *административный интерфейс HI1* – предназначен для обмена административной информацией между LEA и NWO/AP/SvP (рис.1.2). Спецификации ETSI подразумевают полное разделение административного интерфейса HI1 и технических интерфейсов HI2 и HI3 в самой сети NWO/AP/SvP, чтобы обеспечить требуемую конфиденциальность информации об абонентах, находящихся под контролем. Обычно интерфейс HI1 имеет двунаправленную структуру, что объясняется необходимостью передачи запросов о законном перехвате к NWO/AP/SvP, например, информации об активизации, о прекращении перехвата, об изменении его параметров в одну сторону, а также получения соответствующих уведомлений на стороне LEA. Согласно концепции ETSI любая возможность прямого контроля/управления NWO/AP/SvP оборудованием LEMF/LEA исключается.

Ручной интерфейс HI1 обычно представлен в виде бумажного документооборота, где LEA на основании выданной лицензии отправляет по факсу или письмом запрос предоставления услуг законного перехвата. Такая заявка поступает в административный центр. После обработки заявки в LEA возвращается сообщение об активизации процедуры перехвата, а через интерфейсы HI2 и HI3 в сторону LEA будет поступать информация, относящаяся к перехвату *IRI (Intercept Related Information)* и к содержимому связи *CC (Content of Communication)*. Для активизации законного перехвата LEA предоставляет через HI1 следующую информацию:

- идентификатор объекта перехвата,
- период времени, в течение которого должны выполняться перехваты,
- лицензия на законный перехват,
- тип информации, требуемой в результате перехвата (IRI, CC или оба),
- HI2-адрес LEMF для получения IRI-записей,
- HI3-адрес LEMF для пересылки CC-информации,
- другая необходимая информация (механизм доставки через интерфейсы HI2 и HI3, информация о сети и т. д.).

Сообщения от NWO/AP/SvP к LEMF через *интерфейс HI1* отправляются в следующих случаях: после активизации законного перехвата; после его завершения; после изменения параметров активного процесса перехвата; в случае возникновения непредвиденных ситуаций.

Второй интерфейс – *HI2 – интерфейс передачи информации, относящейся к перехватываемому вызову,* предназначен для транспортировки информации *IRI (Intercept Related Information)* от NWO/AP/SvP к LEMF/LEA с помощью выбранного для существующей сетевой инфраструктуры протокола передачи данных, например, протокола X. 25, сигнализации ISDN, X. 31, стека TCP/IP и т. п. Кодирование данных основывается на стандартных протоколах передачи данных, а на уровне представления семиуровневой модели OSI используются правила шифрования *BER (Basic Encoding Rules).* Параметры сообщений IRI кодируются с использованием *ASN.1.*

IRI-записи передаются индивидуально, хотя возможна и групповая доставка нескольких IRI-записей, предназначенных для одного LEA, если это не вносит недопустимых задержек. Именно из-за временных ограничений IRI-записи, как правило, пересылаются немедленно, без накопления. В российских требованиях указано, что время реакции СОРМ с момента регистрации события на станции до момента записи информации о данном событии в порт передачи не должно превышать 200 мс.

Упоминавшийся в параграфе 1.3 стандарт ETSI ES 201 671/ETSI TS 101 671 определяет 4 сообщения для интерфейса HI2. Одно сообщение – *IRI-Report* – для любых не связанных с соединением событий и три сообщения – *IRI-Begin, IRI-Continue, IRI-End* – для ассоциированной с соединением информации:

- IRI-BEGIN – сообщение, открывающее IRI-транзакцию;
- IRI-END – сообщение, закрывающее сеанс передачи сообщений IRI;
- IRI-CONTINUE – сообщение, которое передается в любой момент сеанса передачи сообщений IRI, относящихся к определенному соединению (начало, активная фаза, завершение). В процессе сеанса могут передаваться записи IRI-CONTINUE, содержащие данные о вызове, и CC-информация;
- IRI-REPORT предназначено для передачи информации о действиях абонента, не связанных с соединением, например, при изменении им набора дополнительных услуг.

Параметрами этих сообщений являются связанные с законным перехватом идентификаторы (идентификатор законного перехвата, сеть, сетевой Оператор и др.), временные отметки, направление вызова (к/от находящегося под контролем абонента), состояние соединения (в процессе установления, установлено), теле-

фонные номера/адреса вызывающего и вызываемого абонентов (E164, TEI, IMSI, IMEI, MSISDN, SIP URI и др.), длительность посылки вызова/продолжительность соединения, используемые дополнительные услуги и т. п.

Третий *интерфейс HI3 – интерфейс передачи содержимого связи* – предназначен для транспортировки от NWO/AP/SvP к LEMF/LEA непосредственно содержимого *CC (Content of Communication),* т. е. самого телефонного разговора, содержания факса или другого передаваемого контента.

В ТфОП содержимое телефонных переговоров передается к LEMF, как правило, по каналам 64 Кбит/с. Существуют два варианта, зависящие от сетевой инфраструктуры: стандартные коммутируемые по инициативе LEMF соединения для каждого контролируемого соединения и выделенная сеть передачи LI. Заметим, что HI2 и HI3 – логически различные интерфейсы, хотя и предусматривается возможность синхронизации сообщений потоков данных HI2 и HI3 с помощью общего (со ссылкой) поля данных, вложенного в IRI и CC. Возможность эта ориентируется на сети с коммутацией пакетов и не используется в сетях с коммутацией каналов. Принципы законного перехвата сообщений в пакетных сетях заложены в стандарте ETSI TS 102 232 «Delivery of IP based interception», описывающем общие аспекты интерфейсов HI2 и HI3, как они определены TS 101 671, но уже для IP-сетей. Модель данных законного перехвата по TS 102 232 представлена на рис.1.3.

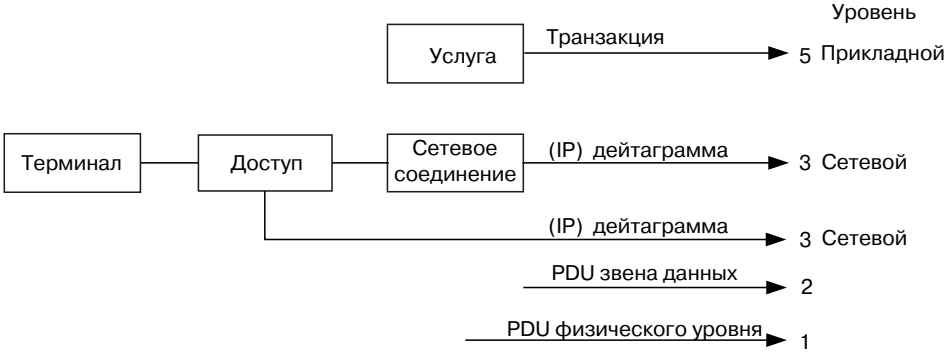


Рис. 1.3. Модель данных законного перехвата по ETSI TS 102 232

Здесь СОРМ на прикладном уровне предполагает передачу транзакций от сервис-провайдера, а на сетевом уровне предполагает законный перехват IP-дейтаграмм от сетевого Оператора или Интернет-провайдера доступа. К этим же вопросам для российского СОРМ в IP-сетях, неформально называемого СОРМ-2, мы вернемся в главе 3.

1.6. CALEA и другие стандарты СОРМ

Североамериканская концепция законного перехвата сообщений известна под официальным названием *CALEA (Communications Assistance for Law Enforcement Act).* Иногда в литературе использовались также американские термины *phone tapping* и *wiretapping*. История американских разработок законного перехвата сообщений начинается с 1995 г. В Joint Standards Development ATIS, в WTSC (бывшая T1P1) и в PTSC (бывшая T1S1) были созданы стандарты J-STD-025, J-STD-025-A, а к настоящему времени – уже J-STD-025-B.

CALEA поддерживает подходы, аналогичные рассмотренным в предыдущем параграфе европейским LI, хотя придирчивое их сравнение позволяет увидеть, что при общей схожести моделей имеются различия, в первую очередь, в части стандартизации СОРМ для мобильных сетей и GPRS. Имеются различия и в определениях ряда субъектов и объектов законного перехвата сообщений, в связи с чем мы приведем здесь таблицу соответствия 1.2.

Таблица 1.2. Соответствие понятий ETSI и CALEA

ETSI		CALEA	
LI	Lawful Intercept	LAES	Lawful Authorized Electronic Surveillance
LEMF	Law Enforcement Monitoring Facility	CF	Collection Function
NWO/AP/SvP	Network Operator/Access Provider/Service Provider	TSP	Telecommunication Service Provider
	Handover Interface port 2	CDC	Call Data Channel
	Handover Interface port 3	CCC	Call Content Channel
IRI	Intercept Related Information		Call-identifying Information
	IRI record		Call-identifying message
HI 1	HI1 interface		Lawful Authorization
HI 2, 3	Handover Interface (HI2, HI3)		e-interface
	Delivery Function/Mediation Function	DF	Delivery Function

В настоящее время в TR-45 создан новый подкомитет в составе рабочей группы CALEA – CWG (TIA CALEA Working Group), роль которого соответствует так называемому стандарту *Safe Harbor*. Не тратя время на детальный анализ CALEA и других национальных апробированных стандартов, приведем таблицу 1.3, в которой перечислены посвященные СОРМ международные стандарты. Основную их часть составляют документы ETSI. Напомним читателям смысл обозначений этих документов:

- ETSI EG - ETSI Guide
- ETSI EN - European Standard - Telecommunications series
- ETSI ES - ETSI Standard
- ETSI SR - ETSI Special Report
- ETSI TR - ETSI Technical Report
- ETSI TS - ETSI Technical Specification

В контексте этой книги нас больше интересуют технические спецификации TS, но для удобства поиска в табл. 1.3 зарубежные стандарты расположены по алфавиту. Инженерным аспектам российской организации СОРМ посвящен следующий параграф.

Таблица 1.3. Международные стандарты СОРМ

Организация	Номер	Версия, год	Название
ETSI	EG 201 040	Version 1.1.1 (1998-04)	Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface; Feasibility study report
ETSI	EG 201 781	Version 1.1.1 (2000-07)	Intelligent Networks (IN); Lawful Interception
ETSI	EN 301 040	Version 2.0.0 (1999-06)	Terrestial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface
ETSI	ES 101 909-20.1 ES 101 909-20.2	Version0.0.11 (2002-11)	Cable IP Handover for Voice and Multimedia Cable IP Handover for data
ETSI	ES 201 158	Version 1.2.1 (2002-04	Telecommunications Security; Lawful Interception (LI); Requirements for Network Functions
ETSI	ES 201 671	Version 2.1.1 (2001-09)	Telecommunications Security; Lawful Interception (LI); Handover Interface for the Lawful Interception of Telecommunications Traffic (revised version)

Продолжение табл. 1.3

Организация	Номер	Версия, год	Название
ETSI	ETR 331	(1996-12)	Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception of telecommunications; Requirements of the law enforcement agencies
ETSI	ETR 363	(1997-01)	Digital cellular telecommunications system; Lawful Interception requirements for GSM (GSM 10.20 version 5.0.1
ETSI	TR 101 514	Version 8.0.0 (2001-05)	Digital Cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM (GSM 01.33 version 7.0.0 Release 1998)
ETSI	TR 101 750	Version 1.1.1 (1999-11	Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Security; Studies into the Impact of lawful interception
ETSI	TR 101 772	Version 1.1.2 (2001-12)	Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; Service independent requirements definition; Lawful interception - top level requirements
ETSI	TR 101 876	Version1.1.1 (2001-01)	Telecommunications security; Lawful Interception (LI); Description of GPRS HI3
ETSI	TR 101 943	Version 1.1.1 (2001-07)	Telecommunications Security; Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture.
ETSI	TR 101 944	Version 1.1.2 (2001-12)	Telecommunications Security; Lawful Interception (LI); Issues on IP Interception
ETSI	TR 102 053	Version 1.1.2 (2001-12)	Telecommunications security; Lawful Interception (LI); Notes on ISDN lawful interception functionality
ETSI	TR 141 033	Version 5.0.0 (2002-06)	Digital cellular telecommunications system (Phase 2+); Lawful Interception requirements for GSM (3GPP TR 41.033 version 5.0.0 Release 5)
ETSI	TS 101 040	Version1.1.1 (1997-05)	Terrestrial Trunked Radio (TETRA); Security; Lawful Interception (LI) interface
ETSI	TS 101 331	Version 1.1.1 (2001-08)	Telecommunications security; Lawful Interception (LI); Requirements of Law Enforcement Agencies
ETSI	TS 101 507	Version 8.0.1 (2001-06)	Digital cellular telecommunications system (Phase 2+); Lawful Interception – Stage 1 (GSM 02.33 version 7.3.0 Release 1998)
ETSI	TS 101 509	Version 8.1.0 (2000-12)	Digital cellular telecommunications system (Phase 2+); Lawful interception; Stage (GSM 03.33 version 8.1.0 Release 1999)
ETSI	TS 101 671	Version 2.10.1 (2004-09)	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic
ETSI	TS 101 861	Version 1.2.1 (2002-03)	Time Stamping Profile

Окончание табл. 1.3

Организация	Номер	Версия, год	Название
ETSI	TS 102 232	Version 1.2.1 (2004-02)	Telecommunications security; Lawful interception; Handover specification for IP delivery
ETSI	TS 102 233	Version 1.2.1 (2004-05)	Telecommunications security; Lawful interception; Service specific details for E-mail delivery
	TS 102 234	Version 1.2.1 (2004-10)	Telecommunications security; Lawful interception; Service specific details for Internet Access Services
ETSI	TS 133 106	Version 6.1.0 (2005-01)	Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful interception Requirements
ETSI	TS 133 107	Version 5.6.0 (2003-09)	Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful interception Architecture and Functions
ETSI	TS 133 108	Version 5.5.0 (2003-09)	Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI)
ETSI	DTS/TIPHON-03020	Version 1.0.1 (2002-11)	TIPHON TM Release 4; Functional Entities, Information Flow and Reference Point Definitions; Lawful Interception
IETF	draft-baker-slem-architecture-02.txt	2003 – 10	Cisco Architecture for Lawful Intercept In IP Networks
IETF	draft-baker-slem-mib-00	2003 – 10	Cisco Lawful Intercept Control MIB
США: ATIS	T1.678	Version 2 (2006 – 01)	Lawfully Authorized Electronic Surveillance(LAES) for Voice over Packet Technologies in Wireline Telecommunications Networks
США: ATIS	T1.724	2004 – 01	Handover Interface for Lawful Interception of Packet-Data Services, Circuit Switched Services, and Multimedia Services within the Universal Mobile Telecommunications System (UMTS), адаптирован по ETSI TS 133.108 V/5
США: TIA	J-STD-025-A	2003 – 02	Lawfully Authorized Electronic Surveillance
США: TIA	J-STD-025-B	2003 – 11	Lawfully Authorized Electronic Surveillance, T1P1/T1S1 joint standard
США: PCIA	Standard 1	Version1.3 (2000 – 05)	CALEA Specification for Traditional Paging
США: PCIA	Standard 2	Version1.3 (2000 – 05)	CALEA Specification for Advanced Messaging
США: PCIA	Standard 3	Version1.3 (2000 – 05)	CALEA Specification for Ancillary Services
Германия	TR TK (TR F V)	Version 4.0 (2003-04)	Technical Directive setting forth Requirements relating to the Implementation of Legal Measures for the Interception of Telecommunications
Нидерланды	TIIT	Version1.0.0 (2002-09)	Transport of Intercepted IP Traffic
Великобритания	NHIS	Version1.0 (2002-05)	National Handover Interface Specification

Как видно из табл. 1.3, наиболее развитыми являются европейские стандарты законного перехвата сообщений. В их основе лежит принятая в январе 1995 года резолюция Совета ЕС, положенная в основу базового документа ETSI – доклада ETR 331, суммирующего требования LEA. Позже этот доклад был переиздан в качестве технического стандарта TS 101 331, учитывающего также технические требования к законному перехвату сообщений ES 201 158, современные телекоммуникационные технологии, работы созданных для стандартизации сетей 3G проекта 3GPP и 3GPP2, а также посвященный СОРМ стандарт 3GPP TS 33.106 (приведенный в табл. 1.2 под номером TS 133 106), к которому вернемся в главе 5, посвященной СОРМ для сетей связи следующего поколения NGN.

1.7. Канал передачи данных к ПУ в российской СОРМ

В российской архитектуре СОРМ функции мониторинга вызовов сосредоточены в пунктах управления (ПУ), соединяемых с коммутационными узлами и станциями трактами Е1, а также, возможно, модемными каналами, как это показано на рис.1.4.

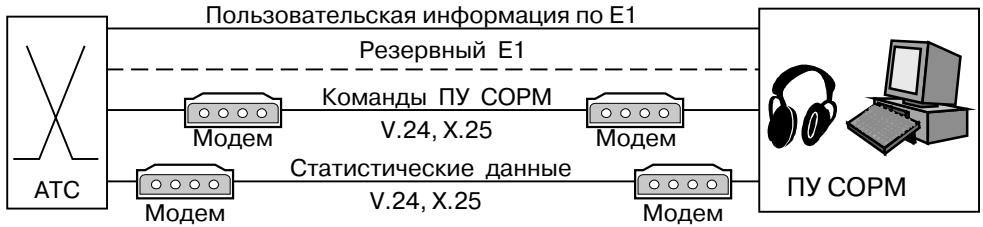


Рис. 1.4. Подключение ПУ СОРМ к АТС через интерфейс X. 25

Требуемое количество каналов и трактов рассчитывается, исходя из нагрузки (емкости узла коммутации). В трактах Е1 канальные интервалы 1 – 15 и 17 – 29 используются для передачи информации контролируемых разговорных каналов узла коммутации. Канальный интервал 16 оборудованием ПУ вообще не обрабатывается, а канальные интервалы 30, 31 нулевого тракта Е1 используются для образования каналов передачи данных между СОРМ узла коммутации и ПУ. Канальный интервал 30 используется для передачи управляющей инфор-

мации – команд и сообщений – и называется *канал 1*, выполняющий некоторые из функций интерфейса HI1 с учетом различий подходов ETSI и российского СОРМ, а также передачу некоторых сообщений, соответствующих интерфейсу HI2. Их схожесть также и в том, что оба они (канал 1 и HI1) двунаправленные. Канальный интервал 31 используется для передачи информации о содержимом связи, называется *канал 2* и является аналогом интерфейса HI2. Если между СОРМ узла и ПУ имеется более одного тракта, то в остальных трактах E1 канальные интервалы 30 и 31 резервируются для случая выхода из строя используемых каналов 30 и 31 или всего нулевого тракта E1.

Протоколами передачи данных между СОРМ узла коммутации и ПУ выбраны сетевой уровень, уровень звена данных и физический уровень протокола X. 25. Выбор этого исторически первого и до сих пор еще применяемого в системах технической эксплуатации ТфОП протокола обусловлен, в частности, и последовательным *(hop-to-hop)* восстановлением при ошибках как на уровне звена данных, так и на сетевом уровне. Это делает X. 25 весьма надежным стеком протоколов при низком качестве линии, хотя, к сожалению, несколько замедляет передачу. В частности, X. 252 может добавлять от 40 до 60 мс ко времени задержки трафика на транзитный участок.

В табл. 1.4 показано, как спецификация X. 25 соответствует трем нижним уровням – физическому, звена данных и сетевому уровням *модели OSI (Open Systems Interconnection)*. Так как спецификация X. 25 предшествовала модели OSI, названия уровней несколько различаются. Физический уровень называется X. 21 и X. 21бис и определяет электрические и физические интерфейсы.

Таблица 1.4. Стек протоколов X. 25

Уровень	Услуга	Примечания
Сетевой (пакетов)	X.25PLP	Протокол пакетного уровня X. 25 – включает в себя механизмы пересылки пакетов
Звена данных	LAPB	Процедура доступа к каналу – включает в себя механизмы устранения ошибок
Физический	X.21	X.21 bis специфицирован для интерфейсов V-серии (обычно RS232). В спецификациях СОРМ в качестве физического уровня указан интерфейс V. 24

Второй уровень представляет собой процедуру управления звеном данных *HDLC (High-level Data Link Control)* и отвечает за надежную передачу данных через физический стык. *Кадр данных* в процедуре HDLC переносит один пакет через интерфейс X.25. Протоколом уровня звена данных является *протокол LAPB (Link Access Protocol – Balanced*). Протокол LAPB применяется в сетях X. 25 для формирования двухточечного соединения между аппаратурой передачи данных DCE и терминальным оборудованием данных DTE и используется для передачи информации уровня 3 протокола X. 25.

Третий уровень – протокол сетевого уровня, называемого в X. 25 уровнем пакетов, предназначен для упаковки данных в пакеты, а также для создания виртуальных каналов, по которым эти пакеты передаются. Этот уровень предоставляет возможность создания соединений с помощью виртуальных каналов, а также приема и передачи данных. Механизм окна, связанный с каждым виртуальным каналом, обеспечивает управление потоком. Средства сброса и рестарта дают возможность выполнять в интерфейсе процедуры восстановления после ошибок.

Соответствующий табл. 1.4 блок данных X. 25 представлен на рис.1.5.

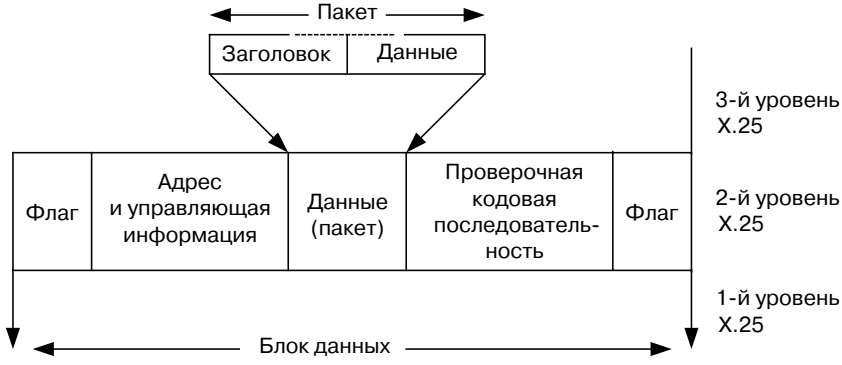


Рис. 1.5. Блок данных X. 25

Начальный флаг (8 битов) и конечный флаг (8 битов) обрамляют пакеты и служат для того, чтобы отделить один пакет от другого. Начальный флаг служит также в качестве битов синхронизации, чтобы СОРМ узла коммутации и ПУ могли синхронизировать скорости передачи. К данным добавлено адресное поле пакета

из 8 битов (4 бита для вызывающей аппаратуры DTE и 4 бита для вызываемой аппаратуры DCE).

Управляющие данные (8-16 битов) содержат порядковый номер пакета, благодаря которому принимающая сторона может идентифицировать пакеты с ошибками, испорченные и потерянные пакеты, а также переставлять пакеты, которые поступили с нарушением очередности. Кроме того, управляющие данные содержат номер виртуальной цепи (4 бита) и виртуального канала (8 битов) по которым перемещаются данные, если тракт предварительно назначен. И, наконец, в блок данных входят средства защиты от ошибок в виде контрольного кода CRC (16 битов).

Поля X.25 уровня 3 образуют пакет X.25, показанный на рис. 1.6. Заголовок X.25 уровня 3 образуют универсальный идентификатор формата GFI (General Format Identifier), представляющий собой 4-битовое поле определения формата пакета, *идентификатор логического канала LCI (Logical Channel Identifier)*, состоящий из номера группы логических каналов и номера логического канала в группе, и *идентификатор типа пакета PTI (Packet Type Identifier)*.

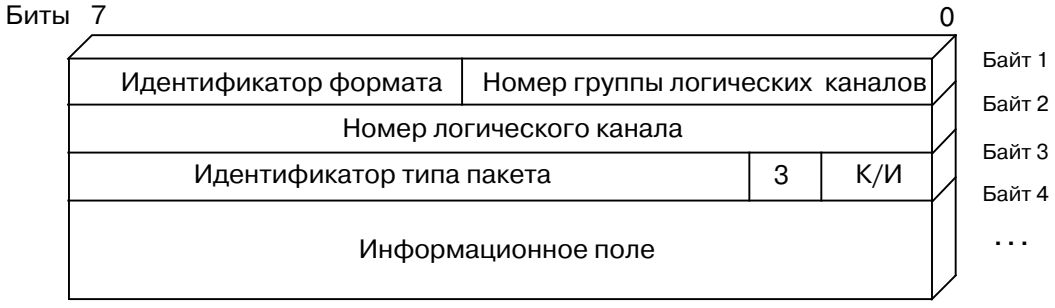


Рис. 1.6. Структура пакета X. 25

Нулевой бит К/И в байте 3 указывает, является ли пакет информационным или управляющим. Остальная часть байта 3 служит для указания типа управляющего пакета. В следующем байте две группы по 4 бита служат для указания длины адресного поля, соответственно, вызывающего и вызываемого DTE. Затем следуют сами эти поля. В ряде случаев в конце пакета могут быть добавлены данные пользователя (до 16 байтов).

Глава 2. СОРМ в телефонной сети общего пользования

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

2.1. Функции поддержки СОРМ для ТфОП

Приведенный эпиграф подчеркивает разумные технические ограничения реализации СОРМ в телефонной сети общего пользования (ТфОП), которые на качественном уровне, как в эпиграфе, совершенно очевидны. Количественные же значения этих ограничений выражены табл. 2.1 и 2.2, приведенными ниже в этой главе. Строго говоря, расчеты значений в этих таблицах и табл. 3.1 следующей главы требуют более тонких математических моделей и оценок вероятностно-временных характеристик, обсуждение которых выходит за рамки этой книги. Но прежде отметим, что требования СОРМ распространяются на все коммутационные узлы и станции стационарной телефонной сети, кроме оконечных станций, максимальная абонентская емкость которых не превышает 256 номеров. За этим единственным исключением поддержка СОРМ обязательна для всех оконечных (ОУС), транзитных (ТУС) и оконечно-транзитных (ОТУ) узлов связи.