Методы инспекции пакетов и анализа трафика

Лекция 4
COPM и DPI

Фицов Вадим Владленович

ст.преп. кафедры ИКС

Содержание лекции:

- **Lawful Intercept (Inspection)**

- COPM
- COPM 1
- COPM 2

- COPM и DPI

- COPM 3?

Lawful Intercept

По известным причинам в телекоммуникационных сетях США, Европы, РФ и других государств давно существует практика законного перехвата телефонных разговоров и сообщений LI (Lawful Interception).

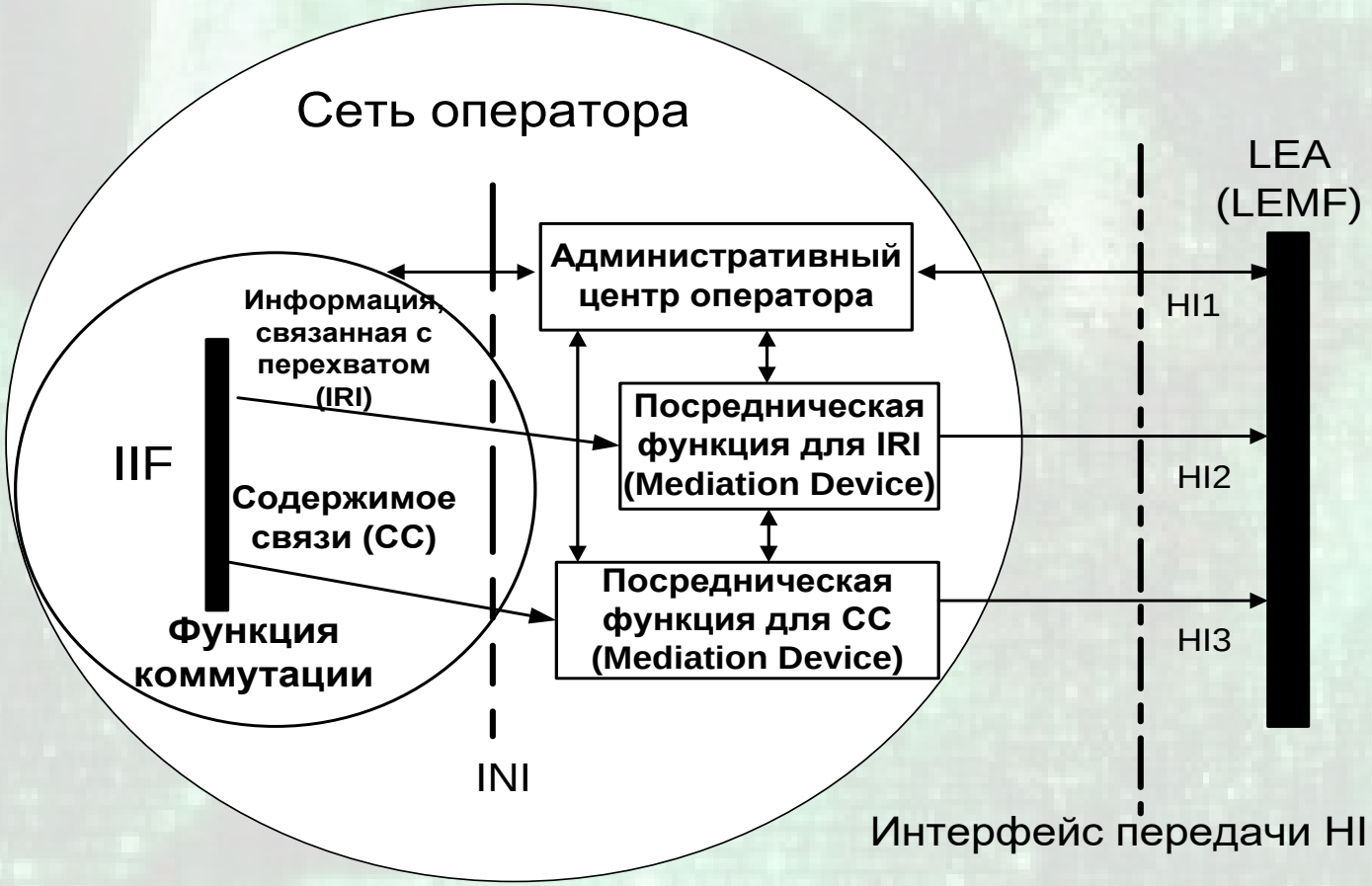
Такие процедуры определены в стандартах европейской ETSI (European Telecommunications Standards Institute) и североамериканской CALEA (Communications Assistance for Law Enforcement Act).

В России оборудование законного перехвата известно под названием СОРМ (средства оперативно розыскных мероприятий).

Концепция ETSI

TS 101 331 «Requirements of Law Enforcement Agencies»

- IIF: Функция внутреннего перехвата
- INI: Внутренний интерфейс сети



- HI1: Административная информация
- HI2: Информация, связанная с перехватом
- HI3: Содержимое соединения

Интерфейс HI 1

Ручной интерфейс HI 1

обычно представлен в виде **бумажного** документооборота,

где LEA на основании выданной лицензии

отправляет по **факсу или письмом**

запрос на предоставление услуг законного перехвата.

6

Интерфейс HI 2

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.

Интерфейс HI 3

Интерфейс HI3 –

интерфейс передачи содержимого связи –

для транспортировки непосредственно содержимого

CC (Content of Communication),

т.е. самого телефонного разговора,

содержания факса

или другого передаваемого контента,

от NWO/AP/SvP к LEMF/LEA.

Концепция CALEA

CALEA (Communications Assistance for Law Enforcement Act)

Интерфейс взаимодействия ПУ СОРМ и Оператора услуг

10

Сравнение понятий ETSI и CALEA

ETSI	
LI	**Lawful Intercept**
LEMF	**Law Enforcement Monitoring Facility**
NWO/AP/ SvP	**Network Operator/Access Provider/ Service Provider**
	Handover Interface port 2
	Handover Interface port 3
IRI	**Intercept Related Information**
	IRI record
	HI1 interface
HI	**Handover Interface (HI2, HI3)**
	Delivery Function/Mediation Function

11

Сравнение понятий ETSI и CALEA

CALEA	
LAES	**Lawful Authorized Electronic Surveillance**
CF	**Collection Function**
TSP	**Telecommunication Service Provider**
CDC	**Call Data Channel**
CCC	**Call Content Channel**
	Call-identifying Information
	Call-identifying message
	b-interface
	e-interface
DF	**Delivery Function**

Сравнение 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
	HI1 interface		b-interface
HI	Handover Interface (HI2, HI3)		e-interface
	Delivery Function/Mediation Function	DF	Delivery Function

13

Орг.	Номер	Версия, год	Название
ETSI	EG 201 040	Version 1.1.1 (**1998+04**)	TETRA; Security; Lawful Interception (LI) interface;
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**)	TETRA; Security; Lawful Interception (LI) interface
ETSI	ES 101 909+20.1/2	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
ETSI	ETR 331	(**1996+12**)	Security Techniques Advisory Group (STAG); Definition of user requirements for lawful interception
ETSI	ETR 363	(**1997+01**)	Digital cellular telecommunications system; Lawful Interception requirements for **GSM**
ETSI	TR 101 514	Version 8.0.0 (**2001+05**)	Digital Cellular telecommunications system; Lawful Interception requirements for **GSM**

Орг.	Номер	Версия, год	Название
ETSI	TR 101 750	Version 1.1.1 (**1999+11**)	TIPHON; Security; Studies into the Impact of lawful interception
ETSI	TR 101 772	Version 1.1.2 (**2001+12**)	TIPHON; Service independent requirements definition; Lawful interception + top level
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; 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. Lawful Interception requirements for **GSM** (3GPP TR 41.033
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

Орг.	Номер	Версия, год	Название
ETSI	TS 101 507	Version 8.0.1 (**2001+06**)	Digital cellular telecommunications system; Lawful Interception
ETSI	TS 101 509	Version 8.1.0 (**2000+12**)	Digital cellular telecommunications system; Lawful interception;
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
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**
ETSI	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**)	**UMTS**; **3G** Security; Lawful interception Requirements
ETSI	TS 133 107	Version 5.6.0 (**2003+09**)	**UMTS**; **3G** Security; Lawful interception Architecture and Functions

Орг.	Номер	Версия, год	Название
ETSI	TS 133 108	Version 5.5.0 (2003+09)	**UMTS; 3G security; Handover** interface for Lawful Interception (LI)
ETSI	DTS/TIPHON+03020	Version 1.0.1 (2002+11)	TIPHON TM ; Functional Entities, Information Flow and Reference Point Definitions; LI;
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
ATIS США	T1.678	Version 2 (2006 – 01)	Lawfully Authorized Electronic Surveillance(LAES) for **Voice over Packet** Technologies in Wireline Telecom Networks
ATIS	T1.724	2004 – 01	**Handover** Interface for Lawful Interception of Packet+Data Services, Circuit Switched Services, and Multimedia Services within the **UMTS**, адаптирован по ETSI TS 133.108 V/5
TIA США	J+STD+025+A	2003 – 02	Lawfully Authorized Electronic Surveillance
TIA	J+STD+025+B	2003 – 11	Lawfully Authorized Electronic Surveillance, T1P1/T1S1 joint standard

Орг.	Номер	Версия, год	Название
PCIA США	Standard 2	Version1.3 (2000 – 05)	CALEA Specification for Advanced Messaging
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

18

COPM

19

СОРМ

Первые в Росии упомянутые в литературе Устройства **подслушивания** телефонных переговоров были установлены

в помещении IV Государственной думы в **1913** году.

СПб: Таврический дворец

20

Старый ФЗ №15 (О связи) от 16.02.95 ст.14:
Операторы обязаны содействовать органам и предоставлять возможность СОРМ

Приказ № 135 Минсвязи России от 11.08.95
«О порядке **внедрения** системы технических средств по обеспечению **СОРМ на электронных АТС** на территории Российской Федерации»

21

ФЗ 126 (07.07.2003) ст.64:

о ограничении прав пользователей при СОРМ:

1. Операторы обязаны **предоставлять органам**, информацию о пользователях и услугах связи, и пр.

2. Операторы обязаны **обеспечивать реализацию** по согласованию с органами, требований к сетям связи для СОРМ, **недопускать раскрытия** организационных и тактических приемов проведения СОРМ.

3. **Приостановление оказания услуг** на основе письма руководителя органа СОРМ

4. Порядок взаимодействия устанавливается Правительством РФ.

5. Операторы обязаны оказывать содействие органам.

Знаковые документы Минкомсвязи

ПРИКАЗ	ГОД	СЕТИ
№226	1992	Предоставить помещения, каналы, данные.
№ 70 /№ 71	1999	ТФОП/СПС
№6	2008	Все сети (кроме телеграфа и телекса)
№ 174	2011	СПС
№ 268	2012	ТФОП
№ 83	2014	СПД

Организация мероприятий СОРМ

Требования к СОРМ:

- Охват всей взаимоувязанной сети связи (ВСС)
- Скрытие факта активизации мероприятий СОРМ
- Надежность доставки перехваченной информации

24

Контроль за абонентом в рамках СОРМ

Контроль за пользователем

статистический контроль

- **Данные о вызове (идентификаторы абонента и терминала, время, категория абонента, адрес, ФИО);**
- **Данные по зарегистрированному терминалу**

полный контроль

- **Данные статистического контроля**
- **Запись переговоров**
- **Перехват пользовательской информации**

статистический контроль

- **Данные о вызове**

- идентификаторы абонента
- идентификаторы терминала
- время
- категория абонента
- адрес
- ФИО

- **Данные по зарегистрированному терминалу**

- категория абонента
- адрес
- ФИО
…

26

полный контроль

- Данные статистического контроля
- Запись переговоров
- Перехват пользовательской информации

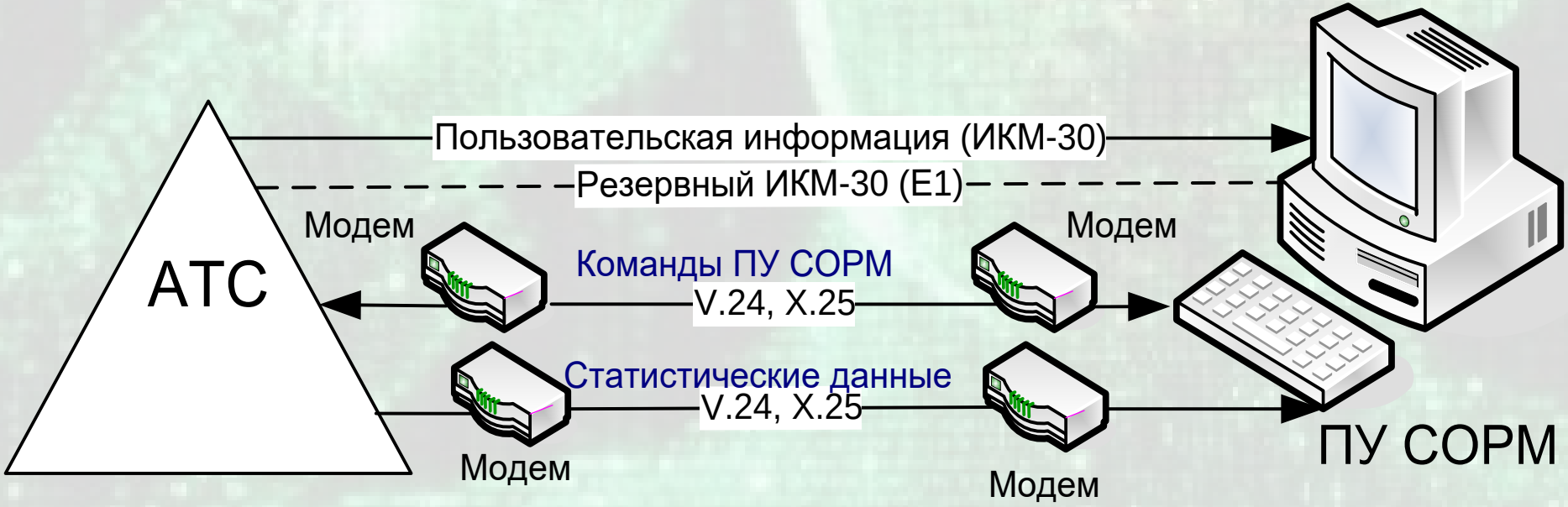
COPM 1

Российский СОРМ

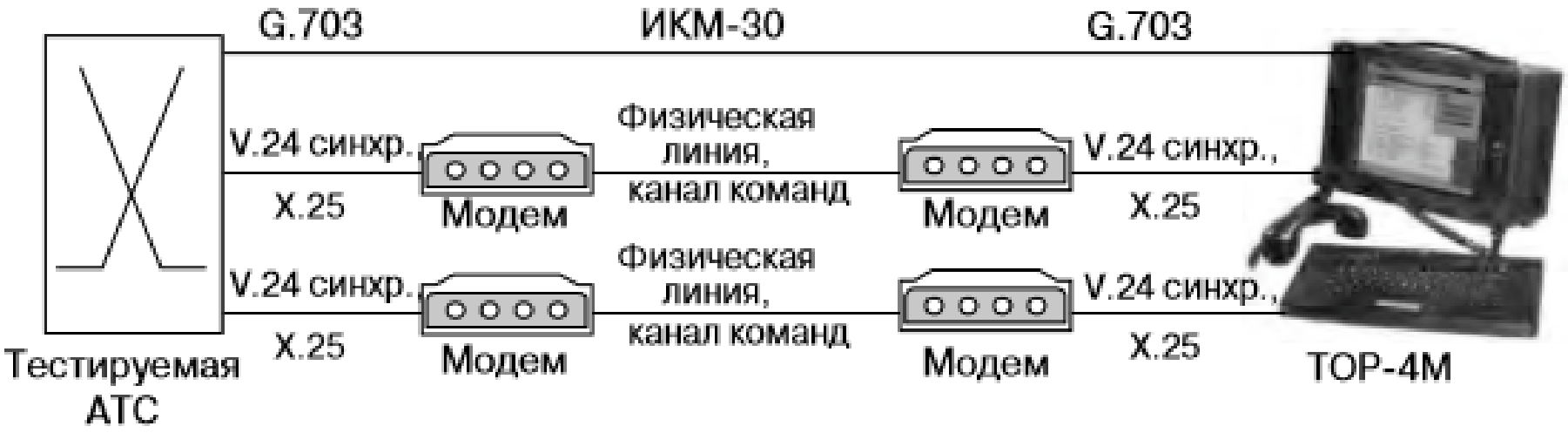
Емкость ОУС	Количество контролируемых абонентов сети	Количество контролируемых абонентов ОУС	Одновременный контроль соединений, не более	Количество каналов, не более	Количество трактов Е1, не более
257 – 2000	0	8	4	8	1
2000	0	15	6	12	1
6000	0	30	8	16	1
10000	1024	128	28	56	2
20000	1024	256	56	112	4
40000	1024	512	56	112	4
60000 и более	1024	1024	56	112	4

29

Российский СОРМ

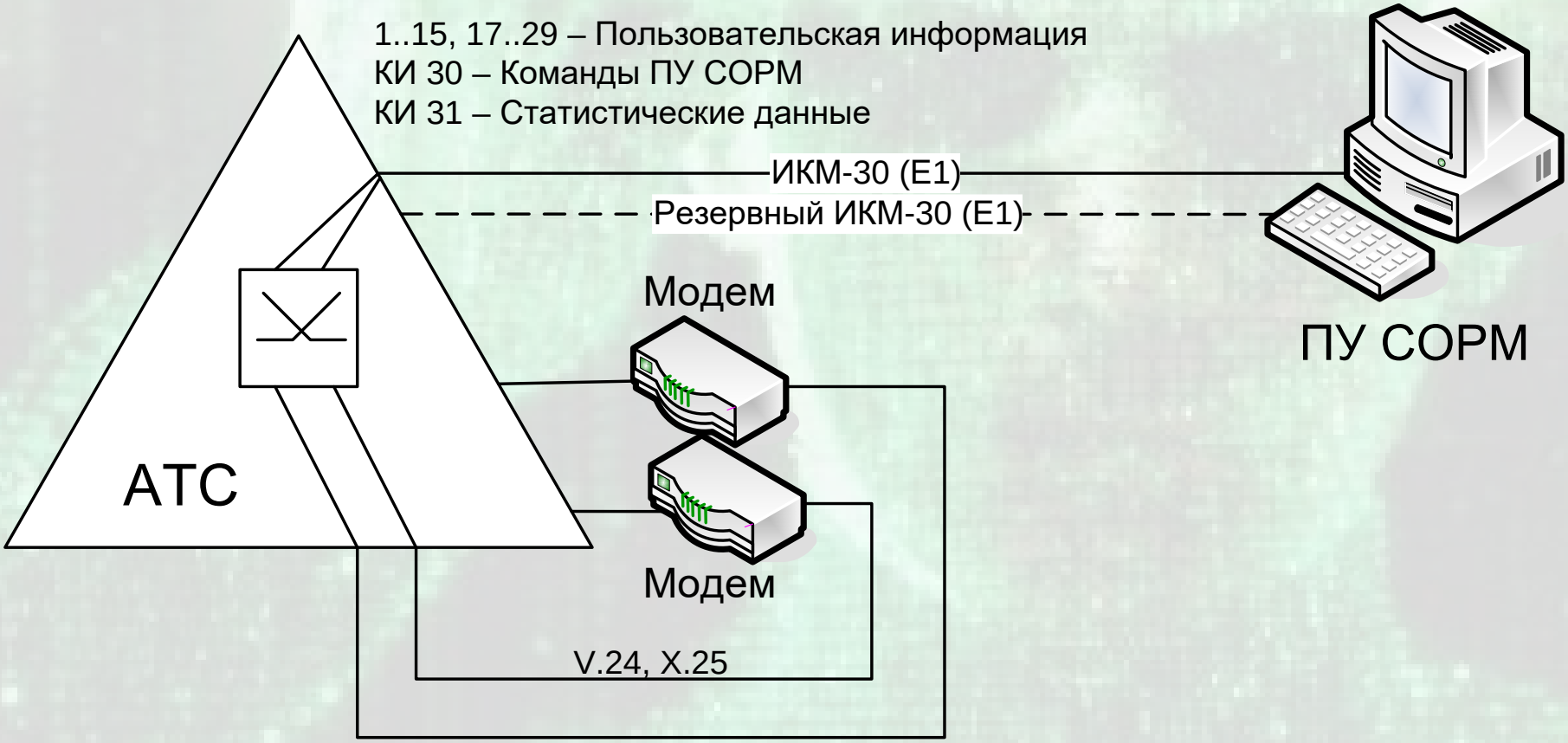


Российский СОРМ



31

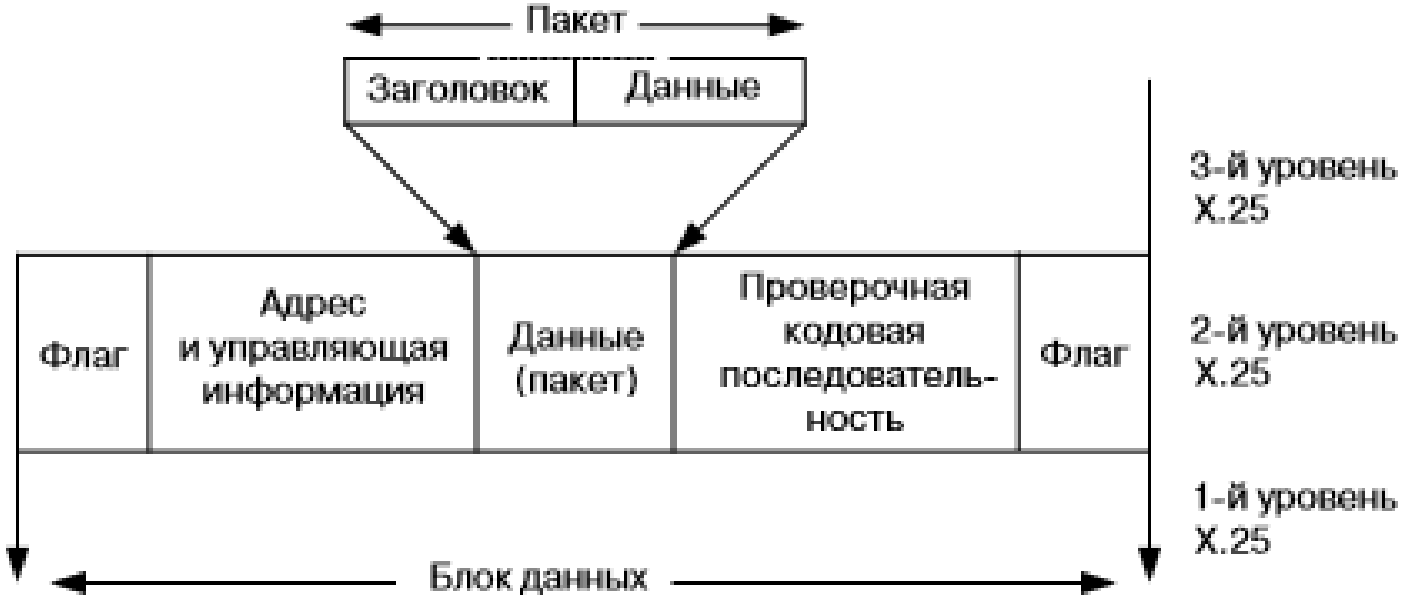
Российский СОРМ



32

Российский СОРМ

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



Команды СОРМ

№ команды	Название команды	
1	**Запуск СОРМ**	
2	**Остановка СОРМ**	
3	**Задание пароля**	
4	**Закрепление контрольной соединительной линии за группой**	
5	**Постановка объекта на контроль**	
6	**Снятие объекта с контроля**	
7	**Подключение к разговорному тракту**	
8	**Освобождение контрольной соединительной линии**	
9	**Исключение контрольной соединительной линии из группы**	

Команды СОРМ

№ команды	Название команды	
10	**Запрос на передачу данных об объектах наблюдения**	
11	**Запрос на передачу информации о соответствии между КСЛ и группами**	
12	**Запрос на передачу списка дополнительных видов обслуживания**	
13	**Прерывание выдачи сообщений на запросы содержимого таблиц**	
14	**Тестирование каналов передачи данных**	
15	**Изменение параметров объекта контроля**	
16	**Запрос на передачу информации о соответствии имени входящего пучка станции и его условного номера**	
17	**Запрос версии ПО станции**	

Каналы передачи данных между СОРМ и ПУ:

- **Канал 1 (30 КИ)** - используется для передачи управляющей информации – команд и сообщений.

- **Канал 2 (31 КИ)** – используется для передачи информации о наблюдаемых соединениях – сообщения.

- **Тракт ИКМ-30** –

- **1..15, 17..29 КИ**(Канальные интервалы) - или ВИ

для трансляции информации, передаваемой в контролируемых разговорных трактах.

- **16 КИ** - оборудованием **ТОР-4М (ПУ)** не обрабатывается.

Формат команд управления и сообщений канала 1:

Заголовок
Содержание команды (канал №1)

Заголовок **имеет следующий формат:**

	D7	D6	D5	D4	D3	D2	D1	D0
1	преамбула = CCH							
2	номер СОРМ							
3	код команды							
4	длина команды в байтах							
5	п							
6	а							
7	р							
8	о							
9	л							
10	ь							

Формат команд управления и сообщений канала 1:

Заголовок
Содержание команды (канал №1)

Рис. 2.2. Формат команды № 4

Расшифровка параметров заголовка:

Номер байта	Название	Описание
1	преамбула	Определяет истинную команду. Имеет одинаковое значение для всех команд
2	номер СОРМ	соответствующего центра коммутации подвижной связи (ЦКП).
3	код команды	
4	длина	количество байт поля содержания команды.
5-10	пароль	предотвращающим несанкционированный доступ в процесс функционирования СОРМ и к ее данным. Команды должны выполняться только при совпадении пароля в команде с действующим паролем в СОРМ

Формат сообщений канала 1 от СОРМ к ТОР- 4М (ПУ) :

Заголовок
Содержание сообщения (канал №1)

Заголовок **имеет следующий формат:**

	D7	D6	D5	D4	D3	D2	D1	D0
1	Преамбула = ССН							
2	Номер СОРМ							
3	код сообщения							
4	Длина сообщения в байтах							
5	Общее количество							
6	сообщений							
7	Номер текущего							
8	сообщения							
9	Тип регистра ЦКП							
10	Резерв							

Расшифровка параметров заголовка:

Номер байта	Название	Описание
1	преамбула	Определяет истинную команду. Имеет одинаковое значение для всех команд
2	номер СОРМ	соответствующего центра коммутации подвижной связи (ЦКП).
3	код команды	
4	длина	количество байт поля содержания команды.
5-6	доп. инф.	1 или дополнительные данные
7-8	Номер сообщения	Двоичное число
9	тип регистра ЦКП (GSM)	00Н - из базы данных **HLR** ЦКП 01Н - из базы данных **VLR** ЦКП

Команды канала 1: Данные об объекте наблюдения

(СООБЩЕНИЕ № 3):

КОД СООБЩЕНИЯ = 23Н

ОПИСАНИЕ: сообщения передаются в качестве ответа на команду "Запрос на передачу данных об объектах наблюдения".

Заголовок сообщения		
1	Условный номер	
2	объекта	
3	Тип объекта	
4	Признак номера телефона	
5	Кол-во знаков в номере телефона	
6	Ц2	Ц1
…		
14	Ц18	Ц17
15	FFH	
16	FFH	
17	Категория контроля	
18	Номер группы КСЛ	
19	Метка приоритета	
20	Состояние объекта	
21	Контроль местоположения	
22	Кол-во знаков в идентификатор IMSI	
23	Ц2	Ц1
…		
31	Ц18	Ц17

32	Кол-во знаков в идентификатор IMEI	
33	Ц2	Ц1
…		
41	Ц18	Ц17
42	Кол-во знаков в адресе местоположения	
43	MCC.2	MCC.1
44	MNC.1	MCC.3
45	LAC.1	MNC.2
46	CL.1	LAC.2
47	FH	CL.2
48	Состояние ПС	

Расшифровка параметров сообщения №3:

Описание параметров сообщения № 3
(“**Данные об объектах наблюдения**”)
аналогично соответствующим параметрам команды № 5 (“**Постановка объекта на контроль**).
При запросе данных о нескольких объектах наблюдения (
в команде № 10 “**Запрос на передачу данных об объектах наблюдения**”),
на ПУ должны выдаваться последовательно
сообщения № 3 о каждом наблюдаемом объекте СОРМ.

В сообщении № 3 выдаются

- **номер телефона** наблюдаемого объекта (байты с 6-го по 14-ый),
- идентификаторы **IMSI** (байты с 23-го по 31-ый),
- **IMEI** (байты с 33-го по 41-ый) с соответствующим параметром - количество знаков в номерной информации.

Расшифровка параметров сообщения №3:

Группа данных	Шифр	Описание
Состояние объекта	00H	объект имеет возможность пользования исходящей/входящей связью
	01H	абонент не имеет возможности пользования входящей связью
	02H	абонент не имеет возможности пользования исходящей связью
Местоположение наблюдаемого абонента в СПРС	MCC	код страны подвижной станции
	MNC	код сети подвижной связи
	LAC	зона действия ЦКП
	CL	сота (ячейка) сети подвижной связи
состояние подвижной станции	01H	зарегистрирована в СПРС;
	00H	не зарегистрирована в СПРС

Формат сообщений канала 2 от СОРМ к ПУ:

Заголовок
Содержание сообщения (канал №2)

Заголовок **имеет следующий формат:**

	D7	D6	D5	D4	D3	D2	D1	D0
1	Преамбула = ССН							
2	Номер СОРМ							
3	код сообщения							
4	Длина сообщения в байтах							
5	Номер							
6	вызова							
7	Тип объекта							
8	Условный номер							
9	объекта							
10	Признак отбора объекта							
11	Параметры связи							
12	Код фазы ДВО							

Развитие СОРМ от 70 к 268

Организация КПД теперь предусматривает два варианта реализации:
- с использованием КИ30 и КИ31 и протокола X.25;
- с использованием выделенного канала Ethernet и протокола TCP/IP.

При втором варианте КПД1 и КПД2 организовываются по выделенному каналу Ethernet с использованием протокола TCP/IP и двух программных портов. Порт 1 используется для организации КПД1. Порт 2 используется для организации КПД2.

Каждый пакет протокола TCP/IP передаваемых данных начинается с заголовка команды или сообщения. Не допускается размещение одной и той же команды или одного и того же сообщения в разных пакетах.

Допустимое время постановки объектов на контроль и снятие их с контроля на транзитных узлах связи при использовании протоколов X.25 и TCP/IP – не более 15 с.

46

Развитие СОРМ от 70 к 268

По аналогии с подвижным СОРМ-1, появилось сообщение 12, позволяющее передавать сообщения электросвязи.

Для крупных **транзитных** узлов максимальное число объектов контроля возросло с 1024 до 2048, а для оконечных и транзитно-оконечных — осталось равным 1024. Максимальное количество первичных цифровых потоков для транзитных и оконечно-транзитных узлов осталось равным 8, а для оконечных узлов — сократилось до 4.
Изменились таблицы зависимости максимального количества объектов контроля от номерной ёмкости и количества пучков каналов связи узла связи.

В командах, связанных с постановкой объекта на контроль, при указании признака номера телефона, исчезла возможность указания **зонового** номера. Вместо этого нужно указывать 10-значный федеральный (междугородний) номер.

47

Развитие СОРМ от 70 к 268

Номер команды	Название команды по приказу 268	Название команды по приказу 70 (если отличается от 268)	Код команды
1	Запуск технических средств ОРМ	Запуск СОРМ	01H
2	Останов технических средств ОРМ	Останов СОРМ	02H
3	Задание пароля		03H
4	Закрепление КСЛ за группой		04H
5	Постановка объекта на контроль		05H
6	Снятие объекта с контроля		06H
7	Подключение к разговорному тракту		07H
8	Освобождение контрольной соединительной линии		08H
9	Исключение контрольной соединительной линии из группы		09H
10	Запрос на передачу данных об объектах контроля	Запрос на передачу данных об объектах наблюдения	0AH
11	Запрос на передачу информации о соответствии между КСЛ и группами		0BH
12	Запрос на передачу списка услуг связи	Запрос на передачу списка дополнительных видов обслуживания	0CH
13	Прерывание выдачи сообщений на запросы содержимого таблиц		0DH
14	Тестирование каналов передачи данных		0EH
15	Изменение параметров объекта контроля		0FH
16	Запрос на передачу информации о соответствии имени пучка каналов и его условного номера	Запрос на передачу информации о соответствии имени входящего пучка станции и его условного номера	10H
17	Запрос версии ПО узла связи	Запрос версии ПО станции	11H

48

Развитие СОРМ от 70 к 268

Сообщения КПД 1

Номер сообщения	Название сообщения по приказу 268	Название сообщения по приказу 70 (если отличается от 268)	Код сообщения
1	Авария		21H
2	Перезапуск ПО станции		22H
3	Данные об объектах контроля	Данные об объектах наблюдения	23H
4	Информация о соответствии между КСЛ и группами		24H
5	Список услуг связи	Список ДВО абонента	25H
6	Несанкционированный доступ к программным средствам технических средств ОРМ	Несанкционированный доступ к программным средствам СОРМ	26H
7	Подтверждение приёма команды из пункта управления ОРМ	Подтверждение приёма команды из ПУ	27H
8	Подтверждение о выполнении команды из пункта управления ОРМ	Подтверждение о выполнении команды из ПУ	28H
9	Ответное тестовое сообщение		29H
10	Данные о соответствии условных номеров пучков каналов и их реальных станционных имен	Данные о соответствии условных номеров входящих пучков и их реальных станционных имен	2AH
11	Версия ПО станции		2BH
12	Передача сообщений электросвязи	–	2CH

Развитие СОРМ от 70 к 268

Сообщения КПД 2

Номер сообщения	Название сообщения по приказу 268	Название сообщения по приказу 70 (если отличается от 268)	Код сообщения
1.1	Прием полного номера телефона вызываемого абонента		41H
1.2	Ответ вызываемого абонента		42H
1.3	Разъединение		43H
1.4	Использование услуг связи	Использование услуг ДВО	44H
2.1	Подключение контрольной соединительной линии		51H
2.2	Освобождение контрольной соединительной линии		52H
2.3	Ответное тестовое сообщение		53H

50

Развитие СОРМ от 70 к 268

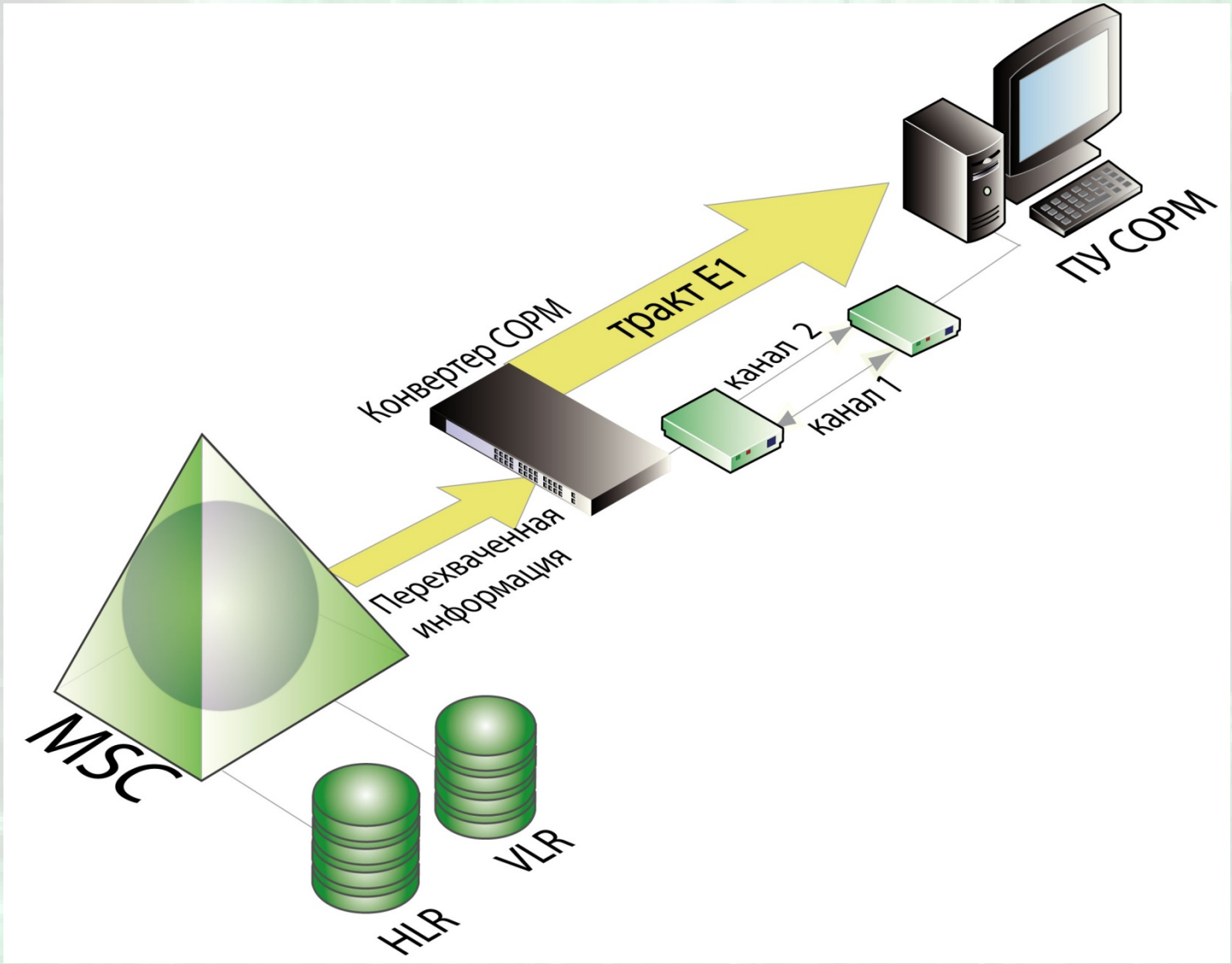
Некоторые выводы

Какие выгоды дает 268-й приказ?

1. Субъекты ОРД смогут получать новый вид информации: сообщения электросвязи.
2. ФСБ получает возможность на крупных транзитных узлах ставить на контроль не 1024 объекта, а целых 2048.
3. Квитанции на законных основаниях могут теперь потечь по TCP/IP. А это, во-первых, снимает проблемы X.25 (его просто не станет), а во-вторых, существенно увеличит пропускную способность квитанционного канала, что в свою очередь позволит получить гораздо больше статистики (например, при постановках по неполному номеру).
   При этом вариант доставки квитанций по X.25 всё равно остаётся. Поэтому ПУ должны уметь работать по обоим вариантам.
4. Для стационарного СОРМ-1 сохранилась потребность в 8-потоковых устройствах.

51

Организация СОРМ на СПС



Идентификаторы СОРМ

- Номер пользователя ТфОП, СПС
(MS ISDN)

- Идентификатор подвижного абонента для СПС (IMSI)

- Идентификатор подвижной станции СПС (IMEI)

- Местоположение абонента
(LAC, CellID)

Дополнительные сообщения.

Канал 1 **Сообщение № 12.**

«Передача коротких сообщений наблюдаемым абонентом»

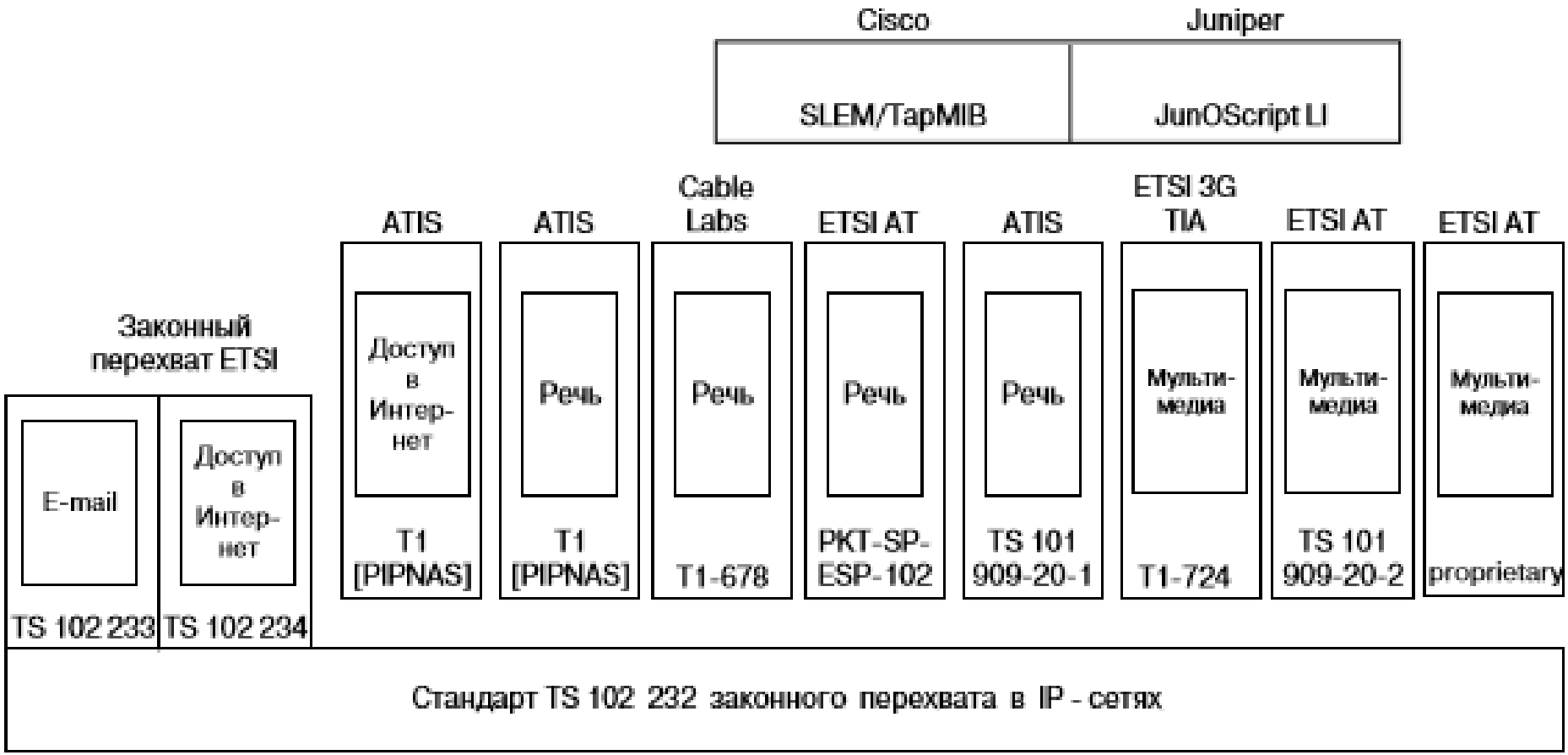
Канал 2 **Сообщение № 1.6**

«Изменение местоположения наблюдаемого абонента»

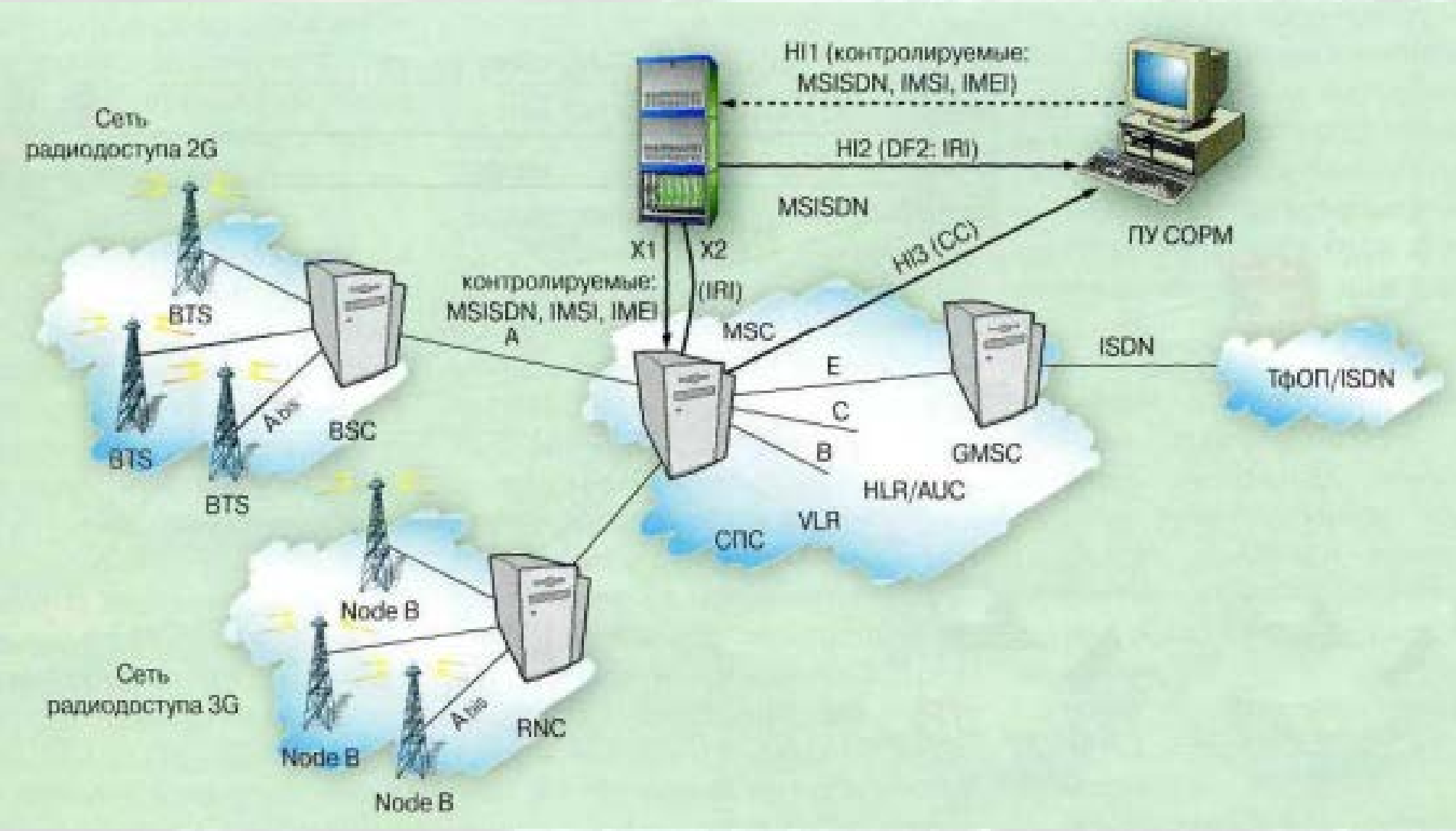
54

COPM 2

СОРМ 2


Cisco
Juniper
SLEM/TapMIB
JunOScript LI
ATIS
ATIS
Cable Labs
ETSI AT
ATIS
ETSI 3G TIA
ETSI AT
ETSI AT
Законный перехват ETSI
E-mail
Доступ в Интер-нет
Доступ в Интер-нет
Речь
Речь
Речь
Речь
Мульти-медиа
Мульти-медиа
Мульти-медиа
T1 [PIPNAS]
T1 [PIPNAS]
T1-678
PKT-SP-ESP-102
TS 101 909-20-1
T1-724
TS 101 909-20-2
proprietary
TS 102 233
TS 102 234
Стандарт TS 102 232 законного перехвата в IP - сетях

56


HI1 (контролируемые: MSISDN, IMSI, IMEI)
HI2 (DF2: IRI)
MSISDN
ПУ СОРМ
HI3 (CC)
X1
X2
(IRI)
контролируемые: MSISDN, IMSI, IMEI
A
MSC
E
C
B
GMSC
ISDN
ТфОП/ISDN
HLR/AUC
VLR
СПС
Сеть радиодоступа 2G
BTS
BTS
BTS
Abis
BSC
Node B
Node B
Node B
Abis
RNC
Сеть радиодоступа 3G

57

СОРМ 2

2003 г. Минсвязь РФ - первые документы: СОРМ-2.

•«Технические требования **к узлам** телематических служб и **передачи данных** для обеспечения проведения оперативно+розыскных мероприятий»

•«Технические требования **к устройству** системы технических средств по обеспечению функций оперативно+розыскных мероприятий на узлах телематических служб и **передачи данных**»

Протокол управления – TCP/IP
Протокол передачи данных - … .

58

СОРМ 2

2014г. Минсвязь РФ – Приказ **№ 83**

- **Email** (электронный почтовый адрес) (SMTP, POP3, IMAP4, HTTP)
mail.ru, yandex.ru, rambler.ru, gmail.com, yahoo.com, aport.ru, rupochta.ru, hotbox.ru

- **ID IM** (icq и др)

- **ID** пользователя услуг (в том числе **OTT call**)

59

СОРМ в СПД Приказ №83 2014г

Класс Технических средств ОРМ	Скорость потока информации, поступающей на технические средства ОРМ, Мбит/с, не менее	Суммарная скорость передачи данных на выходе технического средства ОРМ, предназначенном для связи с ПУ, Мбит/с
I	**100**	Не менее 5% от скорости поступающего потока информации на технические средства ОРМ
II	**400**	
III	**900**	
IV	**4 000**	> 100
V	**9 000**	> 100
VI	**20 000**	> 1000
VII	**100 000**	> 1000

Идентификаторы СОРМ Приказ №83 2014г

- **IPv4 или IPv6**
- **MAC-адрес**
- **IMSI** (международный идентификатор абонента)
- **IMEI** (международный идентификатор мобильного оборудования)
- **MIN** (ID мобильной абонентской радиостанции)
- **Email** (электронный почтовый адрес) (SMTP, POP3, IMAP4, HTTP)

mail.ru, yandex.ru, rambler.ru, gmail.com, yahoo.com, aport.ru, rupochta.ru, hotbox.ru

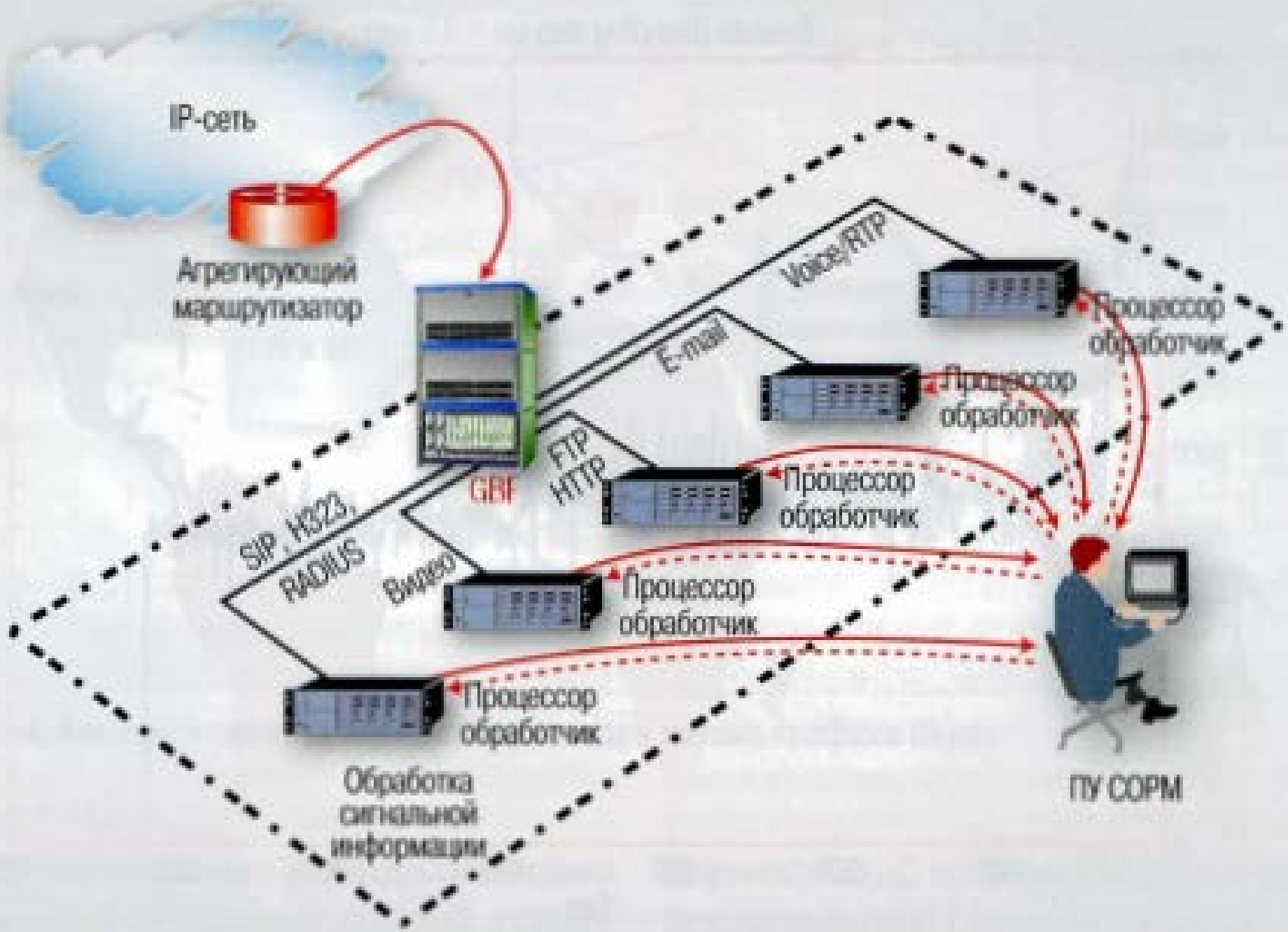
- имя **учетной записи** пользователя
- идентификатор служб обмена сообщениями (IM)

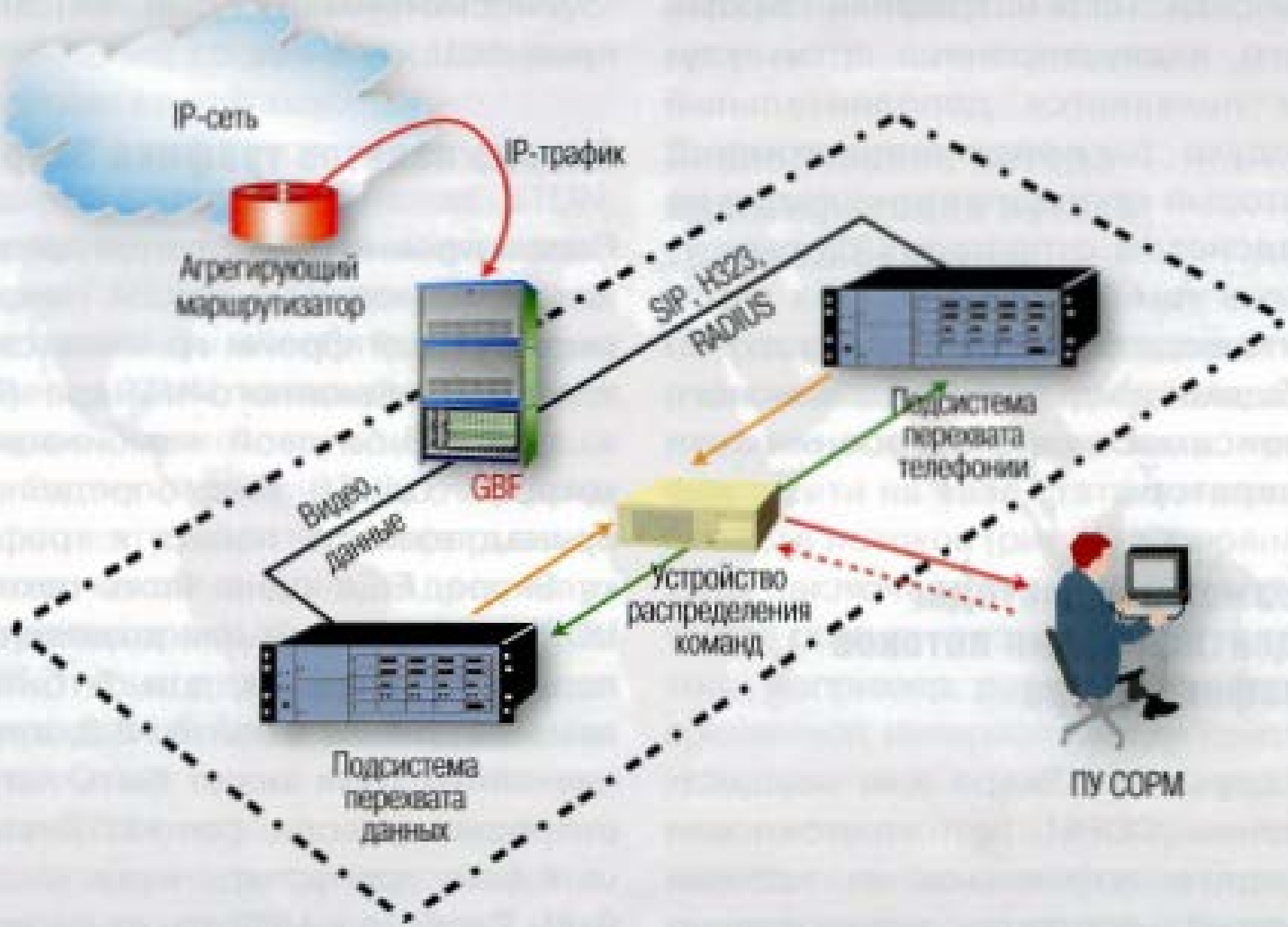
(ICQ, MailRu Agent, Jabber, QIP, Yahoo Messenger, Google Talk, AirWay Chat, IRC и пр)

«В контакте», «Одноклассники», «Мой Мир» и т.п.

- идентификатор пользователя услуг (в том числе OTT call)
- идентификатор абонентской телефонной линии
- **телефонный номер (A и B)**.

61


IP-сеть
Агрегирующий маршрутизатор
GRE
Voice/RTP
E-mail
FTP
HTTP
SIP, H323, RADIUS
Видео
Процессор обработчик
Процессор обработчик
Процессор обработчик
Процессор обработчик
Процессор обработчик
Обработка сигнальной информации
ПУ СОРМ


IP-сеть
IP-трафик
Агрегирующий маршрутизатор
SIP, H323, RADIUS
GBF
Видео, данные
Подсистема перехвата телефонии
Устройство распределения команд
Подсистема перехвата данных
ПУ СОРМ

63

X.25, V.24
CCC/CDC
Центр перехвата
Устройство посредника
Probe - точка съема
HI1
HI2
HI3
SIP, H.323
RTP
RTP
RTP
Транспортная сеть
SBC
AS
CSCF
HSS
Ядро IMS
Медиа-шлюз
ТфОП

64

Хранение данных

Вся отобранная информация хранится в энергозависимой памяти объемом не менее **2 Гбайт**, записывается на внутренне устройство записи в режиме кольцевого буфера, которое должно обеспечивать хранение информации за период **не менее 12 часов**. При этом должна быть возможность повторной обработки данных из кольцевого буфера, со скоростью не меньшей скорости записи.

65

Интерфейс взаимодействия

Для взаимодействия технический средств ОРМ с ПУ, разработан протокол, который так и называется, протокол взаимодействия технический средств ОРМ с ПУ.

Данный протокол делится на два:

- протокол передачи данных
- протокол управления.

На логическом уровне между ПУ и техническими средствами ОРМ, обеспечивается соединение в виде TCP-сессии, которое в свою очередь использует TCP как транспортный протокол, а IP как сетевой.

66

Интерфейс взаимодействия СОРМ и сети

- Ethernet 100/1G/10G (copper/fiber)
- SDH (1-64)
- E1, E3, E4, STM-1
- V11-36, X21

67

Интерфейс взаимодействия

- Номера портов используемые в соединение не должны попадать в номера из диапазона стандартных служб. Запрещено подключение нескольких ПУ на один и тот же порт.

- Настройка и конфигурирование технических средств осуществляется с ПУ, который подключается по **№0 каналу(канал определяется портами 16117 и 16118)**.

68

Протокол управления

• **команды**, передаваемые с ПУ;

• **ответы**, передаваемые с СОРМ на ПУ и содержащие результаты выполнения команд;

• **извещения**, передаваемые с СОРМ на ПУ и содержащие данные о произошедших в СОРМ событиях

• **подтверждения** о получении извещения от СОРМ, передаваемые с ПУ на СОРМ

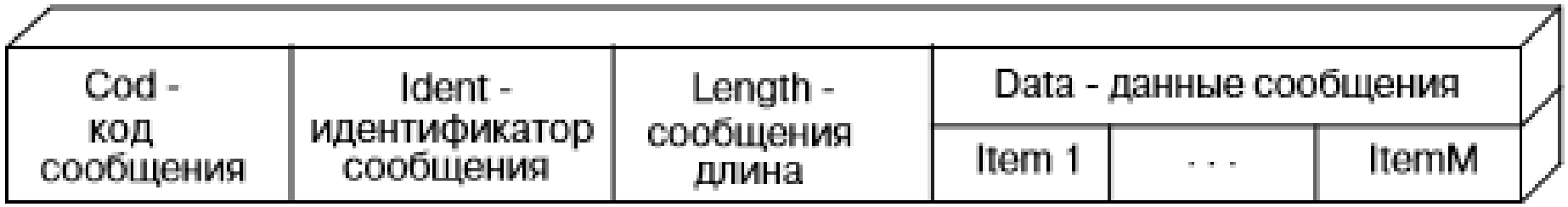


Рис. 4.6. Общая структура сообщений протокола управления

69

Протокол управления

- **команды**

  - инициирования, рестарта и проверки работоспособности канала СОРМ;

  - постановки на контроль, отмены контроля и изменения вида контроля;

  - запроса времени, коррекции часов;

  - включения и отмены фильтра;

  - команды установки параметров отбора и политики фильтрации;

  - команды назначения и отмены параметров сервера аутентификации,
  - и другие

70

Протокол управления

CodItem	LengthItem	Value					
		UCI	Ncontrol	IdCon	Filter	Find	BufPeriod

Рисунок 8. Структура элементов данных Item1, ..., ItemM
команды постановки на контроль и изменения вида контроля.

Содержимое поля CodItem:
0 – установка ID пользователя и вида его контроля;
1 – контроль по имени учетной записи пользователя - login (идентификатор объекта);
2 – контроль по телефонному номеру;
…

71

Протокол управления

Содержимое поля CodItem:

0 – сервер аутентификации Radius IPv4;

1 – сервер аутентификации Radius IPv6;

2 – сервер аутентификации Tacacs+ IPv4;

3 – сервер аутентификации Tacacs+ IPv6;

4 – сервер аутентификации Diameter IPv4;

5 – сервер аутентификации Diameter IPv6.

Протокол передачи данных.

Протокол передачи данных обеспечивает трансляцию с технических средств ОРМ на ПУ

- не декодированных (в виде IP пакетов)
- декодированных (в виде сообщений прикладных протоколов) отобранных
данных.

Для передачи отобранных данных используется отдельное TCP-соединение.

Протокол передачи данных

В протоколе передачи данных используются следующие сообщения:

- извещения, содержащие данные – передаются с технических средств ОРМ на ПУ;
- извещения контроля работоспособности канала передачи данных – передаются через заданный период времени с технических средств ОРМ на ПУ при отсутствии реального потока данных;
- подтверждение о получении извещений (данных) – передаются с ПУ на технические средства ОРМ.
- Извещения и подтверждения, используемые в протоколе передачи (далее – фреймы).

74

Телематические службы

1. Почтовые сервисы Web-mail, включая:
   mail.ru;
   yandex.ru;
   rambler.ru;
   gmail.com;
   yahoo.com.
   apport.ru;
   rupochta.ru
   hotbox.ru;

2. Службы обмена мгновенными сообщениями, включая:
   ICQ.

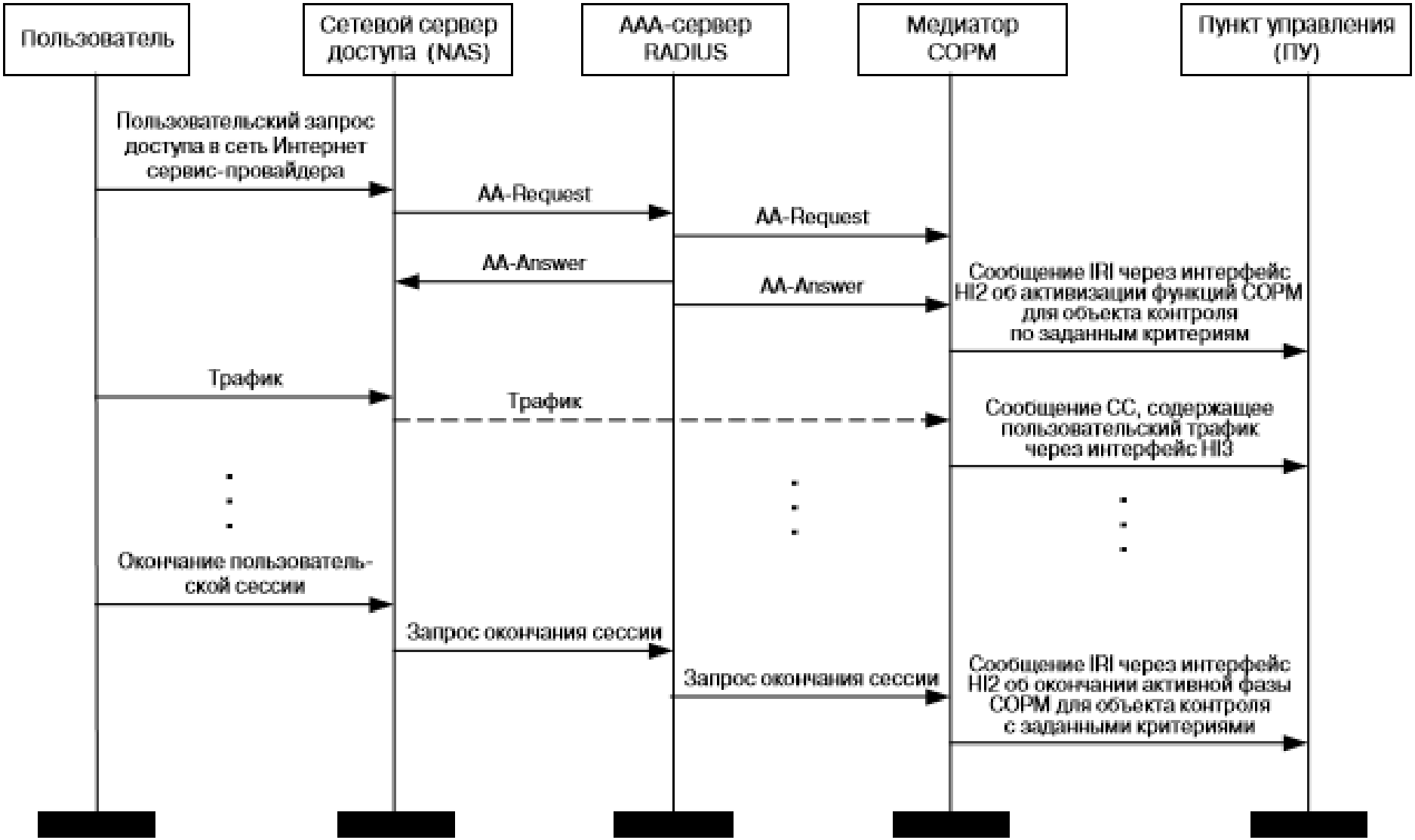
- решение о законном перехвате IP-сообщений

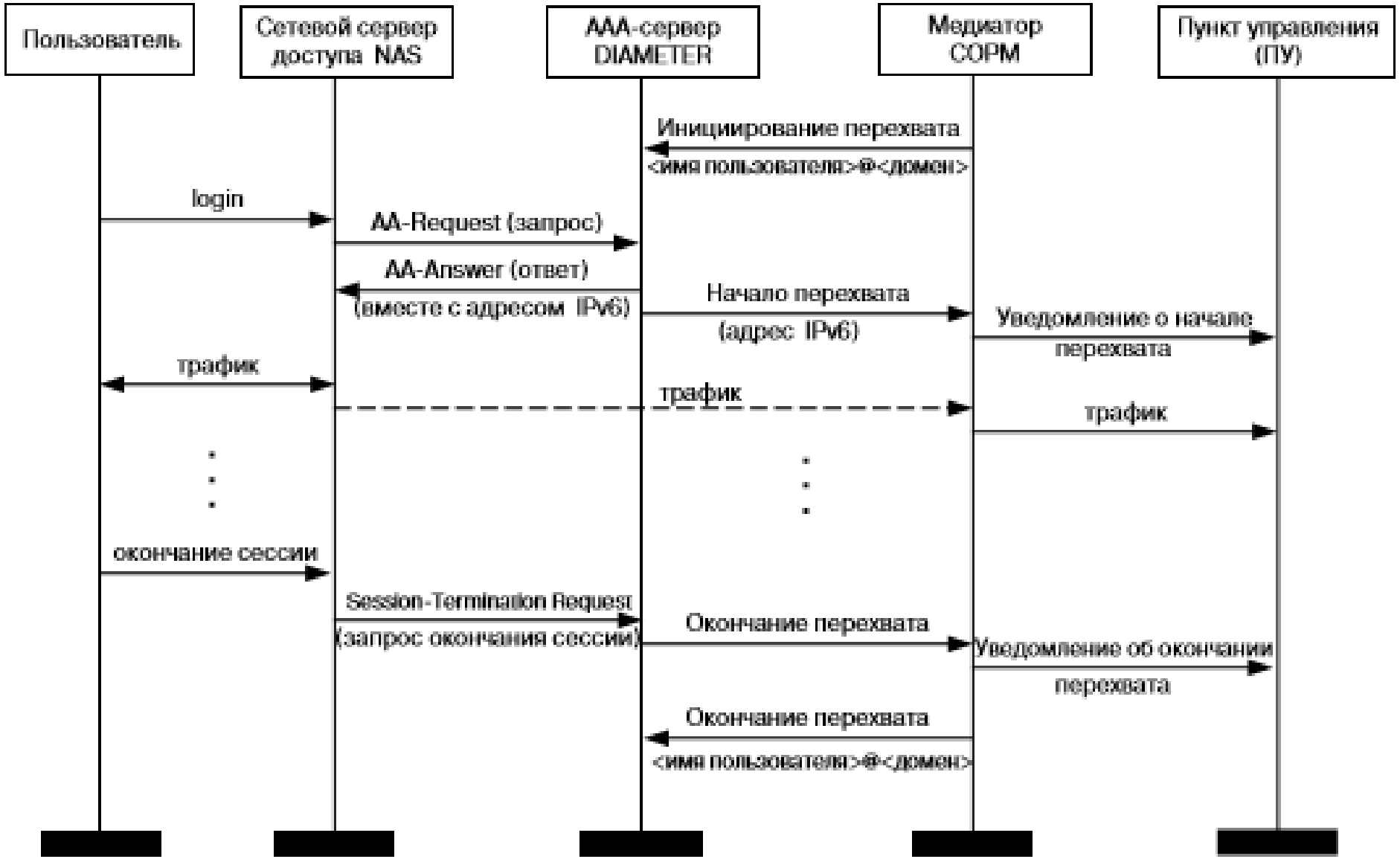
(трафик пользователя или организации перехвачен)

- в БД провайдера находится пользователь
- DHCP назначает пользовательскому компьютеру IP-адрес;
- RADIUS.
- СОРМ-2 записывает IP-адрес пользователя
- СОРМ перехватывает все IP-пакеты и передает в органы;

- DHCP и СОРМ-2 обновляют IP-адрес

76


Пользователь
Сетевой сервер доступа (NAS)
AAA-сервер RADIUS
Медиатор СОРМ
Пункт управления (ПУ)
Пользовательский запрос доступа в сеть Интернет сервис-провайдера
AA-Request
AA-Request
AA-Answer
AA-Answer
Сообщение IRI через интерфейс HI2 об активизации функций СОРМ для объекта контроля по заданным критериям
Трафик
Трафик
Сообщение CC, содержащее пользовательский трафик через интерфейс HI3
Окончание пользователь-ской сессии
Запрос окончания сессии
Запрос окончания сессии
Сообщение IRI через интерфейс HI2 об окончании активной фазы СОРМ для объекта контроля с заданными критериями


Пользователь
Сетевой сервер доступа NAS
AAA-сервер DIAMETER
Медиатор СОРМ
Пункт управления (ПУ)
Инициирование перехвата
<имя пользователя>@<домен>
login
AA-Request (запрос)
AA-Answer (ответ)
(вместе с адресом IPv6)
Начало перехвата
(адрес IPv6)
Уведомление о начале перехвата
трафик
трафик
трафик
окончание сессии
Session-Termination Request
(запрос окончания сессии)
Окончание перехвата
Уведомление об окончании перехвата
Окончание перехвата
<имя пользователя>@<домен>

78

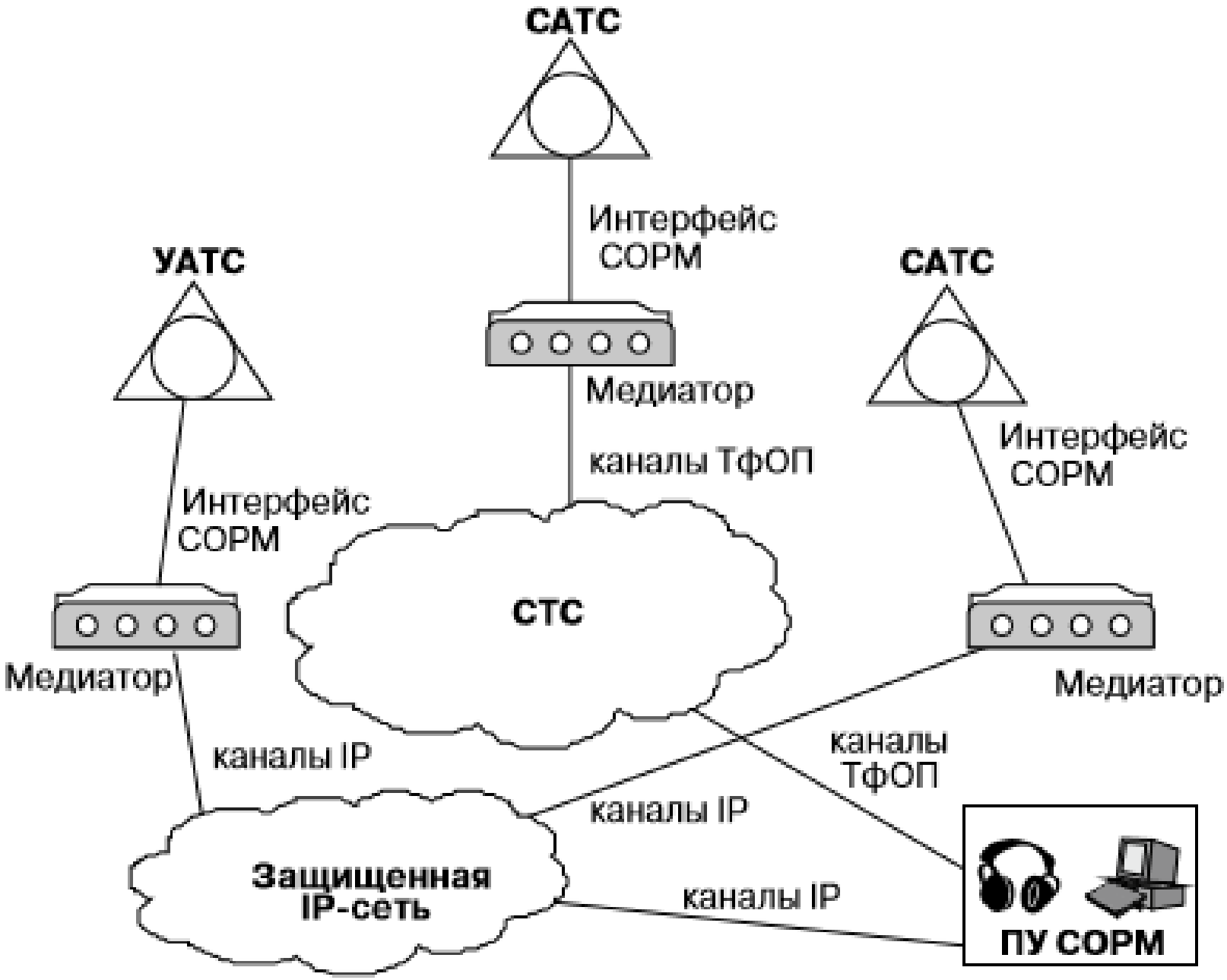
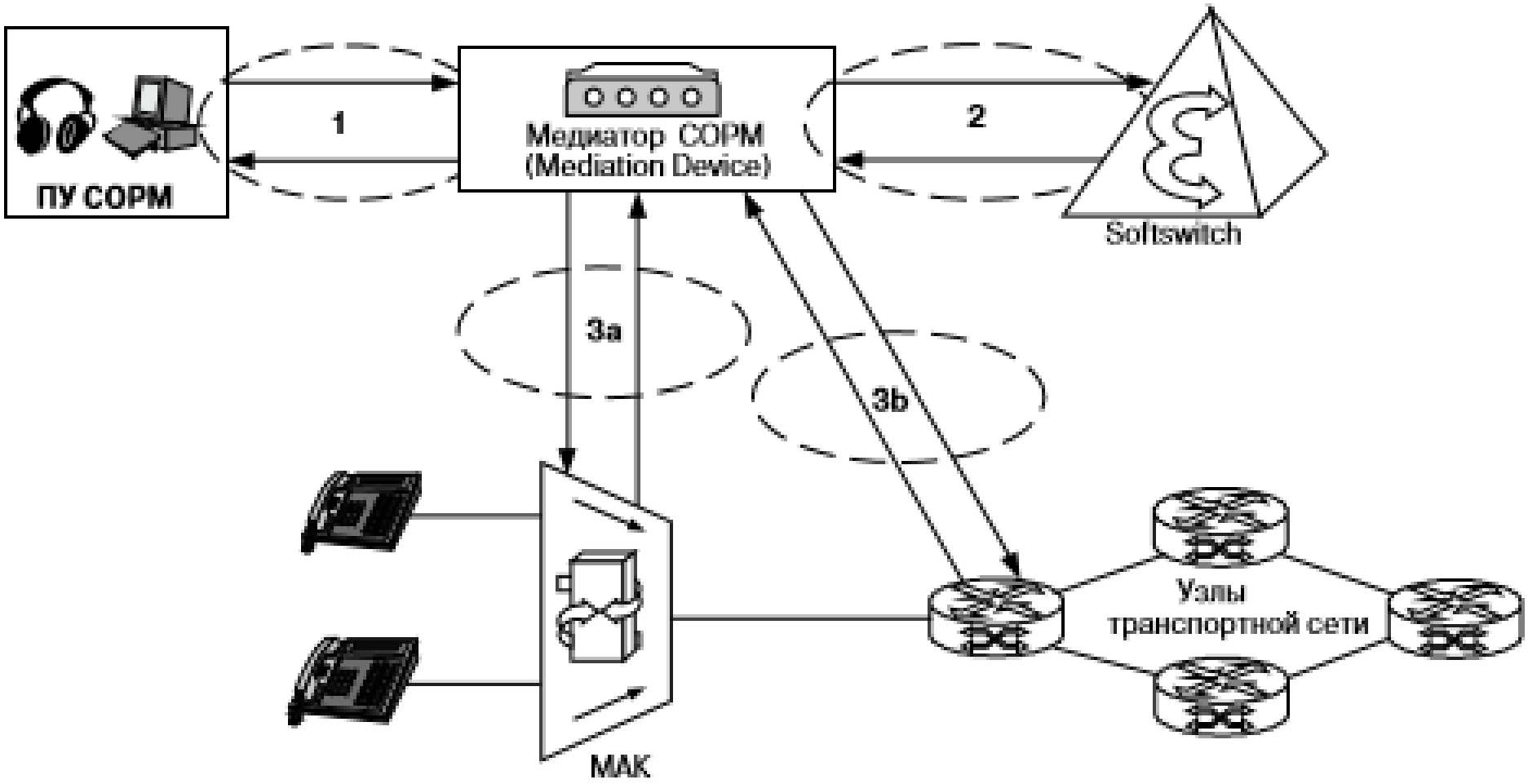
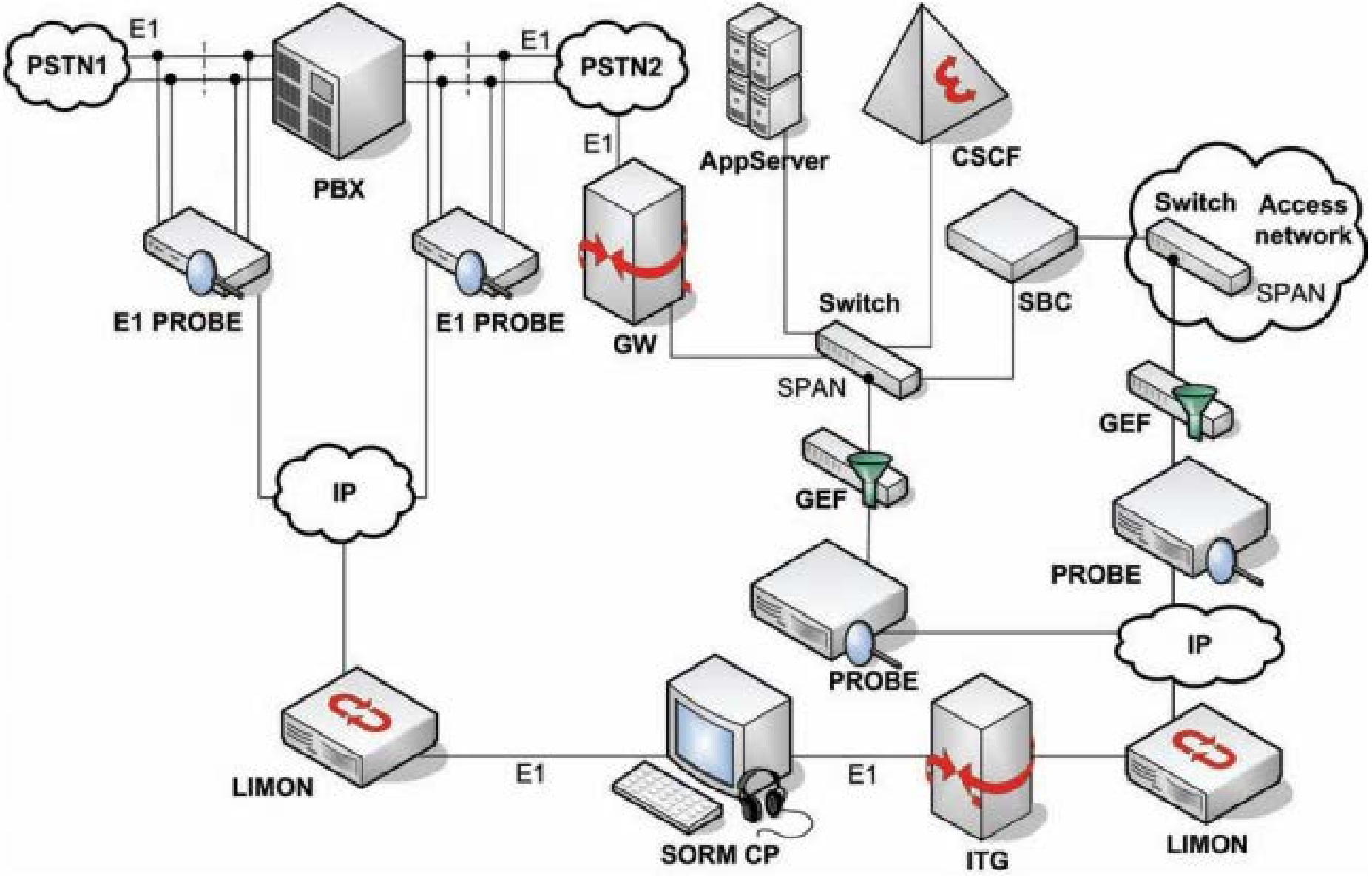


Рис. 5.3. Съем пользовательской информации с АТС малой емкости

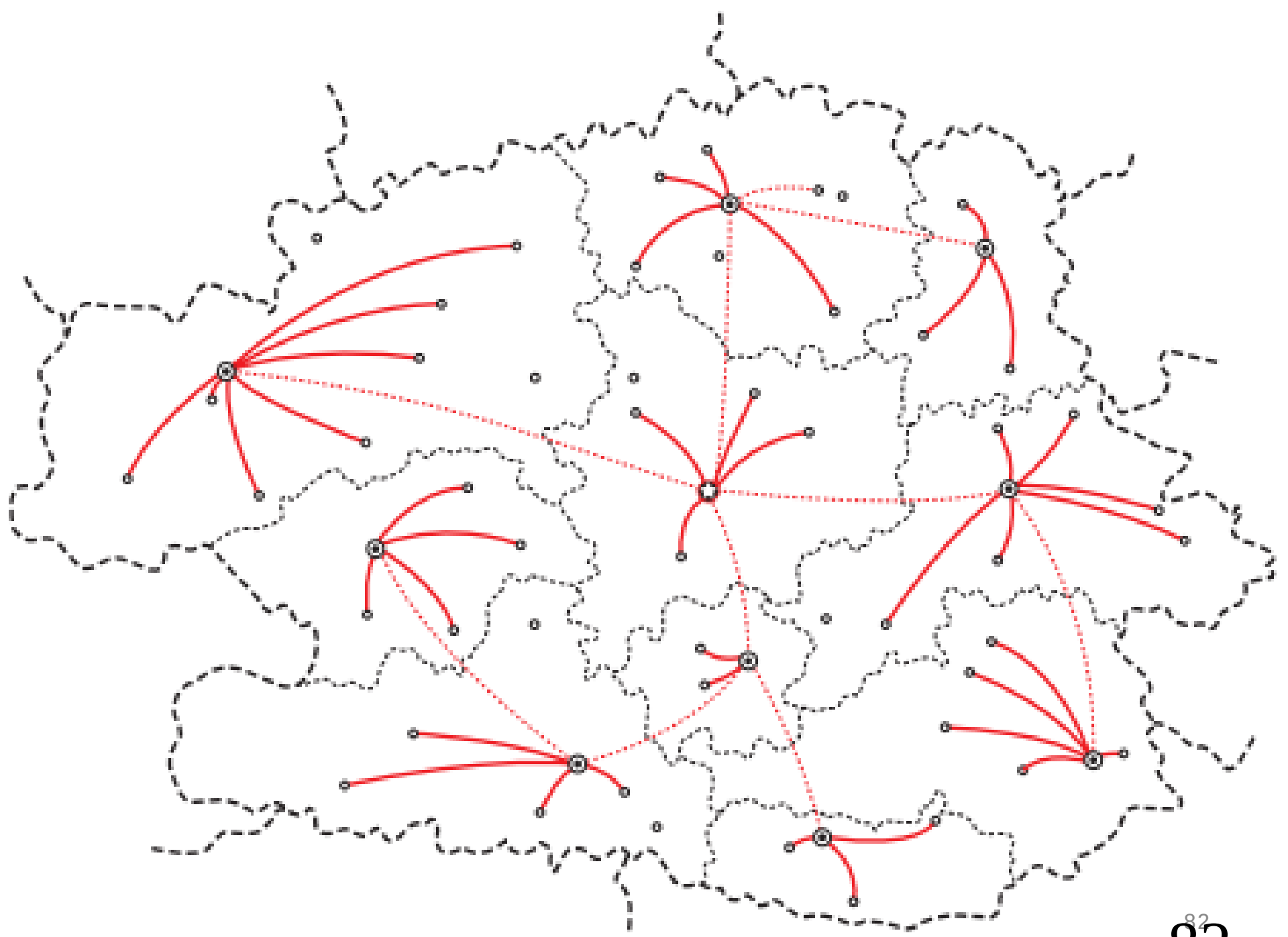
79


ПУ СОРМ
1
Медиатор СОРМ
(Mediation Device)
2
Softswitch
3a
3b
МАК
Узлы
транспортной сети

80


PSTN1
E1
PBX
E1
PSTN2
E1
AppServer
CSCF
Switch
Access network
SPAN
SBC
E1 PROBE
E1 PROBE
GW
Switch
SPAN
GEF
GEF
IP
PROBE
PROBE
IP
LIMON
E1
SORM CP
E1
ITG
LIMON

81



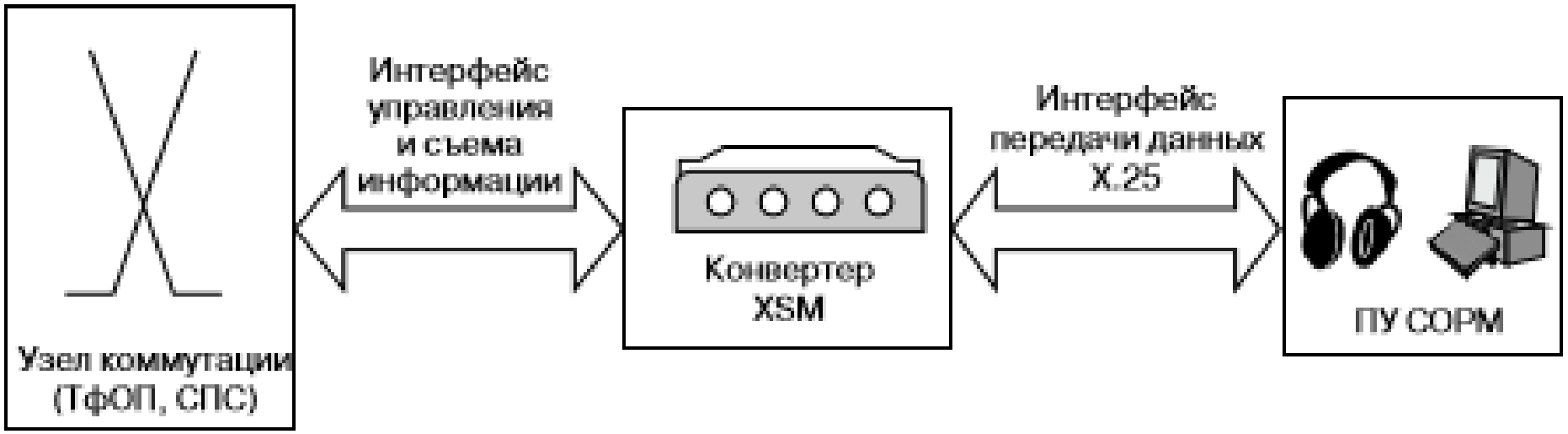


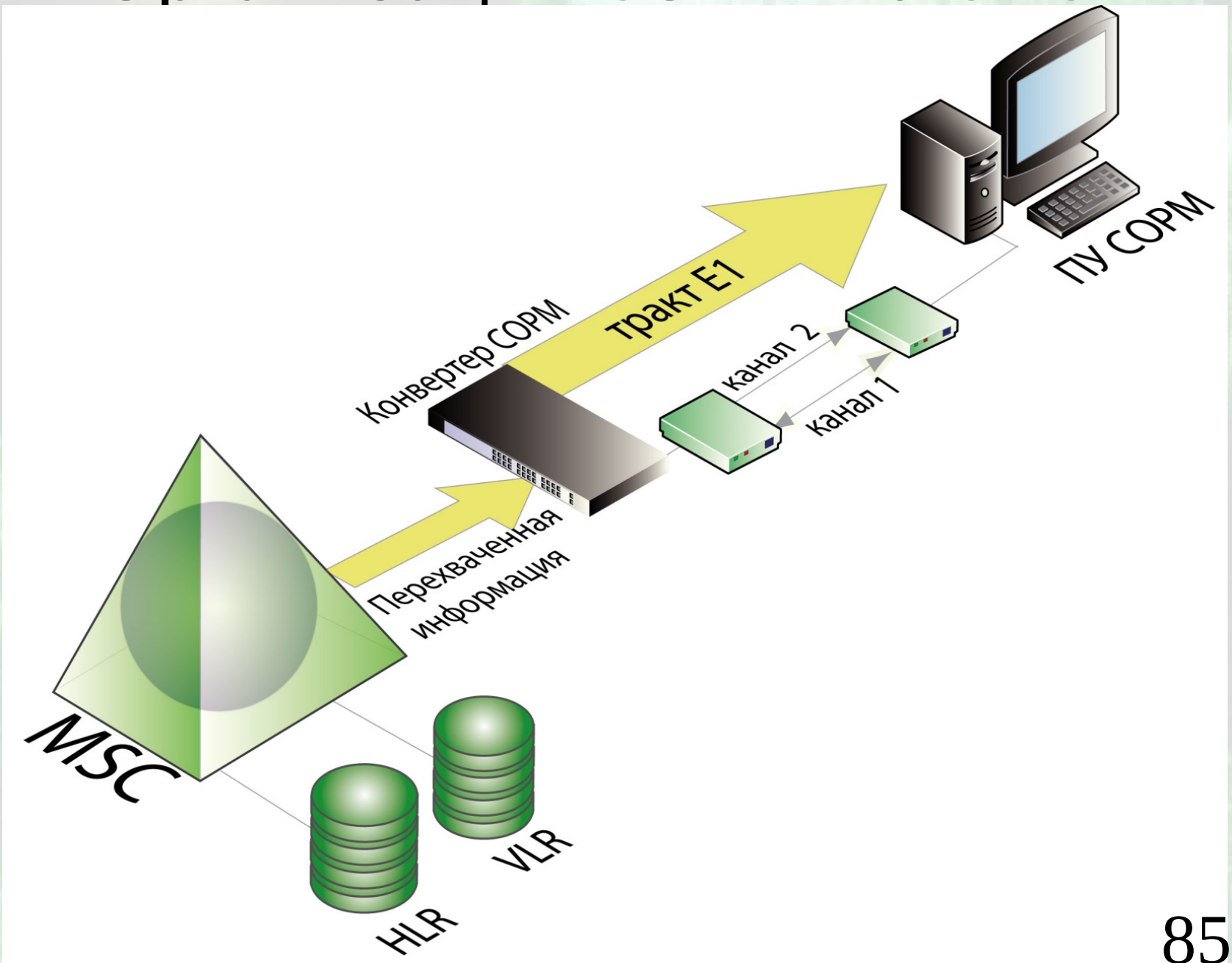
Рис. 5.1. Конвертер СОРМ для ТфОП, СПС и NGN

83

COPM и DPI

84

Организация СОРМ на СПС



Для использования системы DPI в качестве СОРМ следует обеспечить

строго конфиденциальную передачу запрашиваемых данных на пульт управления (ПУ) СОРМ,
в соответствии с приказом Минкомсвязи.

Например, за счет применения **конвертора СОРМ**.

DPI для СОРМ:

- контроль сессии каждого пользователя
- каждого устройства доступа
- контроль приложений абонента
- перенаправление трафика на внешние устройства для целей СОРМ.

Например, для приложений мгновенного обмена сообщениями (instant message (IM)), IP-телефонии, социальных сетей и электронной почты.

87

Схема подключения и анализ характеристик.

Структурно DPI в рамках законного перехвата включает в себя два модуля:

1) Управляющий сервер (УС), включающий в себя:

– DPI Engine;

– сервисные логики;

– модуль работы с платой.

2) Аппаратный фильтр (АФ) или плата DPI.

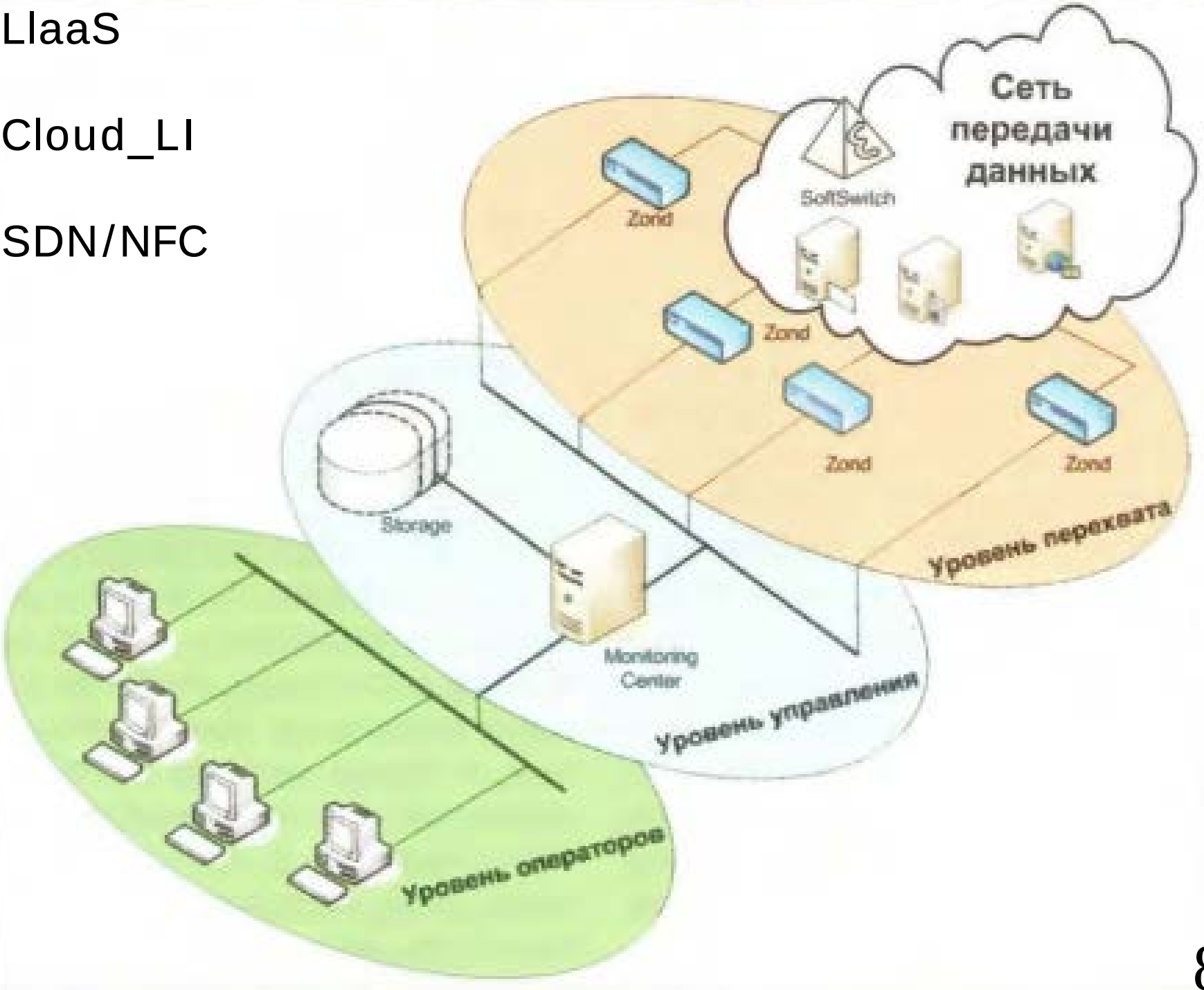
Управляющий сервер (УС) представляет собой многопоточное приложение, которое берет на себя функции взаимодействия с внешними системами по IP-сети, классификацию проходящего сквозь систему трафика, определение политик

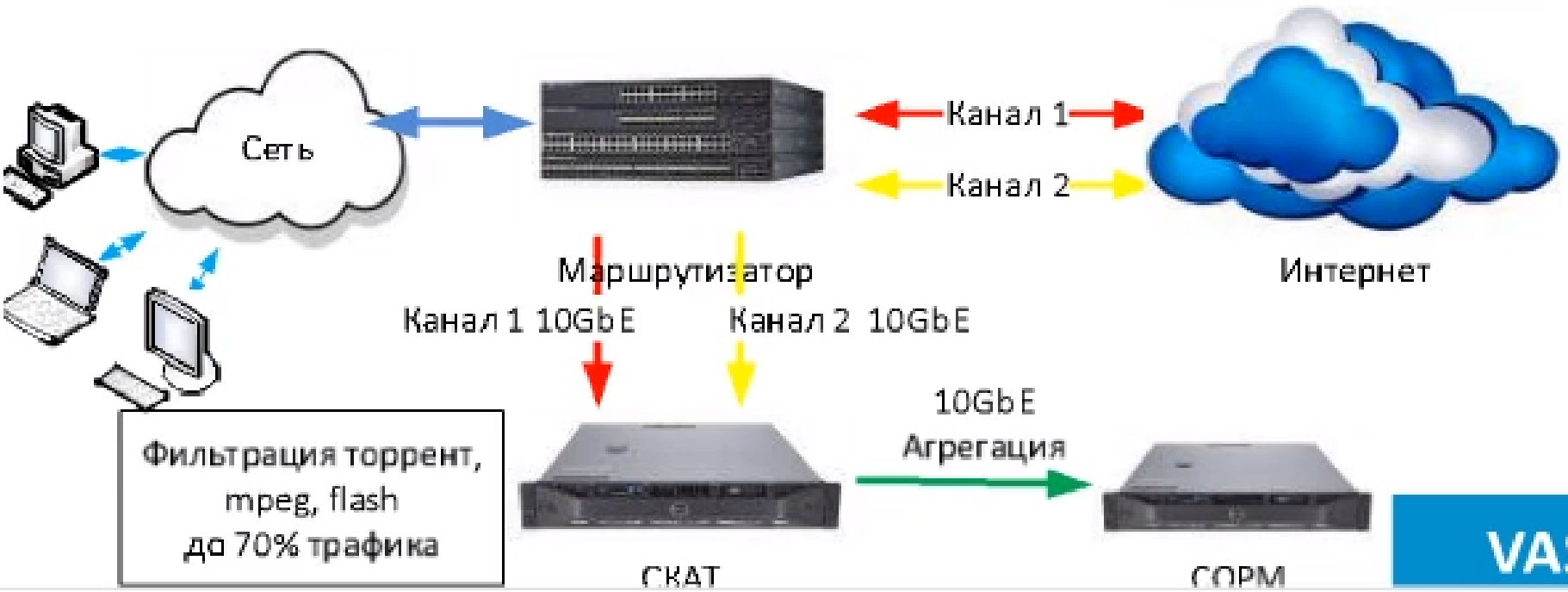
88

LlaaS

Cloud_LI

SDN/NFC




Сеть
Канал 1
Канал 2
Интернет
Маршрутизатор
Канал 1 10GbE
Канал 2 10GbE
10GbE
Агрегация
Фильтрация торрент,
mpeg, flash
до 70% трафика
СКАТ
СОРМ
VAS

90

COPM 3?

91

СОРМ 3?

??? Постановление Правительства РФ
??? № 538 от 27.08.2005 г

сбор и накопление информации
об абонентах телефонии
и (или)
сети передачи данных.

Информации о совершенных платежах

92

СОРМ 3?

• дату и время начала соединения;
• длительность соединения, с;
• тип соединения;
• услуги связи при соединении;
• тип вызывающего абонента;
• коммутатор, обслуживший соединение;
• тип вызываемого абонента;
• идентификатор оператора связи или филиала;
• идентификаторы вызывающего и вызываемого абонента;
• набранный номер вызываемого абонента;
• телефонный номер при переадресации.
• местоположение вызывающего и вызываемого абонента на начало и конец вызова.

93

СОРМ 3?

- служебные сообщения,

- мгновенные сообщения (ICQ, MailRu Agent, Jabber, QIP, Yahoo Messenger, Google Talk, AirWay Chat, IRC),

- короткие сообщения,

- мультимедийных сообщениях.

94

СОРМ 3?

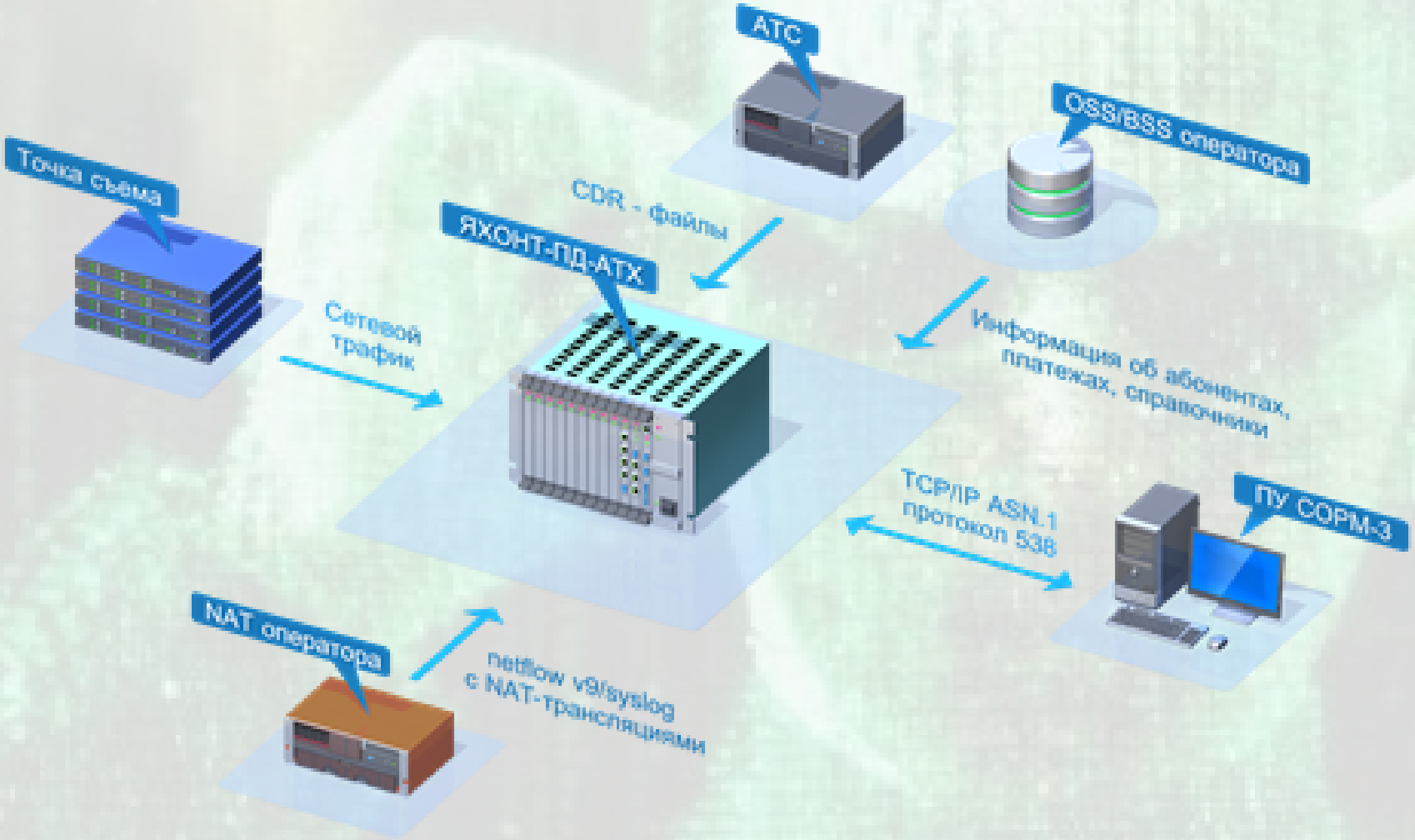
КПД1 – канал управления;

КПД2 – канал данных;

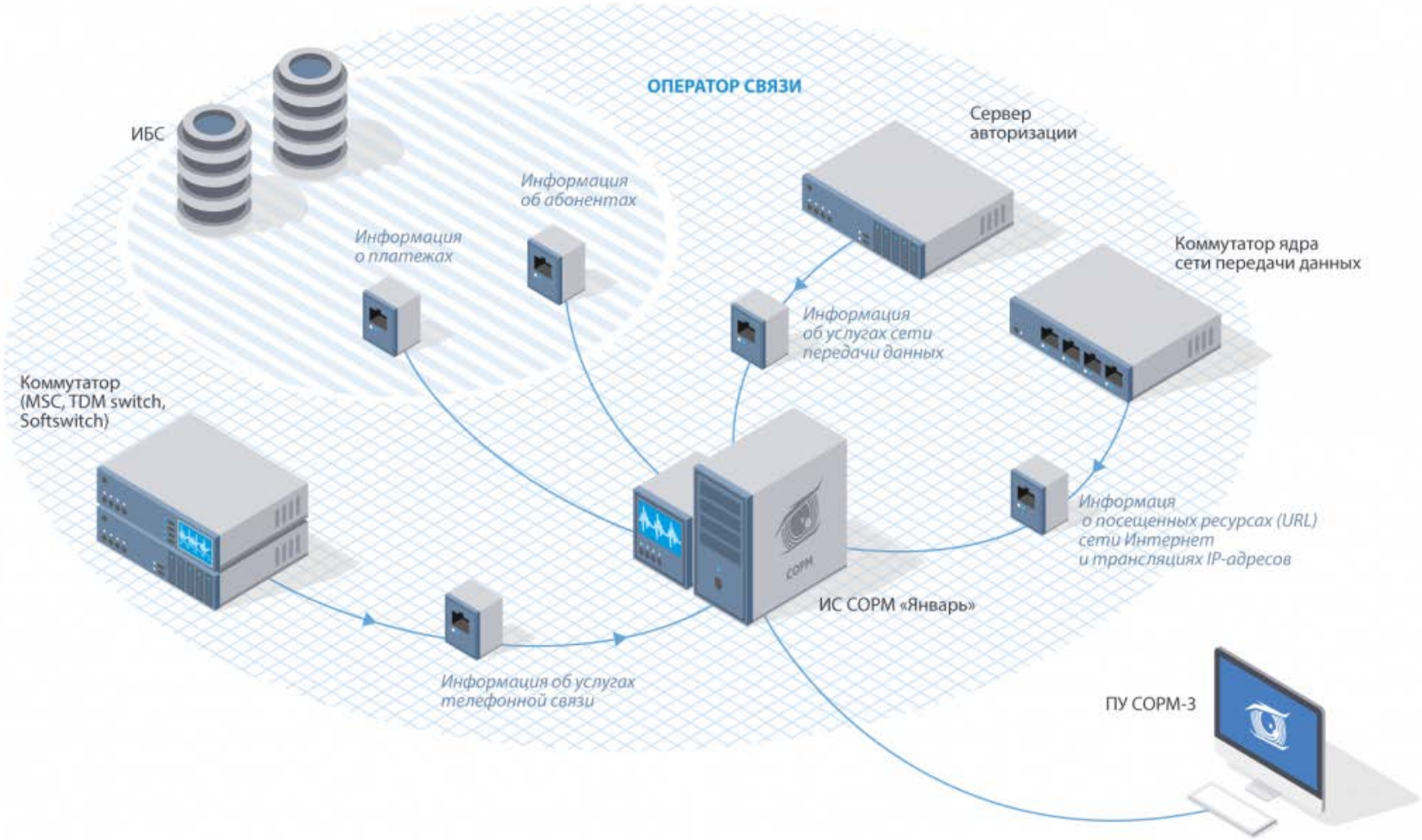
КПД3 – канал мониторинга;

КПД4 – канал неформатированных данных.

95

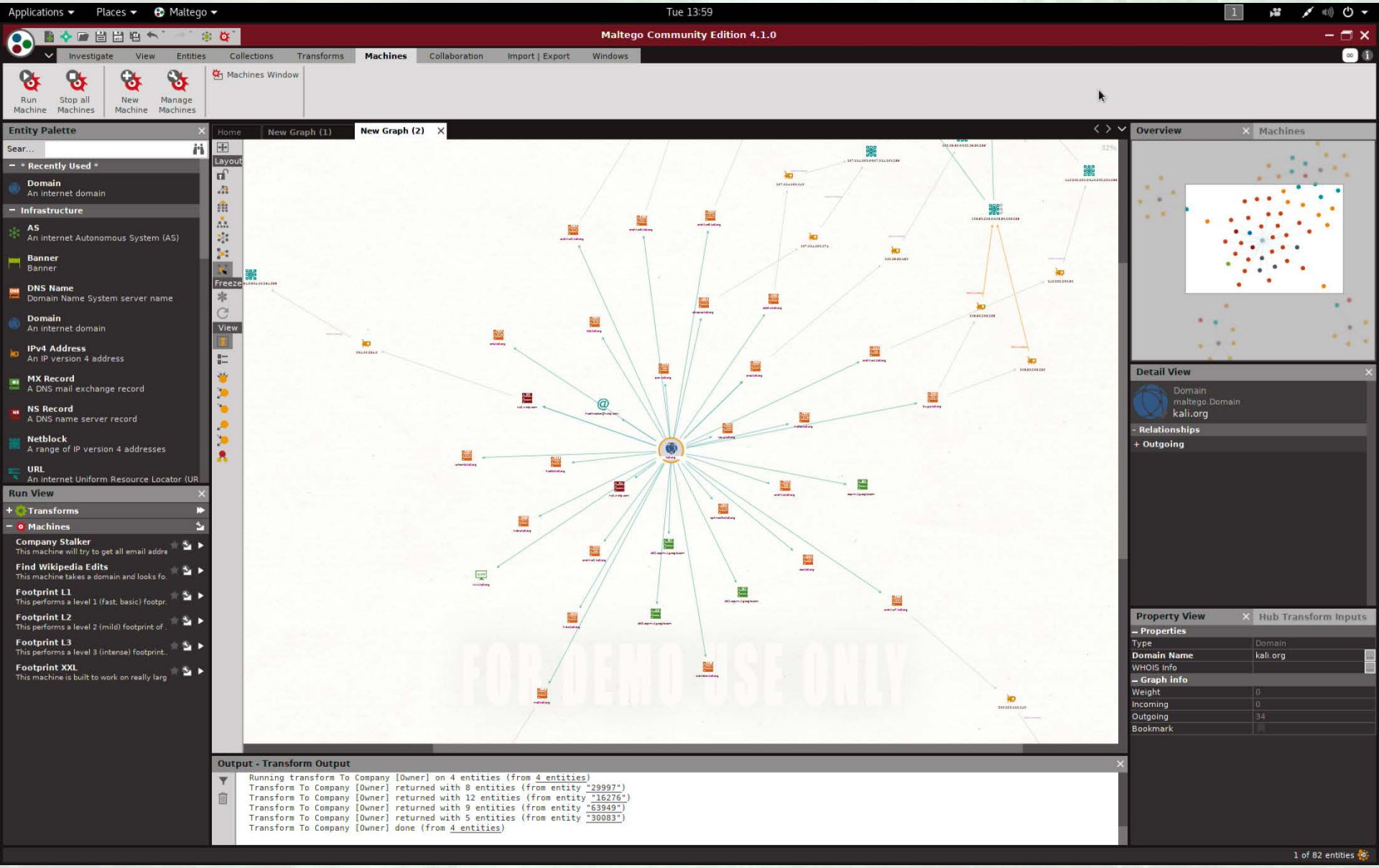

АТС
OSS/BSS оператора
Точка съема
CDR - файлы
ЯХОНТ-ПД-АТХ
Сетевой трафик
Информация об абонентах, платежах, справочники
TCP/IP ASN.1 протокол 538
ПУ СОРМ-3
NAT оператора
netflow v9/syslog с NAT-трансляциями

96


ОПЕРАТОР СВЯЗИ
ИБС
Информация об абонентах
Информация о платежах
Сервер авторизации
Коммутатор ядра сети передачи данных
Информация об услугах сети передачи данных
Коммутатор (MSC, TDM switch, Softswitch)
СОРМ
Информация о посещенных ресурсах (URL) сети Интернет и трансляциях IP-адресов
ИС СОРМ «Январь»
Информация об услугах телефонной связи
ПУ СОРМ-3

97

98


Applications
Places
Maltego
Tue 13:59
Maltego Community Edition 4.1.0
Investigate
View
Entities
Collections
Transforms
Machines
Collaboration
Import | Export
Windows
Run Machine
Stop all Machines
New Machine
Manage Machines
Machines Window
Entity Palette
Recently Used
Domain
An internet domain
Infrastructure
AS
An internet Autonomous System (AS)
Banner
Banner
DNS Name
Domain Name System server name
Domain
An internet domain
IPv4 Address
An IP version 4 address
MX Record
A DNS mail exchange record
NS Record
A DNS name server record
Netblock
A range of IP version 4 addresses
URL
An internet Uniform Resource Locator (UR
Run View
Transforms
Machines
Company Stalker
This machine will try to get all email addre
Find Wikipedia Edits
This machine takes a domain and looks fo.
Footprint L1
This performs a level 1 (fast, basic) footpr.
Footprint L2
This performs a level 2 (mild) footprint of .
Footprint L3
This performs a level 3 (intense) footprint..
Footprint XXL
This machine is built to work on really larg
Home
New Graph (1)
New Graph (2)
Layout
Freeze
View
Overview
Machines
Detail View
Domain
maltego.Domain
kali.org
Relationships
Outgoing
Property View
Hub Transform Inputs
Properties
Type
Domain
Domain Name
kali.org
WHOIS Info
Graph info
Weight
0
Incoming
0
Outgoing
34
Bookmark
FOR DEMO USE ONLY
Output - Transform Output
Running transform To Company [Owner] on 4 entities (from 4 entities)
Transform To Company [Owner] returned with 8 entities (from entity "29997")
Transform To Company [Owner] returned with 12 entities (from entity "16276")
Transform To Company [Owner] returned with 9 entities (from entity "63949")
Transform To Company [Owner] returned with 5 entities (from entity "30083")
Transform To Company [Owner] done (from 4 entities)
1 of 82 entities

99

Спасибо за внимание.

Далее: Особенности применения DPI оператором связи

Вопросы?

Ст. преп. каф. Инфокоммуникационных систем СПбГУТ,

Фицов Вадим Владленович,

100