

Telsoft

# IMS Core

Инструкция по эксплуатации

Document version: 1

## Правовая информация

Copyright © 2002-2024 Telsoft. Все права защищены.

Никакая часть данного документа не может быть воспроизведена или обработана в системах обработки данных, скопирована или использована в других документах без письменного уведомления компании ООО «Телсофт».

Информация, содержащаяся в данном документе, может быть изменена компанией ООО «Телсофт» без предварительного уведомления.

Упомянутые торговые марки являются зарегистрированными торговыми марками их владельцев.

# Содержание

<b>1. Введение</b> .....	<b>6</b>
1.1. Назначение документа .....	6
1.2. Ограничения и допущения .....	6
1.3. Сопутствующая документация .....	6
1.4. Используемые обозначения .....	7
1.5. История изменений документа .....	8
<b>2. Общее описание IMS</b> .....	<b>9</b>
<b>3. Архитектура IMS Core</b> .....	<b>11</b>
3.1. Call Session Control Function .....	12
3.2. P-CSCF .....	13
3.2.1. Общие сведения .....	13
3.2.2. Защита конфиденциальности SIP сигнализации .....	13
3.2.3. Функции обеспечения безопасности .....	13
3.2.4. Манипулирование заголовками и содержимым SIP-сообщений .....	14
3.2.5. Функциональность IMS ALG .....	15
3.2.6. Обнаружение экстренного вызова .....	15
3.2.7. Согласование параметров транскодирования медиа потоков .....	15
3.2.8. Компрессия SIP сигнализации .....	15
3.2.9. Характеристики P-CSCF .....	16
3.2.10. Функции тарификации .....	17
3.3. I-CSCF .....	18
3.3.1. Общие сведения .....	18
3.3.2. Характеристики I-CSCF .....	18
3.3.3. Функции тарификации .....	19
3.4. S-CSCF .....	20
3.4.1. Общие сведения .....	20
3.4.2. Процедура регистрации UE .....	20
3.4.3. Хранение профиля пользователя .....	20
3.4.4. Маршрутизация SIP сессии .....	20
3.4.5. Преобразование MSISDN (Tel URI) – SIP URI .....	21
3.4.6. Характеристики S-CSCF .....	21
3.4.7. Функции тарификации .....	22
3.5. E-CSCF .....	<b>Error! Bookmark not defined.</b>
3.5.1. Общие сведения .....	<b>Error! Bookmark not defined.</b>
3.5.2. Характеристики E-CSCF .....	<b>Error! Bookmark not defined.</b>
3.5.3. Функции тарификации .....	<b>Error! Bookmark not defined.</b>

3.6. SCC-AS .....	Error! Bookmark not defined.
3.6.1. Общие сведения .....	Error! Bookmark not defined.
3.6.2. Характеристики SCC-AS .....	Error! Bookmark not defined.
3.6.3. Функции тарификации.....	Error! Bookmark not defined.
3.7. MRFC и MRFP .....	Error! Bookmark not defined.
3.7.1. Общие сведения .....	Error! Bookmark not defined.
3.8. BGCF, MGCF .....	23
3.8.1. Общие сведения .....	23
3.8.2. Характеристики BGCF .....	23
3.8.3. Функции тарификации.....	24
3.9. IP-SM-GW .....	Error! Bookmark not defined.
3.9.1. Общие сведения .....	Error! Bookmark not defined.
3.10. DNS/ENUM .....	25
3.10.1. Общие сведения .....	25
3.11. Функции тарификации .....	26
3.11.1. Offline тарификация.....	26
3.11.2. Online тарификация .....	26
3.12. HSS.....	Error! Bookmark not defined.
3.12.1. Общие сведения .....	Error! Bookmark not defined.
3.13. MMTel-AS.....	Error! Bookmark not defined.
3.13.1. Общие сведения .....	Error! Bookmark not defined.
3.14. IBCF, TrGW .....	28
3.14.1. Общие сведения .....	28
<b>4. Функциональные возможности.....</b>	<b>29</b>
4.1. Масштабирование .....	30
4.1.1. Режимы масштабирования различных подсистем .....	31
4.2. Отказоустойчивость и глобальное резервирование .....	33
4.2.1. Резервирование подсистем .....	33
4.3. Мониторинг и обслуживание.....	36
4.4. Подсистема мониторинга и сбора SIP трейсов .....	38
4.4.1. Prometheus.....	39
4.4.2. SNMP notifier .....	40
4.4.3. Grafana.....	40
4.4.4. Homer-APP – SIP Trace System .....	41
4.4.5. Основные функции компонентов Homer.....	42
4.4.6. NEPlify .....	42
4.4.7. NEpipe .....	42
4.5. Ролевая модель доступа .....	43

<b>5. Провижининг IMS сервисов .....</b>	<b>45</b>
<b>6. Исполнение приложений .....</b>	<b>46</b>
<b>7. Услуги связи .....</b>	<b>49</b>
7.1. Мультимедийные телефонные услуги – MMTEL .....	49
7.1.1. Голосовая связь (speech).....	50
7.1.2. Видео связь (video) .....	51
7.1.3. Текстовая связь (text) .....	51
7.1.4. Передача факсимильных сообщений (fax) .....	51
7.1.5. Прочие MMTEL сервисы .....	51
7.2. Дополнительные услуги (Supplementary Services).....	52
7.2.1. Идентификация вызывающего пользователя (OIP).....	54
7.2.2. Запрет идентификации вызывающего пользователя (OIR).....	55
7.2.3. Идентификация вызываемого пользователя (TIP) .....	56
7.2.4. Запрет идентификации вызываемого пользователя (TIR).....	56
7.2.5. Переадресация сессий/вызовов (CDIV) .....	57
7.2.6. Удержание сессии/вызова (CH) .....	58
7.2.7. Блокировка сессий/вызовов (CB).....	58
7.2.8. Конференция (CONF) .....	59
7.2.9. Индикатор ожидания сообщения (MWI) .....	60
7.2.10. Ожидание сессии/вызова (CW) .....	61
7.2.11. Передача связи (ECT).....	62
<b>8. Интеграция с системой E-TAS .....</b>	<b>63</b>
<b>9. Перечень стандартов.....</b>	<b>65</b>
9.1. Серия RFC.....	65
9.2. Серия GSMA.....	68
9.3. Серия 3GPP .....	69
<b>10. Глоссарий .....</b>	<b>72</b>

# 1. Введение

---

## 1.1. Назначение документа

Настоящий документ представляет собой руководство по эксплуатации системы IMS Core.

Данный документ содержит следующие аспекты:

- Общее описание IMS.
- Описание архитектуры решения.
- Описание возможностей системы.
- Описание услуг связи.

---

## 1.2. Ограничения и допущения

---

## 1.3. Сопутствующая документация

## 1.4. Используемые обозначения

Таблица 1. Используемые обозначения

Обозначение	Описание
Полужирное начертание	Функциональные элементы (экранные кнопки, название окон и т. д.)
<i>Курсив</i>	Перекрестные ссылки, ссылки на другие документы
<b>ЗАГЛАВНЫЕ БУКВЫ</b>	Название клавиш клавиатуры
<b>Шрифт Courier New</b>	Код
 <b>Примечание</b>	Пояснение к тексту

---

## 1.5. История изменений документа

Таблица 2. История изменений

Версия	Дата	Содержание изменений
1.0	01.10.2021	Документ создан

## 2. Общее описание IMS

IMS (IP Multimedia Subsystem) – спецификация передачи мультимедийного содержимого в сетях электросвязи на основе протокола IP.

Концепция IMS состоит в том, что доставка любой услуги никак не соотносится с коммуникационной инфраструктурой (за исключением ограничений по пропускной способности). Воплощением этого принципа является многоуровневый подход, используемый при построении IMS. Он позволяет реализовать независимый от технологии доступа открытый механизм доставки услуг, который дает возможность задействовать в сети приложения сторонних поставщиков услуг.

В Табл. 3 приведен перечень основных интерфейсов (референсных точек) подсистемы IMS.

Таблица 3. Интерфейсы IMS

Наименование	Объекты	Протокол
Bi	CCF – Billing System	Diameter
Bx	CGF – Billing System	ftp
Cx	HSS – S-CSCF/I-CSCF	Diameter
Dh	SLF – AS	Diameter
Dx	SLF – S-CSCF/I-CSCF	Diameter
Ga	CDF – CGF	Diameter
Gm	UE – P-CSCF	SIP
Ici	IBCF – IBCF	SIP
ISC	S-CSCF – AS	SIP
Ix	IBCF – TrGW	H.248
Izi	TrGW – TrGW	IMS user plane
Ma	I-CSCF – AS	SIP
Mb	P-GW – IMS-AGW / MRFP / IM-MGW / TrGW	IMS user plane
Mg	I-CSCF – MGCF	SIP
Mi	S-CSCF – BGCF	SIP
Mj	BGCF – MGCF	SIP

Наименование	Объекты	Протокол
Mk	BGCF – BGCF	SIP
Mm	IBCF/CSCF/BGCF/IMS ALG – IP multimedia network	SIP
Mn	MGCF – IM-MGW	H.248
Mp	MRFC – MRFP	H.248
Mr	S-CSCF – MRFC	SIP
Mw	CSCF – CSCF	SIP
Mx	CSCF/BGCF – IBCF	SIP
Rf	Interface to CDF	Diameter
Ro	Interface to OCS	Diameter
Sh	HSS – AS	Diameter
Si	IM-SSF – HSS	MAP
Ut	UE – AS	XCAP

### 3. Архитектура IMS Core

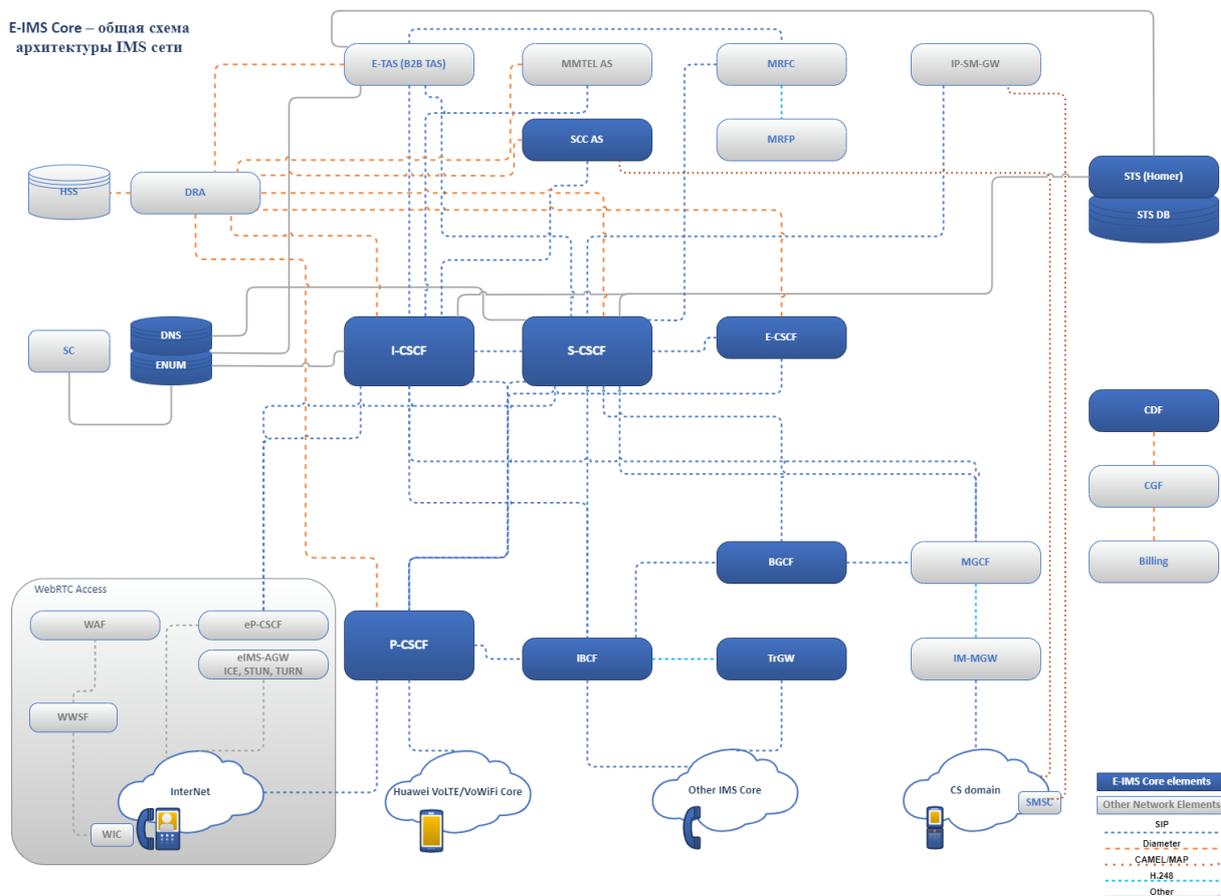


Рис. 1. Архитектура сети IMS

На рисунке 1 представлена общая архитектура системы. К базовым элементам архитектуры сети IMS Core относятся функции, описанные далее.

---

## 3.1. Call Session Control Function

Call Session Control Function (CSCF) – функция управления сеансом связи и маршрутизацией.

Типы CSCF:

- прокси CSCF (proxy CSCF – P-CSCF);
- обслуживающий CSCF (serving CSCF – S-CSCF);
- запрашивающий CSCF (interrogating CSCF – I-CSCF);
- CSCF экстренных служб (emergency CSCF – E-CSCF).

Каждый тип CSCF выполняет свои специализированные задачи, но все они могут:

- генерировать тарификационные данные (CDR);
- направлять тарификационные данные в функции offline тарификации.

Общая роль CSCF:

- участие в процессах регистрации абонентского терминала в сети;
- установление сессии;
- обеспечение механизма SIP маршрутизации.

---

## 3.2. P-CSCF

### 3.2.1. Общие сведения

P-CSCF (Proxy Call Session Control Function) – это функция, которая создает первую контактную точку входа пользователей в IMS Core.

Абонентский терминал (UE) направляет на P-CSCF весь сигнальный IMS трафик. И генерируемый сетью сигнальный трафик в направлении к UE тоже посылается через P-CSCF.

Типовые задачи, выполняемые P-CSCF:

- Защита конфиденциальности SIP сигнализации.
- Межсетевое взаимодействие (IPv4 и IPv6, включая NAT)
- Обеспечение безопасности.
- Манипулирование заголовками и содержимым SIP-сообщений.
- Взаимодействие с PCRF.
- Функциональность IMS ALG.
- Обнаружение экстренного вызова.
- Согласование параметров транскодирования медиа потоков.
- Компрессия SIP сигнализации.
- Обработка DSCP QoS меток.
- Генерация CDR.

---

### 3.2.2. Защита конфиденциальности SIP сигнализации

В задачи P-CSCF входит защита конфиденциальности SIP сигнализации и RTP-потоков данных средствами шифрования.

Так, в частности, в системе поддерживаются следующие основные виды защищённых соединений:

- Передача сигнализации SIP через TLS (TLSv1, SSLv2, SSLv3)
- Передача сигнализации SIP через IPSec (IPv4, IPv6).
- Передача медиа потоков через SRTP
- Организация меж сетевого взаимодействия и преобразование между протоколами SIP TLS – SIP и SRTP – RTP.

Перечень наборов шифрования данных, поддерживаемых P-CSCF для передачи SIP сигнализации (SIP RTP) и медиа потоков (SRTP), представлен в документе *IMS Core. Шифрование данных. Версия 1.0*

---

### 3.2.3. Функции обеспечения безопасности

Ключевой задачей элемента P-CSCF, обеспечивающего взаимодействие внешней (untrusted) сети с внутренними элементами ядра IMS, является обеспечение безопасности.

В части данной функциональности можно выделить следующие ключевые аспекты:

- Скрытие топологии (Topology Hiding).
  - защита адресов шлюзов PSTN
  - защиты от несанкционированного доступа к внутренним элементам ядра IMS
  - защита адресных данных и скрытие топологии внутренней сети
  - скрытие адресов конечных точек RTP-медиапотока
- Межсетевые экраны (Firewalls)
  - временная блокировка IP-адресов (IP ban)
  - защита от Brute-force атак
  - защита от сканирования портов
  - защита от наиболее распространённых форм атак типа отказ в обслуживании (Dos/DdoS): SYN-flooding, ping flooding, UDP flooding, fragmentation bombs
- Фильтрация и регулирование сигнального трафика
  - Регулирование входящего и исходящего потоков SIP-сообщений (перегрузки при регистрации, SIP-flooding, session agent constraints, rate constraints)
  - Фильтрация некорректных SIP-сообщений (формальная верификация)
  - Фильтрация вредоносных SIP-сообщений (SIP Spoofing)

Более детальная информация представлена в приложении *IMS Core. Функции обеспечения безопасности. Версия 1.0*

---

### 3.2.4. Манипулирование заголовками и содержимым SIP-сообщений

Наряду с другими элементами ядра P-CSCF выполняет важные функции по верификации SIP-сообщений и модификации их содержимого.

В частности, выполняются следующие ключевые действия:

- нормализация сообщений
- модификация и шифрование данных заголовков, относящихся к топологии внутренней защищённой сети
- удаление служебных, избыточных и неинформативных частей заголовков

Более детальная информация о встроенном механизме манипулирования содержимым SIP-сообщений, в частности, заголовками (Headers), телом (Body) и стартовой строкой (Start-Line) или строкой запроса (Request-Line)

---

### 3.2.5. Функциональность IMS ALG

В архитектуре IMS имеется логический элемент ALG (Application Level Gateway), отвечающий за выполнение следующих функций:

- управление NAT
- обеспечение безопасного взаимодействия между доменами на уровне сигнализации (SIP/SDP)
- обеспечение взаимодействия между различными приложениями на основе IPv4 и IPv6

В текущей реализации системы эти функции встроены в элемент P-CSCF.

---

### 3.2.6. Обнаружение экстренного вызова

P-CSCF является элементом ядра IMS, который отвечает за обнаружение запроса на экстренный сеанс, когда UE, использующее трафик общедоступной сети, инициирует экстренный сеанс. Затем P-CSCF пересылает запрос E-CSCF в той же сети, если процедуры аутентификации и безопасности не требуют запроса для пересылки на S-CSCF в той же сети.

---

### 3.2.7. Согласование параметров транскодирования медиа потоков

P-CSCF наряду с S-CSCF осуществляет анализ SIP сообщения, содержащего данные SDP с параметрами поддерживаемых кодеков, выполняя функцию посредника в процессе переговоров о возможностях обмена медиа данными и определения необходимости транскодирования.

---

### 3.2.8. Компрессия SIP сигнализации

Возможность сжатия SIP-сообщений крайне важна для IMS, особенно в условиях ограниченной полосы пропускания и необходимости снижения объема сетевого трафика.

На этапе регистрации пользовательское оборудование (UE) и P-CSCF объявляют о своей готовности выполнить компрессию, предоставляя подробные сведения о своих возможностях сжатия, таких как объем памяти, вычислительная мощность, состояния загрузки и инструкции по сжатию.

---

## 3.2.9. Характеристики P-CSCF

### *Поддерживаемые интерфейсы IMS*

Элемент системы P-CSCF поддерживает следующие интерфейсы IMS:

- Gm
- Mg
- Mw
- Rf
- Rx

### *Поддерживаемые методы SIP-сообщений*

Элемент системы P-CSCF поддерживает следующие методы SIP-сообщений:

- ACK
- BYE
- CANCEL
- INFO
- INVITE
- MESSAGE
- NOTIFY
- OPTIONS
- PRACK
- PUBLISH
- REFER
- REGISTER
- SUBSCRIBE
- UPDATE

### *Поддерживаемые медиа кодеки*

Элемент системы P-CSCF поддерживает следующие медиа кодеки:

- AMR-NB
- AMR-WB
- EVS
- G.711 a-Law
- G.711 u-Law
- G.722
- G.723.1
- G.729
- iLBC
- Opus
- Speex
- T.38

---

### 3.2.10. Функции тарификации

В ходе обработки SIP-сессий элемент P-CSCF:

- формирует соответствующие файлы CDR
- осуществляет передачу файлов CDR в элемент CDF по интерфейсу Rf
- подтверждает факт успешной передачи файлов CDR в элемент CDF
- при необходимости осуществляет повторную передачу файлов CDR в элемент CDF по интерфейсу Rf

---

## 3.3. I-CSCF

### 3.3.1. Общие сведения

I-CSCF (Interrogating Call Session Control Function) – это функция, которая создает первую контактную точку в сети оператора для всех внешних соединений с абонентами данной сети.

I-CSCF назначает S-CSCF, основываясь на данных, полученных из HSS. Например, назначение S-CSCF происходит:

- при регистрации пользователя;
- когда незарегистрированный пользователь получает SIP request к сервису, относящемуся к незарегистрированному состоянию OoB.

---

### 3.3.2. Характеристики I-CSCF

#### *Поддерживаемые интерфейсы IMS*

Элемент системы I-CSCF поддерживает следующие интерфейсы IMS:

- Cx
- ENUM/DNS
- ISC
- Ma
- Mg
- Mw
- Mx
- Rf

#### *Поддерживаемые методы SIP-сообщений*

Элемент системы I-CSCF поддерживает следующие методы SIP-сообщений:

- ACK
- BYE
- CANCEL
- INFO
- INVITE
- MESSAGE
- NOTIFY
- OPTIONS
- PRACK
- PUBLISH
- REFER
- REGISTER
- SUBSCRIBE
- UPDATE

### *Поддерживаемые заголовки SIP-сообщений*

Элемент системы I-CSCF поддерживает следующие типовые заголовки SIP-сообщений и обеспечивает их обработку согласно 3GPP TS 24.229 и соответствующим IETF RFC:

- P-Asserted-Identity
- P-Called-Party-ID
- P-Charging-Function-Addresses
- P-Charging-Vector
- P-Visited-Network-ID
- P-Associated-URI
- History-Info
- P-Access-Network-Info
- P-Served-User
- P-Answer-State
- P-Early-Media
- P-Media-Authorisation
- P-Preferred-Identity

---

### **3.3.3. Функции тарификации**

В ходе обработки SIP-сессий элемент I-CSCF:

- формирует соответствующие файлы CDR
- осуществляет передачу файлов CDR в элемент CDF по интерфейсу Rf
- подтверждает факт успешной передачи файлов CDR в элемент CDF
- при необходимости осуществляет повторную передачу файлов CDR в элемент CDF по интерфейсу Rf

---

## 3.4. S-CSCF

### 3.4.1. Общие сведения

S-CSCF (Serving Call Session Control Function) является центральной точкой IMS Core.

Элемент системы S-CSCF обеспечивает выполнение следующих основных функций:

- выполнение процедуры регистрации
- хранение профиля пользователя
- управление машиной состояний сессии
- принятие решения о маршрутизации

---

### 3.4.2. Процедура регистрации UE

S-CSCF обеспечивает регистрацию, перерегистрацию, инициированную сетью отмену регистрации UE согласно 3GPP 23.228 и 24.229.

Типовая процедура регистрации состоит в следующем:

- После отправки пользователем запроса на регистрацию происходит его маршрутизация к S-CSCF.
- При поступлении соответствующего запроса, S-CSCF выполняет ряд действий:
  - инициирует процедуру аутентификации
  - загружает профиль пользователя из HSS
  - подтверждает регистрацию, получив и верифицировав данные или отклоняет регистрацию в противном случае
- После успешного завершения регистрации пользователь может генерировать и принимать IMS запросы.

---

### 3.4.3. Хранение профиля пользователя

Элемент системы S-CSCF осуществляет загрузку и хранение профиля пользователя на период его активности.

Профиль пользователя загружается из HSS, доступ к которому производится через элемент DRA посредством интерфейса Sx.

---

### 3.4.4. Маршрутизация SIP сессии

На основе информации из пользовательского профиля S-CSCF:

- решает, когда и какой AS подключать при получении от пользователя SIP запроса.

S-CSCF принимает запрос и решает вопрос о дальнейшей маршрутизации исходящей (UE-originated) или входящей (UE-terminated) сессии.

Например, при получении запроса исходящей сессии (UE-originated) S-CSCF:

- решает, требуется ли ему подключать AS перед дальнейшей маршрутизацией запроса;
- после взаимодействия с AS S-CSCF либо продолжит сессию в IMS домене, либо переправит ее в другой домен (CS или IMS другого оператора).

Аналогично S-CSCF принимает все запросы, которые будут терминироваться в UE.

После процедуры регистрации S-CSCF знает IP адрес UE и маршрутизирует все запросы только через P-CSCF, т.к. P-CSCF может применять политики безопасности доступа.

---

### 3.4.5. Преобразование MSISDN (Tel URI) – SIP URI

Если UE использует MSISDN (Tel URI) для адресации вызываемой стороны, то S-CSCF перед дальнейшей пересылкой преобразует MSISDN в SIP URI формат, поскольку IMS Core не маршрутизирует запросы, основываясь на MSISDN номерах.

С этой целью может быть запрошена дополнительная информация из базы данных ENUM/DNS.

---

### 3.4.6. Характеристики S-CSCF

#### *Поддерживаемые интерфейсы IMS*

Элемент системы S-CSCF поддерживает следующие интерфейсы IMS:

- Cx
- ENUM/DNS
- ISC
- Mi
- Mg
- Mr
- Mw
- Mx
- Rf

### *Поддерживаемые методы SIP-сообщений*

Элемент системы S-CSCF поддерживает следующие методы SIP-сообщений:

- ACK
- BYE
- CANCEL
- INFO
- INVITE
- MESSAGE
- NOTIFY
- OPTIONS
- PRACK
- PUBLISH
- REFER
- REGISTER
- SUBSCRIBE
- UPDATE

### *Поддерживаемые заголовки SIP-сообщений*

Элемент системы S-CSCF поддерживает следующие типовые заголовки SIP-сообщений и обеспечивает их обработку согласно 3GPP TS 24.229 и соответствующим IETF RFC:

- P-Asserted-Identity
- P-Called-Party-ID
- P-Charging-Function-Addresses
- P-Charging-Vector
- P-Visited-Network-ID
- P-Associated-URI
- History-Info
- P-Access-Network-Info
- P-Served-User
- P-Answer-State
- P-Early-Media
- P-Media-Authorisation
- P-Preferred-Identity
- P-Preferred-Service

---

## **3.4.7. Функции тарификации**

В ходе обработки SIP-сессий элемент S-CSCF:

- формирует соответствующие файлы CDR
- осуществляет передачу файлов CDR в элемент CDF по интерфейсу Rf
- подтверждает факт успешной передачи файлов CDR в элемент CDF
- при необходимости осуществляет повторную передачу файлов CDR в элемент CDF по интерфейсу Rf

---

## 3.5. BGCF

### 3.5.1. Общие сведения

BGCF – один из ключевых элементов системы, обеспечивающий взаимодействие ядра IMS и домена с коммутацией каналов (CS). Элемент MGCF не входит в стандартную поставку ядра IMS.

Чтобы направить вызов в домен с коммутацией каналов (CS домен):

- S-CSCF пересылает SIP запрос к BGCF, который осуществляет выбор соответствующего CS домена.
- BGCF направляет SIP запрос в MGCF, что позволяет маршрутизировать сигнальный и медиа поток по сети IMS Core максимально близко к вызываемому абоненту.
- Когда SIP запрос достигает MGCF, он выполняет преобразование протоколов:
  - SIP протокол с одной стороны;
  - ISDN user part – ISUP с другой.

Потом посылает конвертированное сообщение в SGW CS домена.

- SGW выполняет двухстороннее преобразование транспортного уровня сигнализации:
  - SIGTRAN IP/SCTP/MxUA с одной стороны;
  - SS7 MTP – с другой.

---

### 3.5.2. Характеристики BGCF

#### *Поддерживаемые интерфейсы IMS*

Элемент системы BGCF поддерживает следующие интерфейсы IMS:

- Mi
- Mj
- Mx
- Rf

### *Поддерживаемые методы SIP-сообщений*

Элемент системы BGCF поддерживает следующие методы SIP-сообщений:

- ACK
- BYE
- CANCEL
- INFO
- INVITE
- MESSAGE
- NOTIFY
- OPTIONS
- PRACK
- PUBLISH
- REFER
- REGISTER
- SUBSCRIBE
- UPDATE

---

### **3.5.3. Функции тарификации**

В ходе обработки SIP-сессий элемент BGCF:

- формирует соответствующие файлы CDR
- осуществляет передачу файлов CDR в элемент CDF по интерфейсу Rf
- подтверждает факт успешной передачи файлов CDR в элемент CDF
- при необходимости осуществляет повторную передачу файлов CDR в элемент CDF по интерфейсу Rf

---

## 3.6. DNS/ENUM

### 3.6.1. Общие сведения

#### *DNS*

DNS – это распределённая система для получения информации о доменах, стандартизированная RFC 1034 и RFC 1035.

В рамках архитектуры IMS с помощью DNS осуществляется балансировка запросов к различным элементам и узлам.

Таким образом, DNS играет важную роль в механизме обеспечения отказоустойчивости и резервирования элементов системы.

#### *ENUM*

ENUM – это система (база данных) для сопоставления телефонных номеров, стандартизированная RFC2916 и RFC6116.

ENUM объединяет международную систему телефонных номеров с пространствами имен интернет-адресации (хосты DNS из специального пространства имен e164.агра).

Каждый телефонный номер может быть представлен стандартом E.164 с разрешимым именем хоста DNS.

ENUM базируется на протоколе DNS и позволяет определять по номеру в формате E.164:

- IP домен абонента (информация для маршрутизации)
- Перечень услуг абонента

К категориям услуг абонентов могут быть отнесены следующие:

- Voice
- Video
- IM
- MMS
- Text

ENUM характеризуется следующими особенностями:

- Независимость от типа сетей доступа.
- Возможность осуществления запроса в смежные DNS/ENUM.

---

## 3.7. Функции тарификации

Функции тарификации различных модулей IMS позволяют собрать необходимую для тарификации информацию из SIP запроса.

Виды тарификации:

- online тарификация (когда функция тарификации запрашивает разрешение у биллинговой системы на обработку SIP запроса);
- offline тарификация (когда функция тарификации позволяет обработку SIP запроса, отправляя собранную тарификационную информацию в биллинговую систему для формирования CDR записей).

Схемы тарификации различных сервисов зависят от:

- конфигурации IMS Core;
- срабатывания тех или иных триггеров.

Триггерами могут быть:

- запросы создания, модификации и терминции сессии (sessionbased charging);
- любая SIP транзакция, например, MESSAGE, PUBLISH, SUBSCRIBE (eventbased charging);
- определенные SIP заголовки и SDP информация.

---

### 3.7.1. Offline тарификация

С offline модулем тарификации (offline charging entity – CDF) могут взаимодействовать функции тарификации:

- всех IMS модулей;
- модулей доступа (при этом используется diameter-based Rf интерфейс 3GPP TS 32.299).

На основе информации, полученной из функциональных блоков тарификации всех IMS модулей:

- CDF создает CDR записи;
- CDR записи переправляются в шлюз тарификации (charging gateway function – CGF) через Ga интерфейс (3GPP TS 32.295);
- CGF обрабатывает полученные CDR;
- CGF переправляет полученные CDR в биллинговую систему, используя Vx интерфейс (3GPP TS 32.240).

---

### 3.7.2. Online тарификация

Online тарификация необходима Prepaid сервисам. IMS Core запрашивает перед авторизацией пользователя OCS на использование того или иного сервиса.

OCS отвечает за:

- контроль в реальном времени счета пользователя;
- авторизацию пользователя на использование сервиса;
- списание баланса со счета пользователя за полученные услуги.

С OCS могут взаимодействовать:

- модули ядра IMS, использующие интерфейс Ro:
  - S-CSCF
  - AS
  - MRFC
- прочие модули, не относящиеся к IMS (используя CAMEL application part – CAP).

OCS может создавать CDR записи подобно CGF в дополнение к credit control (тарификация в on-line).

---

## 3.8. IBCF, TrGW

### 3.8.1. Общие сведения

IBCF – элемент системы, обеспечивающий взаимодействие ядра IMS и других сторонних сетей IMS.

IBCF обеспечивает нормализацию SIP заголовков, сокрытие не нужных параметров и фильтрацию данных, не предназначенных для передачи в не доверенные зоны.

## 4. Функциональные возможности

IMS Core или мультимедийная IP-подсистема (IP Multimedia Subsystem) представляет собой архитектурную структуру для передачи мультимедийного содержимого в сетях электросвязи на основе протокола IP. При построении IMS Core используется многоуровневый подход, который позволяет:

- разделять уровни транспорта, управления и приложений;
- реализовать независимый от технологии доступа открытый механизм доставки услуг, который дает возможность задействовать в сети приложения сторонних поставщиков услуг.

Основные свойства архитектуры IMS Core:

- независимость от среды доступа – позволяет операторам и сервис-провайдерам объединять фиксированные и мобильные сети;
- поддержка мультимедийного персонального обмена информацией в реальном времени (голос, видео-телефония) и аналогового обмена информацией между людьми и компьютерами (например, игры);
- полная интеграция мультимедийных приложений реального и нереального времени (например, потоковые приложения и чаты);
- возможность взаимодействия различных видов услуг;
- возможность поддержки нескольких служб в одном сеансе или организации нескольких одновременных сеансов.
- IMS Core интегрирован с MGCF (PLMN, PSTN) и имеет встроенный UAG - P-CSCF (IP, PLMN). Для успешного прохождения вызовов и соблюдения правил обработки трафика IMS может маршрутизировать вызов на основе SIP-заголовков:
  - Request URI
  - From
  - To
  - P-Asserted-Identity
  - P-Served-User
  - P-Visited-Network-ID
  - P-Access-Network-Info
  - Contact
  - History-Info
  - Кастомных заголовков.
- IMS поддерживает текущие требования к IAD:
  - Поддержка P-HEADERS согласно RFC 3455/RFC 5009.
  - Поддержка PRACK (RFC 3262).
  - Поддержка «Multiple early dialogues» (RFC 5027/6228).
  - Поддержка Precondition, согласно RFC 3312.
  - Поддержка Info, согласно RFC 6086
  - ART (AlertRingingTone).
  - Alert-Info header.
- P-CSCF/SBC поддерживает интерфейс Gm в соответствии с 3GPP 24.229.

Платформа IMS Core ориентирована на реализацию коммуникационной инфраструктуры для мобильных операторов с поддержкой услуг связи.

## 4.1. Масштабирование

Масштабирование большинства элементов IMS Core производится горизонтальным образом.

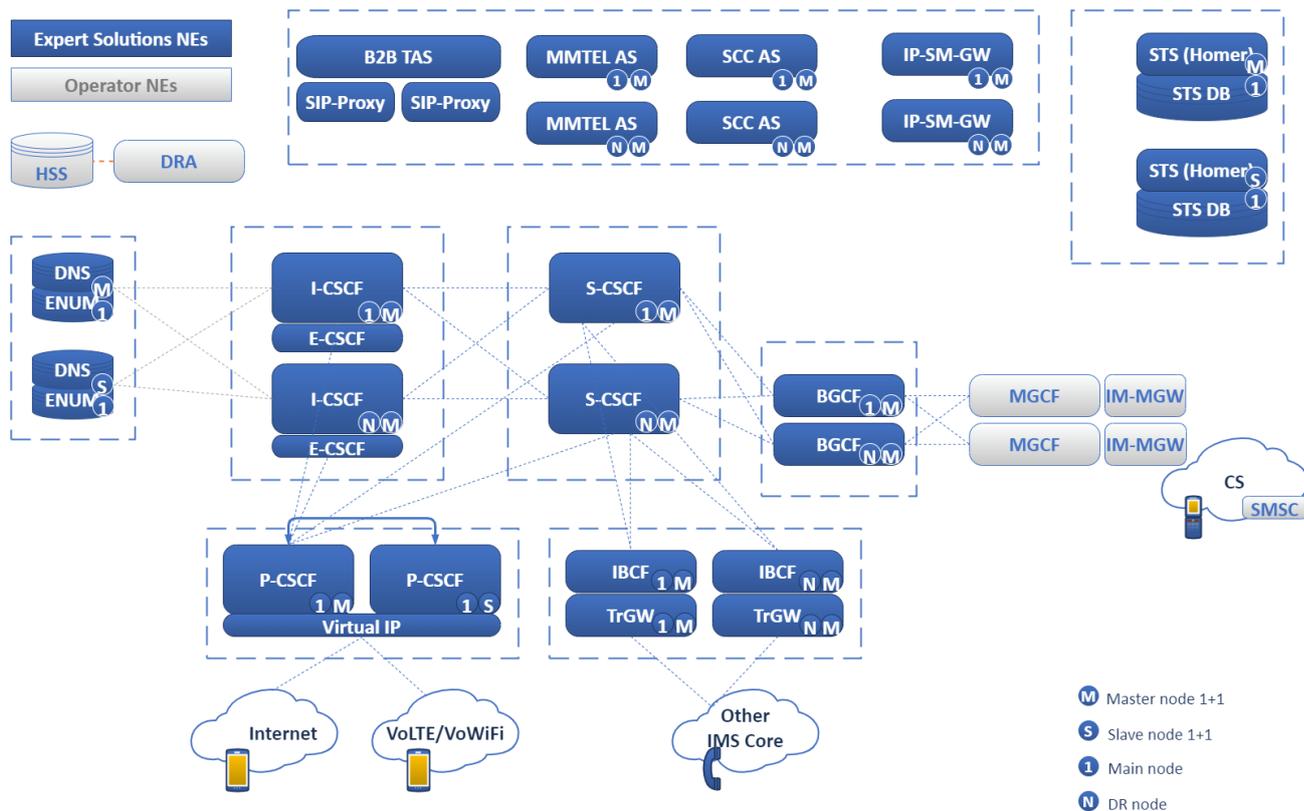


Рисунок 2: Архитектура масштабирования

Архитектура масштабирования представлена на Рисунок 2.

Все подсистемы и модули платформы взаимодействуют с внешним HSS через DRA.

Подразумевается два линка до DRA и дальнейшее масштабирование и резервирование HSS обеспечивается средствами Diameter Routing Agent.

Система E-TAS не использует механизмы балансировки IP трафика на уровнях L3-L7, как для обмена трафиком внутри системы, так и для связи с внешними системами.

---

## 4.1.1. Режимы масштабирования различных подсистем

### I-CSCF:

- Горизонтальное масштабирование, путем добавления новых копий.
- Работа в режиме Master-Master.

### S-CSCF:

- Горизонтальное масштабирование, путем добавления новых копий.
- Работа в режиме Master-Master.

### BGCF:

- Горизонтальное масштабирование, путем добавления новых копий.
- Работа в режиме Master-Master.

### IBCF:

- Горизонтальное масштабирование, путем добавления новых копий.
- Работа в режиме Master-Master.

### TrGW:

- Горизонтальное масштабирование, путем добавления новых копий.
- Работа в режиме Master-Master.

### DNS/ENUM:

- Работа в режиме Master-Slave, только один Master.
- Масштабирование путем добавления Slave копий.
- Все копии DNS могут равноценно обслуживать запросы.
- Возможна установка кэширующего сервера(ов), в случае экстремальных нагрузок на подсистему.

### SIP Trace System (STS):

- Вертикальное масштабирование, путем увеличения процессорной емкости и объема памяти сервера.
- Работа в режиме Master-Slave.
- Все трейсы принимает только активный сервер.
- База данных STS работает в режиме Master-Slave. Master – RW, Slave – RO.
- Общая БД позволяет бесшовно переключаться между серверами.

#### P-CSCF:

- Вертикальное масштабирование, путем увеличения процессорной емкости и объема памяти сервера.
- Работа в режиме Master-Slave.
- Регистрации и вызовы обслуживает Master.
- Между Master и Slave действует протокол DMQ, который позволяет иметь полную копию данных о регистрациях, вызовах, транзакциях и диалогах на обоих серверах. (подробнее ниже)
- Для корректной работы используется виртуальный IP, который поднимается на сетевом интерфейсе активного сервера (Master or Slave).
- P-CSCF (SBC) может иметь региональные выносы, для обеспечения коротких маршрутов прохождения трафика и распределения нагрузки.
- Для распределения нагрузки может использоваться механизм шардирования, когда разным группам абонентов выдают различные параметры подключения, тем самым снижая нагрузку на загруженный элемент.

## 4.2. Отказоустойчивость и глобальное резервирование

E-IMS Core спроектирована таким образом, что не имеет единой точки отказа. Все модули и функции системы задублированы.

Большинство модулей работают в режиме Master-Master, т.е. все развернутые копии ПО одновременно готовы обслуживать вызовы. Тем не менее, ряд систем работают в режиме Master-Slave, что обусловлено техническими ограничениями.

E-IMS Core может быть развернута на разных независимых площадках для обеспечения разделения нагрузки по разным географическим точкам с разными часовыми поясами и обеспечения отказоустойчивости.

Пример схемы гео-резервирования представлен на Рисунок 3

Е-IMS Core – схема распределения функций по виртуальным серверам IMS сети

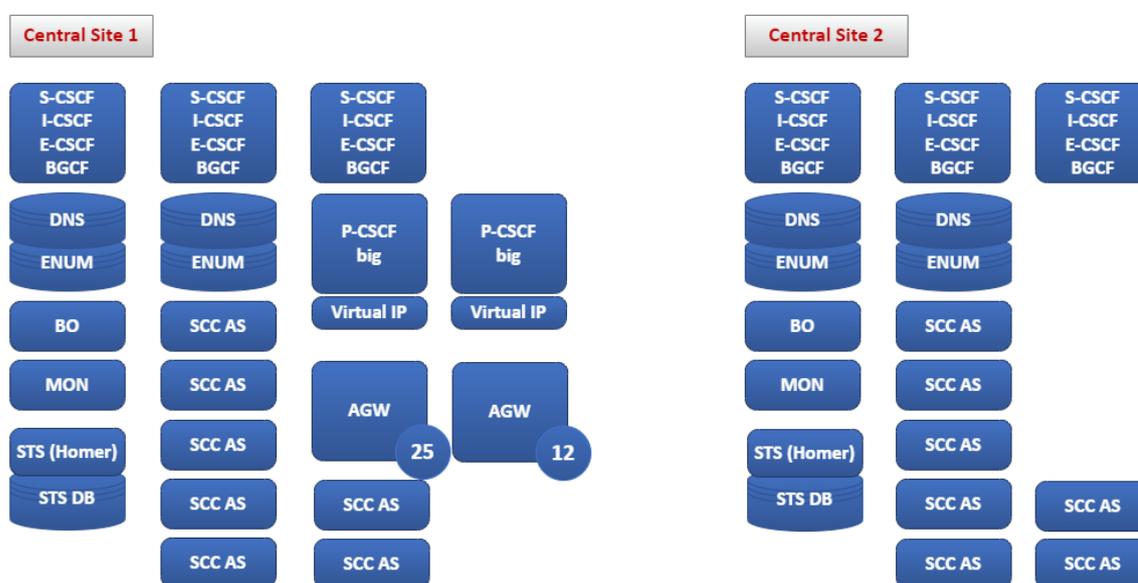


Рисунок 3: Гео-резервирование

### 4.2.1. Резервирование подсистем

Все подсистемы и модули платформы взаимодействуют с HSS через DRA.

Компоненты E-IMS Core подключены к Diameter Routing Agent используя два линка, через которые происходит резервирование и балансировка.

Для оценки доступности Diameter линка используются сообщения Diameter - DWR и DWA, которыми элементы обмениваются раз в X сек. Если линк несколько раз не ответил на запрос, то он помечается не активным. Если позже он стал отвечать на запросы, линк помечается активным.

Резервирование DRA и HSS выходит за рамки данного описания.

Отказоустойчивость DNS обеспечивается путем анализа доступности линков.

Отказоустойчивость протоколов основанных на SIP обеспечивается посылкой и приемом OPTIONS. На основании X не удачных ответов делается вывод о не доступности узла и он временно исключается из пула.

#### **I-CSCF:**

- Работа в режиме Master-Master.

#### **S-CSCF:**

- Работа в режиме Master-Master.

#### **BGCF:**

- Работа в режиме Master-Master.

#### **IBCF:**

- Работа в режиме Master-Master.

#### **TrGW:**

- Работа в режиме Master-Master.

#### **DNS/ENUM:**

- Работа в режиме Master-Slave, только один Master.
- Масштабирование путем добавления Slave копий.
- Все копии DNS могут равноценно обслуживать запросы.
- Возможна установка кэширующего сервера(ов), в случае экстремальных нагрузок на подсистему.
- DNS Master реплицирует данные в DNS Slave.

#### **SIP Trace System (STS):**

- Работа в режиме Master-Slave.
- Все трейсы принимает только активный сервер.
- База данных STS работает в режиме Master-Slave. Master – RW, Slave – RO.
- Общая БД и виртуальный IP, позволяет бесшовно переключаться между серверами.

#### **P-CSCF:**

- Работа в режиме Master-Slave.
- Регистрации и вызовы обслуживает Master.
- Между Master и Slave действует протокол DMQ, который позволяет иметь полную копию данных о регистрациях, вызовах, транзакциях и диалогах на обоих серверах. (подробнее ниже)
- Для корректной работы используется виртуальный IP, который поднимается на сетевом интерфейсе активного сервера (Master or Slave).
- P-CSCF (SBC) может иметь региональные выносы, для обеспечения коротких маршрутов прохождения трафика и распределения нагрузки.
- В случае выхода из строя Master, Slave продолжит обслуживание без влияния на вызовы, т.к. вся картина уже скопирована во внутреннюю структуру данных Slave.
- После восстановления, Master забирает работу на себя.

Протокол DMQ – это распределенная очередь сообщений на основе SIP протокола (RFC3261), обеспечивающая распространение и репликацию данных между серверами.

P-CSCF Master и Slave объединяются в единый канал репликации.

Протокол общения серверами между собой – SIP. Существует два режима отправки – точечный и мульти адресный (broadcast).

Данный протокол используется для передачи разных типов данных, таких как: глобальные переменные, данные о локации, регистрации, вызовах, диалогах, транзакциях, хеш таблиц.

Протокол DMQ обеспечивает определение состояния серверов, их доступность, перед отправкой данных, консистентность передаваемых данных, отсылку уведомлений, регистрацию в KDMQ кластере и безопасность передачи данных.

#### **Monitoring:**

- Работа в режиме Master-Slave.

#### **E- IMS Core Admin:**

- Работа в режиме Master-Slave.

#### **Admin-DB:**

- Работа в режиме Master-Slave.

## 4.3. Мониторинг и обслуживание

IMS Core предусматривает всесторонний съём метрик и счетчиков с компонентов платформы.

Метрики покрывают основные показатели комплекса, например:

Таблица 4. Метрики

Усредненная загрузка процессоров за период измерения.
Пиковая загрузка процессоров за период измерения.
Усредненная загрузка памяти за период измерения.
Среднее время занятия «канала».
Среднее время разговора.
Общий разговорный трафик.
Общий трафик занятия (фаза установления, ожидания ответа, разговор).
Общее количество вызовов (orig+term).
Общее количество orig вызовов.
Общее количество term вызовов.
Пиковое количество одновременных сессий (вызовов).
Среднее количество одновременных сессий за 15 минут (вызовов).
Среднее время установления orig соединения.
Среднее время установления term соединения.
Процент успешности установления вызовов по техническим причинам.
Успешность установления для исходящих вызовов.
Успешность установления для входящих вызовов.
Количество отказов при установлении исходящих голосовых вызовов.
Количество отказов при установлении входящих голосовых вызовов.
Процент отвеченных вызовов.
Процент успешных вызовов.

Процент успешности orig вызовов.
Процент успешности term вызовов.

Выгрузка метрик может осуществляться во внешнюю систему, например, Globus или др., через sftp/https/nfs.

Обычно используется sftp + csv формат.

Для целей оперативного мониторинга состояния системы используется проверенное решение Prometheus + AlertManager + Grafana. Система генерирует алармы, которые могут быть выгружены в системы мониторинга заказчика, например, NetCool (SNMP or CSV). Кастомизация алармов производится по согласованию с Заказчиком.

Мониторинг доступен в Grafana, несколько дашбордов эффективно показывают общую картину происходящего, текущие нагрузки, пиковые значения, параметры работы серверов и другие показатели.

Администрирование платформы осуществляется через специальный web интерфейс, позволяющий управлять всеми элементами, производить их вывод из работы, обслуживание, смену конфигов и скриптов и обратный ввод в работу. Часть настроек доступно исключительно через CLI, linux based команды.

Развертывание ПО производится с помощью автоматизированных сценариев.

Процедура автоматизированных бэкапов позволяет с заданной периодичностью, обычно раз в сутки, сохранять все важные параметры конфигураций в структуре папок, архивировать их и пересылать на внешний sftp сервер.

## 4.4. Подсистема мониторинга и сбора SIP трейсов

В данной главе рассмотрены следующие модули подсистемы мониторинга:

- Prometheus.
- SNMP notifier.
- Grafana.
- Homer-APP. (STS – SIP Trace System)
- HEPlify. (STS)
- HEpipe. (STS)

Архитектура подсистемы мониторинга представлена на Рисунок 4.

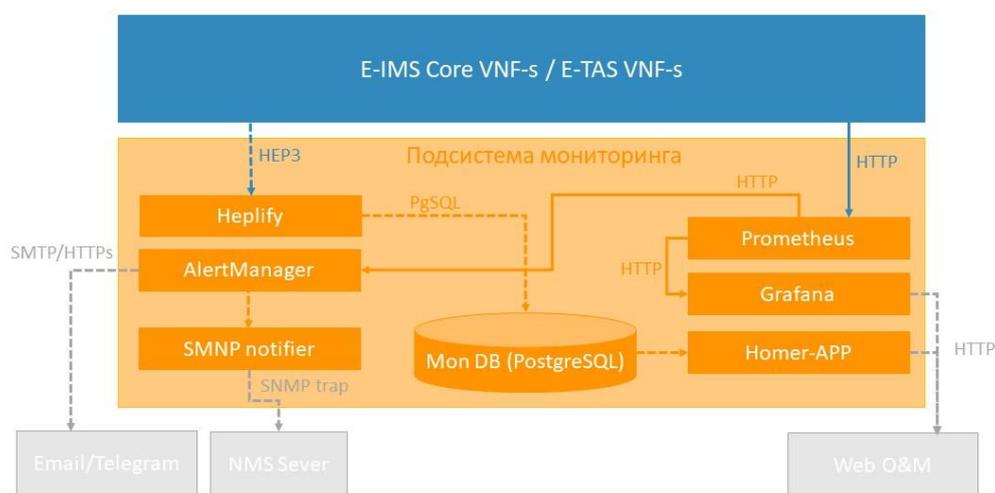


Рисунок 4: Архитектура подсистема мониторинга

## 4.4.1. Prometheus

Prometheus — система мониторинга различных систем и микросервисов, которая с заданным интервалом времени опрашивает все целевые объекты для получения их метрик.

Для сбора метрик на целевые объекты (SIP Proxy, AS, Database) устанавливаются экспортеры, данные от которых передаются на сервер и хранятся в базе данных. Сервер Prometheus периодически опрашивает экспортеры и в случае их недоступности формирует сообщения об ошибках.

Протокол: http, формат данных: JSON, язык формирования запросов: PromQL (Prometheus Query Language).

Архитектура Prometheus представлена на Рисунок 5.

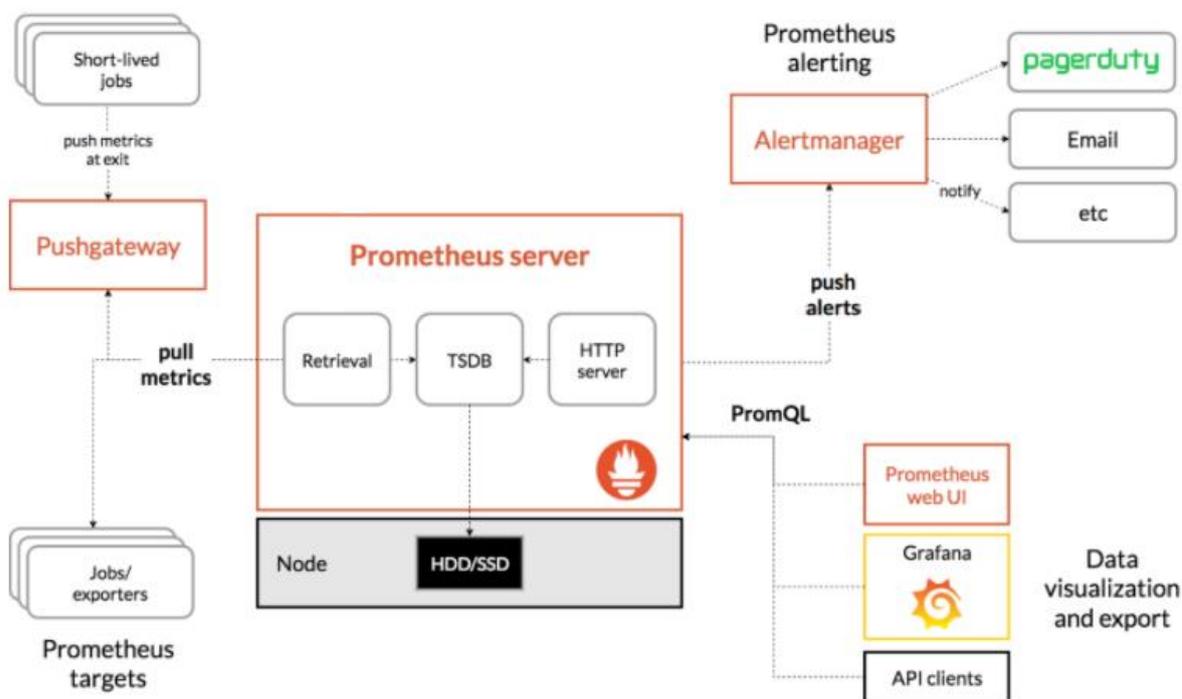


Рисунок 5: Архитектура Prometheus

Prometheus хранит данные в виде временных рядов — наборов значений, соотнесённых с временной меткой (timestamp). Элемент временного ряда (измерение) состоит из имени метрики, временной метки и пары «ключ — значение». Временные метки имеют точность до миллисекунд, значения представлены с 64-битной точностью.

С помощью Grafana можно визуализировать полученные данные в виде наглядных графиков, диаграмм и таблиц.

Для рассылки оповещений используется Alertmanager. Настройки уведомлений задаются в конфигурационном файле, в котором можно добавить ссылки на файлы правил. В правилах прописываются условия, при

которых нужно отправлять уведомления. Отправка уведомлений осуществляется по электронной почте, через веб-хук, HipChat или Telegram.

---

#### 4.4.2. **SNMP notifier**

SNMP notifier является проксирующим модулем между Alertmanager и внешними системами и отвечает за отправку snmp trap.

SNMP trap UID задаются в соответствии с корпоративной структурой UID и для TAS имеют префикс: .1.3.6.1.4.1.19792.30.1.

---

Список сообщений об ошибках и их UID представлены в отдельном файле.

---

---

#### 4.4.3. **Grafana**

Grafana — это платформа для визуализации, мониторинга и анализа данных. Использует метрики Prometheus, и отображает их в виде информативных графиков и диаграмм, организованных в настраиваемые панели.

Grafana позволяет создавать различные dashboard для отображения разных срезов данных, группировать и агрегировать данные по различным параметрам.

Grafana имеет собственный WEB интерфейс, хранит данные пользователей с различными правами доступа.

---

#### 4.4.4. Homer-APP – SIP Trace System

Homer – это решение, предназначенное для захвата, анализа и мониторинга SIP трафика с широкими возможностями масштабирования способное «перемалывать» огромные объёмы трафика свойственные VoIP-операторам малого или среднего размера.

Эта система призвана облегчить инженерам поиск и устранение неисправностей в VoIP-сетях при помощи мощного анализа и визуализации SIP-диалогов между узлами и детальный просмотр всех SIP-сообщений. Решение позволяет сохранять выгружать SIP-трейсы вызовов в виде pcap дампов или текстовых файлов. Еще одним преимуществом решения является возможность разнесения компонентов системы по разным узлам, что позволяет масштабировать систему.

Решение Homer состоит из нескольких подсистем. Рассмотрим эти подсистемы и механизм их взаимодействия между собой.

В составе Homer можно выделить три основные подсистемы:

- HOMER CAPTURE AGENT – агент захватывает трафик из VoIP-сети, копирует и инкапсулирует SIP и RTCP пакеты при помощи протокола NER/EPP и передаёт их на CAPTURE SERVER, причём агент может представлять из себя как модуль для SIP-сервера, так и сервис захвата «сырого» трафика с сетевого интерфейса, который может зеркалироваться с порта(-ов) ethernet-коммутатора куда подключен SIP-сервер (например, модуль транзита трафика РТУ МТТ) на порт(-ы) CAPTURE AGENT.
- HOMER CAPTURE SERVER – сервер, где аккумулируется и хранятся SIP и RTCP пакеты, полученные от CAPTURE AGENT
- HOMER USER INTERFACE – веб-интерфейс для поиска, анализа и визуализации SIP-трейсов которые хранятся в CAPTURE SERVER.

Итак, общая схема работы Homer выглядит так:

CAPTURE AGENT — это системная служба, которая постоянно запущена на узле. Через узел проходит VoIP-трафик, требующий анализа. CAPTURE AGENT захватывает трафик и создает копии сигнальных SIP-сообщений, затем инкапсулирует эти копии пакетов в формат NER/ EEP и передаёт их по сети в коллектор сервера CAPTURE SERVER, сервер получает SIP и RTCP пакеты, разбирает их и помещает в базу данных PostgreSQL. Фактически все SIP-сообщения целиком хранятся в базе данных, но естественно не просто так, а с метаданными, которые и позволяют существенно ускорить поиск и отображение запрашиваемой из веб-интерфейса информации.

Веб-интерфейс USER INTERFACE подключается к базе данных CAPTURE SERVER и загружает данные, запрашиваемые пользователем веб-интерфейса.

---

## 4.4.5. Основные функции компонентов Homer

### Capture Server

- Высокая производительность – тысячи пакетов в секунду.
- Поддержка нескольких баз данных.
- Мощный пользовательский интерфейс для поиска и фильтрации.
- Визуальные диалоги SIP и возможность их выгрузки в pcap-файлы.
- Графики со статистикой и аналитикой.
- Поддержка REST API и виджетов.
- Авторизация пользователей по RADIUS и LDAP.
- Angular/JS интерфейс пользователя.

Capture Server это два отдельных компонента на выбор: HEPlify-Server — написанный на GO, высокопроизводительный сервер, готовый для обработки NEP пакетов от любого NEP агента и NEPop — написанный на NodeJS больше подходящий для обработки потоковых данных.

### Capture Agent

- NEP3 инкапсуляция.
- Шифрование и сжатие содержимого.
- Модульный дизайн.
- SIP, RTP/RTCP, Журналы, CDRs.
- Поддержка TLS.
- Высокопроизводительный.
- Поддержка Linux, Solaris, BSD/OSX, Win32.

### Функции ядра:

- Протокол NEP/EEP.
- SIP-сигналинг.
- WebRTC-сигналинг.
- Протокол RTCP.
- Протокол RTCP-XR.
- Коллектор журналов.
- Гео-меппинг.
- Поддержка Docker.

---

## 4.4.6. HEPlify

Новый легковесный Capture Agent, написанный на GO. Его можно запускать на Linux, ARM или Windows для захвата IPv4 / IPv6 пакетов и отправки их на CaptureServer.

---

## 4.4.7. NEpipe

NEpipe – это приложение командной строки для регистрации произвольных данных (логи, CDR, строк отладки) на сервере мониторинга.

---

## 4.5. Ролевая модель доступа

Управление учётными записями и правами доступа реализуется с помощью компонента Single Sign On Server (более подробно описан в документе Single Sign On Server Administration Guide).

Он обеспечивает выполнение следующих основных задач:

- предоставление «единого входа» и «единого выхода» для приложений браузера;
- поддержка OpenID Connect;
- поддержка OAuth 2.0;
- поддержка SAML;
- Identity Brokering — Аутентификация с внешними OpenID Connect или провайдерами идентификации SAML;
- поддержка федерации пользователей — синхронизация учетных данных пользователей с серверов LDAP и Active Directory;
- мост Kerberos — автоматическая аутентификация пользователей, вошедших на сервер Kerberos;
- двухфакторная аутентификация — поддержка TOTP/HOTP через Google Authenticator или FreeOTP;
- консоль администратора для централизованного управления пользователями, ролями, отображением ролей, клиентами и конфигурацией;
- управление сеансами — администраторы и могут просматривать и управлять сеансами пользователей;
- поддержка CORS — клиентские адаптеры имеют встроенную поддержку CORS;
- интерфейсы поставщиков услуг (SPI) — ряд SPI, позволяющих настраивать различные аспекты сервера. Поток аутентификации, провайдеры федерации пользователей, средства отображения протоколов;
- клиентские адаптеры для приложений JavaScript, WildFly, JBoss EAP, Fuse, Tomcat, Jetty, Spring.

В таблице 4 обозначена предопределенная ролевая модель, с которой поставляется система, также возможна настройка ролей под требование заказчика:

Таблица 4. Набор ролей в системе IMS Core

Система/ подсистема/ функция	Главный админис- тратор	Админист- ратор ОЭ	Админист- ратор ИБ	Пользова- тель ОЭ	Пользова- тель ОМ (монитор- инг)	Пользова- тель ИБ	Пользоват- ель STS (SIP Trace System)
<b>SSO</b>							
Управление политиками безопасности	RW	R	RW	R	na	R	na
Управление пользователями	RW	RW	RW	R	na	R	na
Управление ролями и группами пользователей	RW	RW	RW	R	na	R	na
<b>O&amp;M</b>							
E-Core IMS Admin Backoffice	RW	RW	R	R	R	R	na
Ansible	RW	RW	R	R	R	R	na
Logging Subsystem	RW	R	RW	R	R	R	na
Monitoring Dashboards	RW	RW	R	RW	RW	R	R
SIP Trace System	RW	RW	R	R	R	R	RW
CI\CD							
Harbor	RW	RW	R	R	na	R	na

## 5. Провижининг IMS сервисов

IMS платформа обеспечивает механизмы для вызова различных сервисов. Эта функция называется провизинингом сервиса. Ниже представлена логика работы данного функционала.

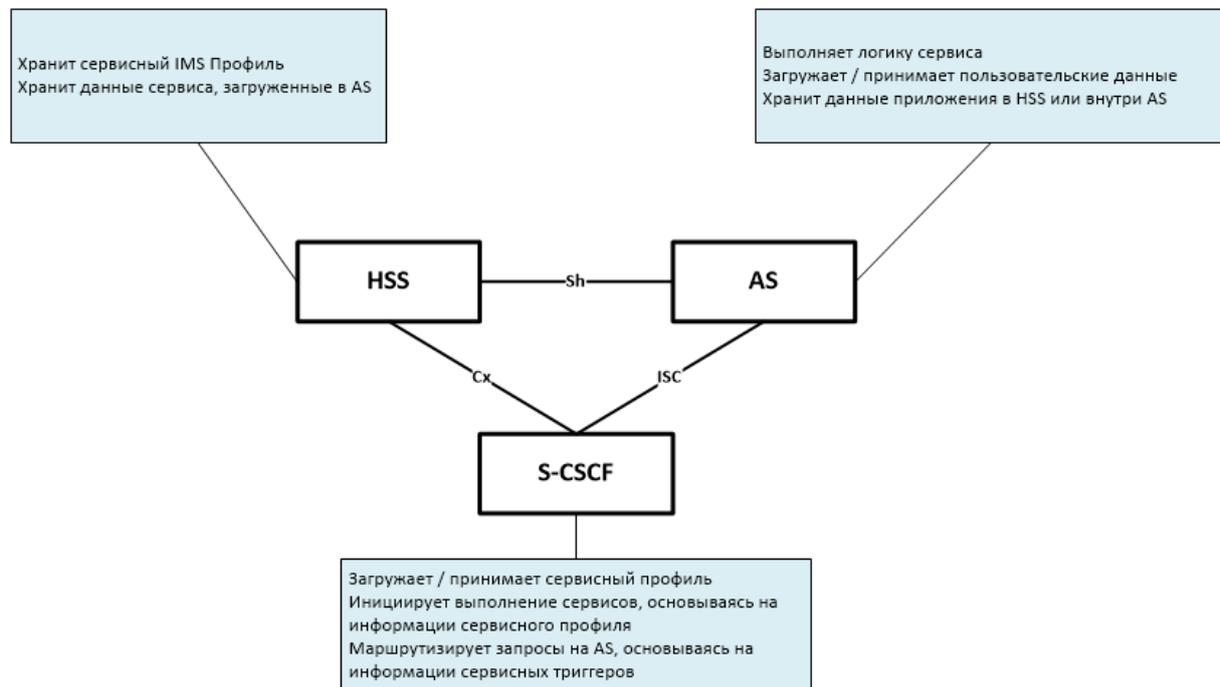


Рис. 9. Логика работы провизининга IMS сервисов

**HSS** – это центральная (master) база данных, которая содержит всю информацию о пользовательских подписках на IMS услуги, в том числе и сервисный профиль IMS. Кроме того, в HSS хранятся специфичные данные для AS.

**S-CSCF**, в свою очередь, обращается к HSS и использует загруженный из HSS сервисный профиль абонента для предоставления абоненту услуг связи, основываясь на сконфигурированных медиа политиках и перечне идентификаторов, доступных пользователю IMS услуг.

Данные медиа политик содержат числовое значение, которое идентифицирует медиа профиль абонента в S-CSCF (т. е. допустимые SDP параметры). Эта информация позволяет оператору связи дифференцировать своих пользователей. Например, «vip» пользователям доступны видео вызовы и все типы голосовых вызовов, включая вызовы с использованием AMR-WB кодека или EVS кодека; «серебряным» пользователям не доступны видео вызовы, но доступны голосовые вызовы с использованием AMR-WB кодека; «бронзовым» пользователям доступны только голосовые вызовы с использованием узкополосного AMR кодека (AMR-NB).

Хранение и передача числового значения, являющегося идентификатором медиа профиля, позволяет оптимизировать пространство хранения в HSS, а также трафик на Cx интерфейсе.

## 6. Исполнение приложений

Сервер приложений (AS) может работать в следующих режимах:

- Terminating user agent (UA).
- Originating UA.
- Redirect server.
- SIP proxy.
- Third-party call control/back to back UA (B2BUA).

1. Terminating user agent (UA) – входящий агент пользователя. В данном режиме сервер приложений принимает запрос от S-CSCF и завершает его. В качестве примера можно привести услугу записи сообщения в почтовый ящик голосовой почты (voicemail service) при недоступности абонента – user out of coverage message recording. Пункт В.2.2 3GPP 23.218. Пункт В.3.1 3GPP 23.218.

2. Originating UA – исходящий агент пользователя. В этом случае сервер приложений является инициатором запроса. В качестве примера можно привести услугу оповещения абонента о записанных сообщениях голосовой почты после его регистрации – voice mail service plays back messages. В этом примере сервер приложений (AS) после получения от S-CSCF сообщения о регистрации абонента (third party REGISTER) генерирует INVITE запрос. Пункт В.3.2 3GPP 23.218.

3. Redirect server – сервер переадресации. В данном режиме сервер приложений генерирует 3xx отклик (содержащий альтернативный набор URI) в ответ на полученный запрос. По получению данного отклика инициатор сгенерирует новый запрос на полученный URI. Новый URI может являться уточненным адресом приложения или адресом пользователя, сформированным, например, на основании местоположения вызываемого пользователя, времени суток, идентификаторов вызываемого и вызываемого пользователей, либо других атрибутов. В качестве примера можно привести услугу CFonCLI – "Call Forwarding on Calling Line Identification" (переадресация на основе идентификатора вызываемого пользователя). Пункт В.1.3 3GPP 2218.

4. SIP proxy. В данном режиме сервер приложений (AS) принимает запрос; добавляет, удаляет, либо модифицирует содержимое заголовков сообщения (в соответствии с RFC3261) и пересылает его обратно S-CSCF. В качестве примера можно привести услугу CFonCLI – "Call Forwarding on Calling Line Identification" (переадресация на основе идентификатора вызываемого пользователя). Пункт В.1.4 3GPP 23.218.

## 5. Third-party call control/back to back UA (B2BUA).

5.1. В данном режиме сервер приложений принимает запрос от S-CSCF, терминирует его и генерирует новый запрос (Routing B2BUA). В качестве примера можно привести услугу проигрывания звукового сообщения – announcement. Пункт В.2.1 3GPP 23.218.

5.2. Также в данном режиме сервер приложений может выступить инициатором, сгенерировав различные запросы, логически объединенные на уровне сервера AS (Initiating B2BUA).

Сервер приложений может получать специфические пользовательские данные, необходимые для исполнения сервисной логики несколькими путями:

- через операторскую систему управления (OSS);
- непосредственно от пользователя через Ut интерфейс;
- от HSS через Sh интерфейс.

Логика провизининга услуги:

1. Исходящий, либо входящий запрос поступает в S-CSCF.
2. S-CSCF загружает сервисный профиль (профили) пользователя из HSS. Шаг 2 исполняется, только если S-CSCF обслуживает незарегистрированного пользователя и сервисный профиль (профили) отсутствуют в S-CSCF.
3. S-CSCF оценивает все iFC в порядке их приоритета. Если критерий iFC удовлетворен – запрос направляется серверу приложений (AS) для исполнения сервисной логики.
4. Сервер приложений (AS) исполняет сервисную логику, запрашивая (при необходимости) дополнительную информацию в HSS.
5. Результат исполнения сервисной логики направляется обратно в S-CSCF. В зависимости от данного результата S-CSCF переходит к следующему шагу:
  - оценка следующего по приоритету iFC;
  - маршрутизация полученного от AS сообщения адресату;
  - направление отклика инициатору исходного запроса.

Таблица ниже описывает основные установки критериев начальной фильтрации (iFC), которые могут быть созданы для VoLTE абонента, имеющего подписку на голосовые услуги и услуги по отправке текстовых сообщений.

Таблица 5. Основные установки критериев начальной фильтрации

Критерии фильтрации	iFC 1	iFC 2	iFC 3	iFC 4
SPT: SIP method	Invite	Invite	Invite	Message
SPT: Session case	Terminating	Terminating	Originating	Originating
SIP Header				content-type:application /vnd.3gpp.sms request-URI:+79031234567
Session description	m=audio	m=audio	m=audio	
Application server	sip:tas77@ip.beeline.ru	sip:tas77@ip.beeline.ru	sip:tas77@ip.beeline.ru	sip:ipsmgw77@ip.beeline.ru
Priority	1	2	3	4
Profile indicator part	Registered	Unregistered	Registered	Registered

## 7. Услуги связи

---

### 7.1. Мультимедийные телефонные услуги – MMTEL

MMTEL (IMS Multimedia Telephony) – это стандартизированный набор мультимедийных сервисов для мобильных и фиксированных абонентов. MMTEL позволяет устанавливать соединения между пользователями, а также предоставлять пользователям дополнительные услуги (supplementary services).

MMTEL состоит из двух частей:

- базовое соединение (basic communication);
- опциональные дополнительные сервисы (optional supplementary services).

В MMTEL сервисы входят следующие стандартизированные медиа услуги:

- Голосовая связь – Speech.
- Видео связь – Video.
- Текстовая связь – Text.
- Передача факсимильных сообщений – Fax.
- Передача файлов – File Transfer.
- Совместное использование видео, аудио, изображения, файлов – Video sharing, Audio sharing, Image sharing, File sharing.

Основываясь на этих возможностях могут быть реализованы различные услуги, включая голосовые вызовы, видео вызовы, голосовые вызовы с video sharing, голосовые вызовы с передачей файлов, чат и другие.

## 7.1.1. Голосовая связь (speech)

Далее приведен перечень кодеков, которые поддерживаются сетью IMS и абонентским оборудованием для голосовой связи:

- AMR-NB (Adaptive Multi-Rate – NarrowBand);
- AMR-WB (Adaptive Multi-Rate – WideBand);
- EVS (Enhanced Voice Services).

Также обязательна поддержка обработки DTMF сигнализации.

### Кодеки AMR

Спецификация кодека AMR-NB определена в рекомендациях ETSI (1999), AMR-WB – в рекомендациях ITU-T/3GPP (2002/2001)

В таблице ниже приведен перечень поддерживаемых режимов:

Таблица 6. Поддерживаемые режимы. Кодеки AMR

	Полоса частот аудио сигнала	Частота дискретизации	Битовая скорость
AMR-NB	200 – 3 400 Гц	8 кГц	5.9, 7.2, 8.0, 9.6, 13.2, 16.4, 24.4 кбит/с
AMR-WB	50 – 7 000 Гц	16 кГц	6.6, 8.85, 12.65, 14.25, 15.85, 18.25, 19.85, 23.05, 23.85 кбит/с

Задержка – 20мс, размер фрейма – 5мс, тип кодирования – ACELP.

### Кодек EVS

Спецификация кодека определена в рекомендациях 3GPP (2014) TS 26.441-451, 26.952.

В таблице ниже приведен перечень поддерживаемых режимов:

Таблица 7. Поддерживаемые режимы. Кодеки EVS

	Полоса частот аудио сигнала	Частота дискретизации	Битовая скорость
Narrowband (NB)	20 – 4 000 Гц	8 кГц	5.9, 7.2, 8.0, 9.6, 13.2, 16.4, 24.4 кбит/с
Wideband (WB)	20 – 8 000 Гц	16 кГц	5.9, 7.2, 8.0, 9.6, 13.2, 16.4, 24.4, 32.0, 48.0, 64.0, 96.0, 128.0 кбит/с
Super wideband (SWB)	20 – 16 000 Гц	32 кГц	9.6, 13.2, 16.4, 24.4, 32.0, 48.0, 64.0, 96.0, 128.0 кбит/с
Fullband (FB)	20 – 20 000 Гц	48 кГц	16.4, 24.4, 32.0, 48.0, 64.0, 96.0, 128.0 кбит/с

Задержка – 20мс, размер фрейма – 12мс, тип кодирования – ACELP/MDCT.

---

## 7.1.2. Видео связь (video)

Далее приведен перечень кодеков, которые поддерживаются сетью IMS и абонентским оборудованием для для видео связи (видео-кодеки не входят в состав базовой поставки):

1. H.264 / MPEG-4 часть 10 (Advanced Video Coding – AVC), ограниченный базовый профиль (Constrained Baseline Profile – CBP), уровень 2 – поддержка обязательна:

- рекомендация ITUT H.264 или полностью идентичная ей рекомендация ISO/IEC MPEG4 часть 10;
- макс. скорость видеопотока (VCL) – 384 кбит/с;
- разрешение@частота кадров – 320×240@20,0; 352×288@15,2.

2. H.264 / MPEG-4 часть 10 (AVC), CBP, уровень 3.1

- рекомендация ITUT H.264 или полностью идентичная ей рекомендация ISO/IEC MPEG4 часть 10;
- макс. скорость видеопотока (VCL) 14000 кбит/с;
- разрешение@частота кадров 720×480@80,0; 720×576@66,7; 1280×720@30,0.

3. H.265 / (High Efficiency Video Coding – HEVC), основной профиль (Main Profile), основной ярус (Main Tier), уровень 1

- рекомендация ITUT H.265 или полностью идентичная ей рекомендация ISO/IEC 230082 MPEG-H часть 2;
- макс. скорость видеопотока (VCL) 10000 кбит/с;
- разрешение@частота кадров 720×480@84.3; 720×576@75.0; 960×544@60.0; 1280×720@33.7.

---

## 7.1.3. Текстовая связь (text)

Спецификация протокола приведена в рекомендации ITU-T T.140 (Протокол мультимедийных приложений для текстовой связи – Protocol for multimedia application text conversation). Текстовые символы передаются в UTF-8 форме ISO 10646-1.

---

## 7.1.4. Передача факсимильных сообщений (fax)

Спецификация протокола приведена в рекомендации ITU-T T.38 (Процедуры для факсимильной связи через IP сети – Procedures for real-time Group 3 facsimile communication over IP networks).

---

## 7.1.5. Прочие MMTEL сервисы

Передача файлов, video/audio/image/file sharing, чат основан на протоколе MSRP – Message Session Relay Protocol (RFC4975). Поддержка не входит в базовую поставку.

## 7.2. Дополнительные услуги (Supplementary Services)

Для поддержки дополнительных IMS услуг на сети установлен сервер телефонных приложений (Telephony Application Server – TAS), который является SIP-сервером, включенном в IMS через ICS интерфейс, и обеспечивает поддержку дополнительных сервисов MMTEL.

В дополнение к логике управления SIP вызовами TAS поддерживает интерфейс для обеспечения возможности настройки сервисов пользователем. Существуют следующие стандартизированные возможности по настройке сервисов:

- XCAP через Ut интерфейс (между абонентским терминалом и сервером приложений);
- конфигурация посредством SIP протокола.

В таблице ниже показаны стандартизированные IMS supplementary сервисы. Часть из этих сервисов включены в IMS профиль GSMA (IR.92) для голоса и SMS. При этом GSMA вводит дополнительные ограничения для услуг переадресации и блокировки вызовов.

Таблица 8. Описание дополнительных услуг

Доп. услуга	Описание	Соответствие GSMA IR.92
Идентификация вызывающего пользователя (Originating Identification Presentation – OIP)	Сервис позволяет "абоненту В" получить идентификаторы вызывающего абонента	Да
Запрет идентификации вызывающего пользователя (Originating Identification Restriction – OIR)	Сервис позволяет "абоненту А" скрыть свой идентификатор (свои идентификаторы) от других абонентов	Да
Идентификация вызываемого пользователя (Terminating Identification Presentation – TIP)	Сервис позволяет "абоненту-А" получить идентификатор вызываемого им пользователя	Да
Запрет идентификации вызываемого пользователя (Terminating Identification Restriction – TIR)	Сервис позволяет "абоненту В" устанавливать запрет на представление идентификатора / идентификаторов (PuUI)	Да
Удержание сессии/вызова (Communication Hold – CH)	Сервис позволяет пользователю приостановить медиа поток установленной сессии и впоследствии восстановить его	Да

Доп. услуга	Описание	Соответствие GSMA IR.92
Конференция (Conference – CONF)	Сервис позволяет пользователю организовать взаимодействие с двумя или более партнерами одновременно	Да
Переадресация сессий/вызовов (Communication Diversion – CDIV)	Сервис позволяет перенаправлять сессии/вызовы, адресуемые обслуживаемому пользователю ("абоненту В") и удовлетворяющие predetermined условиям, на терминирующего пользователя ("абонента С")	Да
Блокировка сессий/вызовов (Communication Barring – CB)	Сервис позволяет пользователям селективно блокировать установление сессий	Да
Индикатор ожидания сообщения (Message Waiting Indication – MWI)	Сервис позволяет индицировать обслуживаемому пользователю о наличии в его ящике сообщений	Да
Перевод вызова (Explicit communication transfer – ECT)	Сервис позволяет пользователю, имеющему активную сессию (активный вызов), перевести данную сессию (вызов) другому абоненту	Да
Ожидание сессии/вызова (Communication Waiting – CW)	Сервис позволяет пользователю, имеющему активную сессию (активный вызов), быть проинформированным о дополнительной входящей сессии (входящем вызове)	Да

Ниже приведено описание основных supplementary сервисов.

При описании приняты следующие сокращения:

- абонент А – вызывающий абонент (абонент, инициирующий вызов);
- абонент В – вызываемый абонент (абонент, которому адресован вызов);
- абонент С – абонент, на номер (идентификатор) которого переадресован вызов;
- UEA – терминал вызывающего абонента (абонентаА);
- UEВ – терминал вызываемого абонента (абонентаВ);
- UEC – терминал абонента, на номер (идентификатор) которого переадресован вызов (абонентаС);
- O\_P-CSCF (исходящий P-CSCF) – P-CSCF, обслуживающий абонентаА;
- T\_P-CSCF (терминирующий P-CSCF) – P-CSCF, обслуживающий абонентаВ;
- O\_TAS (исходящий TAS) – TAS, обслуживающий абонентаА;
- T\_TAS (терминирующий TAS) – TAS, обслуживающий абонентаВ.

## 7.2.1. Идентификация вызывающего пользователя (OIP)

Сервис OIP (Originating Identification Presentation) позволяет абоненту-В получить идентификаторы вызывающего абонента.

Публичные идентификаторы пользователя (PuUI) передаются в трех заголовках SIP INVITE запроса:

1. Заголовок «From», который может быть установлен пользователем в любое значение.
2. Заголовок «P-Preferred-Identity», в котором пользователь указывает один из имеющихся публичных идентификаторов (PuUI), которым он хочет идентифицировать вызов.
3. Заголовок «P-Asserted-Identity», в котором передается авторизованный публичный идентификатор пользователя (PuUI).

В этом случае в части идентификации пользователя SIP INVITE запрос может выглядеть следующим образом:

```
INVITE sip:mikhail@ip.operator.ru SIP/2.0
From: "IgorL" <sip:igor@ip.operator.ru >;tag=171828
P-Preferred-Identity: <sip:igor@ip.operator.ru>
```

O\_P-CSCF сравнивает полученный запрос с имеющимися данными, сохраненными при регистрации абонента-А в сети на предмет корректности идентификатора, указанного им в заголовке "P-Preferred-Identity". При этом возможны следующие варианты:

1. Идентификатор "P-Preferred-Identity" корректен. В этом случае P-CSCF заменяет заголовок "P-Preferred-Identity" на "P-Asserted-Identity" с аналогичным значением.
2. Идентификатор "P-Preferred-Identity" не корректен. В этом случае P-CSCF удаляет заголовок "P-Preferred-Identity" и создает новый заголовок "P-Asserted-Identity" со значением публичного идентификатора пользователя по умолчанию (default PuUI) – фактически первым PuUI, полученным при регистрации.

В результате SIP INVITE запрос будет выглядеть следующим образом:

```
INVITE sip:mikhail@ ip.operator.ru SIP/2.0
From: "IgorL" <sip:igor@ip.operator.ru >;tag=171828
P-Asserted-Identity: <sip:igor@ip.operator.ru >
```

Таким образом, заголовок "P-Asserted-Identity" несет информацию о подтвержденном (авторизованном) идентификаторе пользователя и используется не только для предоставления OIP услуги, но и для идентификации авторизованного пользователя внутри IMS сети. Заголовок "P-Asserted-Identity" будет содержаться в SIP запросе, полученным абонентом-В, когда запрос пройдет через доверенную сеть сигнализации при условии, что настройки сети в соответствии с технической политикой оператора не деактивируют OIP услугу. Если CSCF обнаружит, что

следующий узел сети, которому должен быть направлен запрос, не является доверенным – заголовок "P-Asserted-Identity" будет удален.

## 7.2.2. Запрет идентификации вызывающего пользователя (OIR)

OIR (Originating Identification Restriction) сервис позволяет абоненту-А скрыть свой идентификатор (свои идентификаторы) от других абонентов. Пользователи могут активировать данный функционал в профиле TAS либо по умолчанию, либо при каждом вызове. Для совершения вызова со скрытым идентификатором абонент-А должен установить в запросе SIP INVITE заголовок "From" в значение "anonymous".

```
INVITE sip:mikhail@ip.operator.ru SIP/2.0
From: "anonymous" <sip:anonymous@invalid>;tag=xyz
```

Возможна ситуация, что пользователь подписан на OIR сервис и хочет, чтобы исходящий вызов был анонимным в любой случае, независимо от того – какое значение выставил пользовательский терминал в заголовке "From" запроса SIP INVITE. В этом случае TAS будет устанавливать значение заголовка "From" в значение "anonymous" при любом вызове, выступая в качестве "back to back user agent (B2BUA)".

Поскольку заголовок "P-Asserted-Identity" используется в т.ч. для идентификации пользователя внутри сети, его значение не может быть установлено в "anonymous". Поэтому дополнительный SIP заголовок "Privacy" используется для того, чтобы идентифицировать, что абонент-А хочет скрыть свой идентификатор (совершить анонимный вызов). Для активации OIR сервиса для конкретного вызова, абонент-А должен включить в запрос SIP INVITE заголовок "Privacy", установленный в значение "id", на основании чего терминирующий P-CSCF удалит заголовок "P-Asserted-Identity" перед маршрутизацией запроса абоненту-В.

Если пользователь активировал OIR сервис на постоянной основе – заголовок "Privacy: id" будет устанавливать TAS в каждом SIP INVITE запросе.

```
INVITE sip:mikhail@ip.operator.ru SIP/2.0
From: "anonymous" <sip:anonymous@invalid>;tag=xyz
P-Asserted-Identity: <sip:igor@ip.beeline.ru >

Privacy: id
```

Активация / деактивация сервиса OIR на постоянной основе может быть сделана, например, посредством отправки пользователем XCAP сообщения через Ut интерфейс.

---

### 7.2.3. Идентификация вызываемого пользователя (TIP)

TIP (Terminating Identification Presentation) сервис позволяет абоненту-А получить идентификатор вызываемого им пользователя. Абонент-В будет идентифицироваться заголовком "P-Asserted-Identity", устанавливаемым Т\_Р-CSCF узлом в первом SIP отклике на основе заголовка "P-Preferred-Identity"

---

SIP/2.0 183 Session Progress

P-Asserted-Identity: <mikhail@ip.operator.ru>

---

При маршрутизации сообщения "183 (Session Progress)" от вызываемого к вызывающему пользователю через узлы, доверенные друг другу, значение заголовка "P-Asserted-Identity" будет сохранено.

---

### 7.2.4. Запрет идентификации вызываемого пользователя (TIR)

TIR (Terminating Identification Restriction) сервис позволяет абоненту-В устанавливать запрет на представление идентификатора / идентификаторов (PuUI) аналогично сервису OIR для абонента-А. Для того, чтобы активировать OIR сервис абонент-В добавляет заголовок "Privacy" со значением "id" в каждый SIP отклик, содержащий "P-Preferred-Identity" заголовок. Т\_Р-CSCF при маршрутизации сообщения добавляет в него заголовок "P-Asserted-Identity" и сохраняет значение заголовка "Privacy" без изменения. О\_Р-CSCF на основании заголовка Privacy удаляет заголовок P-Asserted-Identity перед маршрутизацией сообщения абоненту-В.

---

SIP/2.0 183 Session Progress

P-Asserted-Identity: <mikhail@ip.operator.ru>

Privacy: id

---

Абонент-В может подписаться на TIR сервис, предоставляемый на постоянной основе. В этом случае Т\_ТAS будет добавлять заголовок "Privacy: id" в каждый отклик абонента-В, содержащий заголовок "P-Asserted-Identity". Активация / деактивация сервиса OIR на постоянной основе может быть сделана, например, посредством отправки пользователем XCAP сообщения через Ut интерфейс.

---

## 7.2.5. Переадресация сессий/вызовов (CDIV)

**Сервис CDIV (Communication Diversion)** позволяет перенаправлять сессии/вызовы, адресуемые обслуживаемому пользователю и удовлетворяющие predetermined условиям, на terminating пользователя.

CDIV унаследован от аналогичных услуг сетей PSTN/PLMN и по сути является набором сервисов, включающим в себя:

**Сервис безусловной переадресации (CFU – Communication forwarding unconditional).** Обеспечивает безусловную сетевую переадресацию всех сессий/вызовов, адресованных обслуживаемому пользователю.

**Сервис переадресации по занятости (CFB – Communication forwarding busy).** Обеспечивает условную сетевую переадресацию сессий/вызовов, адресованных обслуживаемому пользователю в случае его занятости другой сессий / другим вызовом.

**Сервис переадресации по неответу (CFNR - Communication forwarding no reply).** Обеспечивает условную сетевую переадресацию сессий/вызовов, адресованных обслуживаемому пользователю в случае неответа обслуживаемого пользователя в течение predetermined периода времени.

**Сервис переадресации по отсутствию регистрации (CFNL - Communication forwarding on not logged-in).** Обеспечивает условную сетевую переадресацию сессий/вызовов, адресованных обслуживаемому пользователю в случае если обслуживаемый пользователь не зарегистрирован в сети.

**Сервис переадресации по недоступности (CFNRc - Communication diversion on mobile subscriber not reachable).** Обеспечивает условную сетевую переадресацию сессий/вызовов, адресованных обслуживаемому пользователю в случае его недоступности (отсутствии IP связанности).

**Сервис отклонения вызова (CD – Communication deflection).** Позволяет обслуживаемому пользователю ответить на входящую сессию/вызов с запросом переадресации.

Управление правилами переадресаций осуществляется через XCAP протокол.

---

## 7.2.6. Удержание сессии/вызова (CH)

CH (Communication Hold) сервис позволяет пользователю приостановить медиа поток установленной сессии и впоследствии восстановить его.

Когда пользователь хочет "повесить вызов на удержание" он нажимает соответствующую кнопку на своем терминале в результате чего терминал (UE) посылает запрос UPDATE или RE-INVITE к терминалу встречного пользователя с атрибутом "line" SDP, установленным в значение "inactive" или "sendonly".

Когда пользователь хочет восстановить вызов он нажимает необходимую кнопку на своем терминале в результате чего терминал (UE) повторно посылает UPDATE или RE-INVITE запрос к терминалу встречного пользователя с атрибутом "line" SDP установленным в значение "sendrecv" или "recvonly".

На время удержания вызова TAS может проигрывать пользователю звуковое сообщение (announcement).

---

## 7.2.7. Блокировка сессий/вызовов (CB)

Сервис блокировки связи (CB - Communication Barring) позволяет пользователям селективно блокировать установление сессий. Сервис может быть разделен на три основных класса – блокировка входящей связи (ICB – incoming communications barring), блокировка исходящей связи (OCB – outgoing communication barring) и отклонение анонимной связи (ACR – anonymous communication rejection).

ICB представляет собой сервис, отклоняющий входящие сессии обслуживаемого пользователя, которые удовлетворяют определенным критериям в соответствии с клиентской подпиской и настройками.

OCB представляет собой сервис, отклоняющий попытки установления исходящих сессий обслуживаемого пользователя, которые удовлетворяют определенным критериям в соответствии с клиентской подпиской и настройками.

ACR представляет собой частный случай ICB сервиса, который позволяет блокировать входящие сессии от анонимных пользователей.

---

## 7.2.8. Конференция (CONF)

Сервис CONF (Conference) позволяет пользователю организовать взаимодействие с двумя или более партнерами одновременно. В организации конференции участвуют модули MRFC (Media Resource Function Controller) и MRFP (Media Resource Function Processor), обеспечивающие объединение (смешивание) медиапотокот от нескольких пользователей.

Для создания конференции пользователь нажимает соответствующую кнопку на своем терминале (UE), в результате чего терминал посылает запрос INVITE на SIP-URI, известный как conference-factory URI (sip:conf-factory@mmtel.ims.mnc099.mcc250.3gppnetwork.org.).

## 7.2.9. Индикатор ожидания сообщения (MWI)

Сервис MWI (Message Waiting Indication) позволяет TAS индицировать обслуживаемому пользователю о наличии в его ящике сообщений (message account) сообщений различных типов.

Для активации этого сервиса пользовательский терминал (UE) должен отправить в сеть SIP SUBSCRIBE запрос, пример которого приведен ниже.

```
SUBSCRIBE sip:mikhail@ip.operator.ru SIP/2.0
Via: SIP/2.0/UDP [5555::a:b:c:d]:1400;branch=4uetb
Route: <sip:[5555::55:66:77:88];lr>
Route: <sip:orig@ip.operator.ru>
From: <mikhail@ip.operator.ru>;tag=7547d
To: <mikhail@ip.operator.ru>
Event: message-summary
Expires: 86400
Accept: application/simple-message-summary
Contact: <sip:[5555::a:b:c:d]:1400>
Content-Length: 0
```

В этом примере:

- "Request URI" идентифицирует пользовательский ящик сообщений (message account) и в зависимости от технической политики оператора должен быть указан либо в форме публичного идентификатора пользователя (PuUI как в нашем примере), либо публичного идентификатора сервиса (PSI);
- заголовок Event должен содержать значение "messagesummary", которое определяет, что пользователь хочет активировать MWI услугу;
- заголовок Accept должен содержать значение "application/simplemessagesummary", индицирующее тип информации MWI (простой текстовый формат), который может быть обработан терминалом отправителя.

TAS, получив SUBSCRIBE запрос, проверяет текущую подписку пользователя на предмет возможности использования MWI сервиса, после чего:

- возвращает "200 (OK)" отклик на запрос пользователя, индицируя, что активация сервиса была успешно выполнена;
- генерирует и посылает NOTIFY сообщение пользователю (см. пример ниже), содержащее общую (суммарную) информацию, касающуюся текущего статуса ящика сообщений (message account).

В дальнейшем сообщения нотификации могут содержать расширенную информацию, включая заголовки "to", "from", "subject", "date", "priority"

```
NOTIFY sip:mikhail@ip.operator.ru SIP/2.0
From: <sip:mikhail@ip.operator.ru>;tag=31415
```

```
To: <sip:mikhail@ip.operator.ru>; tag=7547d
Subscription-State: active; expires=86399
Event: message-summary
Content-Type: application/simple-message-summary
Content-Length: (...)
Messages-Waiting: yes
Message-Account: sip:mikhail@ip.operator.ru
Voice-Message: 2/1 (1/0)
Video-Message: 0/1 (0/0)
```

---

В приведенном примере в ящике сообщений пользователя (message account) содержатся 3 голосовых сообщения (в т.ч. два новых сообщения, одно срочное сообщение) и одно прочитанное видео сообщение. В примере не приведены данные по сообщениям типа fax-message, pager-message, multimedia-message, text-message.

---

## 7.2.10. Ожидание сессии/вызова (CW)

Сервис CW (Communication Waiting) позволяет пользователю, имеющему активную сессию (активный вызов), быть проинформированным о дополнительной входящей сессии (входящем вызове).

Существуют два режима предоставления услуги – сеть-ориентированный режим (network-based CW) и терминал-ориентированный режим (terminal-based CW). В случае сеть-ориентированного режима TAS определяет срабатывание режима ожидания вызова и информирует об этом пользователя. В случае терминал-ориентированного режима UE-B определяет срабатывание режима ожидания вызова и информирует об этом TAS. Ниже приведены call flow для обоих режимов.

Обслуживаемый пользователь (абонент-B) получает индикацию ожидающего вызова (через тональный или визуальный сигнал). Вызывающий пользователь (абонент-A) также получает уведомление о том, что совершенный им вызов находится в состоянии ожидания. Это достигается тем, что TAS, либо UE (в зависимости от режима CW) добавляет заголовок "Alert-Info" со значением, равным "urn:alert:service:call-waiting" в отклик "180 (RINGING)". Также TAS обслуживаемого пользователя (TAS-B) может проигрывать голосовое сообщение вызывающему пользователю (абоненту-A).

---

### 7.2.11. Передача связи (ECT)

Explicit Communication Transfer (ECT) – это услуга, которая предоставляет стороне, участвующей в сессии, возможность переадресации сессии на третью сторону.

В переадресации участвуют три роли:

- передающая сторона: сторона, которая инициирует передачу активной сессии;
- получатель: сторона, которая остается в сессии, которая переводится на третью сторону;
- цель: третья сторона, на которую переводится сессия. После переадресации она становится передающей стороной.

Возможны две начальные ситуации, в которых возможна переадресация:

- Передающая сторона не имеет постоянной консультационной связи с целью передачи (слепая / безусловная переадресация).
- Передающая сторона имеет консультационную связь с целью (консультационный перевод).



- Переадресация по занятости.
- Переадресация по не ответу.
- Переадресация по недоступности.
- Выборочная переадресация.
- Индивидуальная переадресация.
- Ограничение вызовов.
- Музыка на удержании.
- Мелодия вместо гудков.
- Перевод вызова.
- Перевод вызова консультационный.
- Перехват вызова.
- Запись разговоров.
- Голосовая почта.
- Черный и белый список.
- Факс.
- Внешняя АТС по SIP.
- Звонок с сайта.
- API управления вызовами / уведомление о событиях (XSI).
- BLF (пульт мониторинга занятости абонентов).

## 9. Перечень стандартов

В текущем разделе представлен перечень стандартов, использованных при:

- разработке элементов системы
- реализации интерфейсов к:
  - внутренним элементам ядра IMS
  - сторонним элементам ядра IMS
  - внешним соединениям

---

### 9.1. Серия RFC

RFC (Request for Comments) – документ из серии пронумерованных информационных документов Интернета, содержащих технические спецификации и стандарты, подготовленные рабочими группами:

- Целевой группой по проектированию Интернета (IETF)
- Целевой группой по исследованиям в Интернете (IRTF)
- Советом по архитектуре Интернета (IAB)

В таблице ниже представлен перечень спецификаций RFC, использованных при реализации системы.

*Таблица 9. Перечень спецификаций RFC, использованных при реализации элементов системы*

Номер RFC	Наименование документа	Версия док.
1889	RTP: A Transport Protocol for Real-Time Applications	1996-01
2486	The Network Access Identifier	1999-01
2616	Hypertext Transfer Protocol -- HTTP/1.1	1999-01
2822	Internet Message Format	2001-04
2833	RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals	2000-05
2915	The Naming Authority Pointer (NAPTR) DNS Resource Record	2000-09
2976	The SIP INFO Method	2000-10
3261	SIP: Session Initiation Protocol	2002-06
3262	Reliability of Provisional Responses in the Session Initiation Protocol (SIP)	2002-06
3263	Session Initiation Protocol (SIP): Locating SIP Servers	2002-06

3264	An Offer/Answer Model Session Description Protocol	2002-06
3265	Session Initiation Protocol (SIP)-Specific Event Notification	2002-06
3311	The Session Initiation Protocol (SIP) UPDATE Method	2002-09
3312	Integration of Resource Management and Session Initiation Protocol (SIP)	2002-10
3323	A Privacy Mechanism for the Session Initiation Protocol (SIP)	2002-11
3325	Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks	2002-11
3326	The Reason Header Field for the Session Initiation Protocol (SIP)	2002-12
3327	Path Extension Header Field for SIP	2002-12
3403	Dynamic Delegation Discovery System (DDDS). Part Three: The Domain Name System (DNS) Database	2002-10
3428	Session Initiation Protocol (SIP) Extension for Instant Messaging	2002-12
3455	Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)	2003-01
3515	The Session Initiation Protocol (SIP) Refer Method	2003-04
3550	RTP: A Transport Protocol for Real-Time Applications	2003-07
3551	RTP Profile for Audio and Video Conferences with Minimal Control	2003-07
3556	SDP Bandwidth Modifiers for RTCP Bandwidth	2003-07
3588	Diameter Base Protocol	2003-09
3608	Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration	2003-10
3680	A Session Initiation Protocol (SIP) Event Package for Registrations	2004-03
3840	Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)	2004-08
3841	Caller Preferences for the Session Initiation Protocol (SIP)	2004-08
3842	A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)	2004-08
3891	The Session Initiation Protocol (SIP) "Replaces" Header	2004-09
3959	The Early Session Disposition Type for the Session Initiation Protocol (SIP)	2004-12

3960	Early Media and Ringing Tone Generation	2004-12
3966	The tel URI for Telephone Numbers	2004-12
3986	Uniform Resource Identifier (URI): Generic Syntax	2005-01
4006	Diameter Credit-Control Application	2005-08
4028	Session Timers in the Session Initiation Protocol (SIP)	2005-04
4032	Update to the Session Initiation Protocol (SIP). Preconditions Framework	2005-03
4244	An Extension to the Session Initiation Protocol (SIP) for Request History Information	2005-11
4301	Security Architecture for the Internet Protocol	2005-12
4566	SDP: Session Description Protocol	2006-07
4585	Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)	2006-07
4596	Guidelines for Usage of the Session Initiation Protocol (SIP). Caller Preferences Extension	2006-07
4733	RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals	2006-12
4867	RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB). Audio Codecs	2007-04
4960	Stream Control Transmission Protocol	2007-09
6050	A Session Initiation Protocol (SIP) Extension for the Identification of Services	2010-11
6116	The E.164 to Uniform Resource Identifiers (URI). Dynamic Delegation Discovery System (DDDS) Application (ENUM)	2011-03
6117	IANA Registration of Enumservices: Guide, Template, and IANA Considerations	2011-03
6223	Indication of Support for Keep-Alive	2011-04
6733	Diameter Base Protocol	2012-10

## 9.2. Серия GSMA

Ассоциация GSMA (Global System for Mobile Communications) — организация, представляющая интересы операторов мобильной связи по всему миру.

В таблице ниже представлен перечень спецификаций GSMA, использованных при реализации системы.

*Таблица 10. Перечень спецификаций GSMA, использованных при реализации элементов системы*

Номер IR	Наименование документа	Версия док.
64	IMS Service Centralization and Continuity Guidelines	14.0
67	DNS and ENUM Guidelines for Service Providers and GRX and IPX Providers	14.0
92	IMS Profile for Voice and SMS	15.0
95	SIP-SDP Inter-IMS NNI Profile	8.0

## 9.3. Серия 3GPP

3GPP (3rd Generation Partnership Project) — консорциум, разрабатывающий спецификации для мобильной телефонии.

В таблице ниже представлен перечень спецификаций 3GPP, использованных при реализации системы.

Таблица 11. Перечень спецификаций 3GPP, использованных при реализации элементов системы

Номер TS	Наименование документа	Версия док.
22.173	IP Multimedia Core Network Subsystem (IMS) Technical Specification Multimedia Telephony Service and supplementary services; Stage 1	17.3.0
23.002	Network architecture	17.0.0
23.003	Numbering, addressing and identification	17.7.0
23.203	Policy and charging control architecture	17.2.0
23.228	IP Multimedia Subsystem (IMS); Stage 2	17.3.0
23.237	IP Multimedia Subsystem (IMS) Service Continuity; Stage 2	17.0.0
23.292	IP Multimedia Subsystem (IMS) centralized services; Stage 2	17.0.0
24.173	IMS multimedia telephony communication service and supplementary services; Stage 3	17.2.0
24.229	IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3	17.8.1
24.237	IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) Service Continuity; Stage 3	17.2.0
24.292	IP Multimedia (IM) Core Network (CN) subsystem Centralized Services (ICS); Stage 3	17.0.0
24.604	Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification	17.0.0
24.628	Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification	17.0.0

24.629	Explicit Communication Transfer (ECT) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification	17.0.0
26.071	Mandatory speech CODEC speech processing functions; AMR speech CODEC; General description	17.0.0
29.002	Mobile Application Part (MAP) specification	17.2.0
29.162	Interworking between the IM CN subsystem and IP networks	17.0.0
29.163	Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks	17.3.0
29.165	Inter-IMS Network to Network Interface (NNI)	17.4.0
29.214	Policy and Charging Control over Rx reference point	17.4.0
29.228	IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents	17.1.0
29.229	Cx and Dx interfaces based on the Diameter protocol; Protocol details	17.2.0
29.230	Diameter applications; 3GPP specific codes and identifiers	17.2.0
29.238	Interconnection Border Control Functions (IBCF) – Transition Gateway (TrGW) interface, Ix Interface; Stage 3	17.0.0
29.278	Customized Applications for Mobile network Enhanced Logic (CAMEL) Phase 4; CAMEL Application Part (CAP) specification for IP Multimedia Subsystems (IMS)	17.0.0
32.101	Telecommunication management; Principles and high level requirements	17.0.0
32.240	Telecommunication management; Charging management; Charging architecture and principles	18.0.0
32.260	Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging	17.4.0
32.295	Telecommunication management; Charging management; Charging Data Record (CDR) transfer	17.0.0
32.297	Telecommunication management; Charging management; Charging Data Record (CDR) file format and transfer	17.2.0
32.299	Telecommunication management; Charging management; Diameter charging applications	17.0.0
32.409		

32.409	Telecommunication management; Performance Management (PM); Performance measurements; IP Multimedia Subsystem (IMS)	17.0.0
32.432	Telecommunication management; Performance measurement: File format definition	17.0.0
32.435	Telecommunication management; Performance measurement; eXtensible Markup Language (XML) file format definition	17.0.0
32.454	Telecommunication management; Key Performance Indicators (KPI) for the IP Multimedia Subsystem (IMS); Definitions	17.0.0
32.600	Telecommunication management; Configuration Management (CM); Concept and high-level requirements	17.0.0
33.203	3G security; Access security for IP-based services	17.1.0
33.328	System Aspects; IP Multimedia Subsystem (IMS) media plane security	17.1.0

## 10. Глоссарий

### З

**3GPP (3rd Generation Partnership Project)** – партнерский проект, занимающийся стандартизацией в области мобильной связи. 3GPP осуществляет классификацию пользовательских терминалов (UE) в зависимости от максимальной скорости передачи в нисходящем (Downlink-DL) и восходящем (Uplink-UL) каналах, допустимым конфигурациям MIMO и поддерживаемым уровням модуляции.

### А

**AMR-NB (Adaptive Multi-Rate Narrowband)** – узкополосный многоскоростной адаптивный кодек.

**AMR-WB (Adaptive Multi-Rate Wideband)** – широкополосный многоскоростной адаптивный кодек.

**APN (Access Point Name)** – точка доступа к сети.

**Application Server (AS)** – это ядро системы E-TAS. Работает на Linux машине. Подсистема принимает и обрабатывает сообщения протокола SIP, а также определяет, каким образом должен быть инициирован исходящий вызов. Подсистема отвечает за реализацию базовых сервисов обработки вызовов и оказываемые абоненту услуги, включая переадресацию, короткие номера и другие услуги, настроенные пользователем в портале.

### В

**BGCF (Breakout Gateway Control Function)** – узел выбора домена с коммутацией каналов сети IMS.

**Black White List** – услуга позволяет ограничить прием звонков на многоканальные номера компании от указанных в настройках номеров или пулов номеров (масок). Это может быть полезно, когда на многоканальные номера поступает большое кол-во ошибочных или злонамеренных звонков.

**BLF (Busy Lamp Field)** – услуга, которая позволяет через функцию SIP-телефонов отслеживать текущее состояние линий других абонентов облачной АТС с помощью светящихся индикаторов. SIP-телефона.

**Blind Call Transfer** – услуга, при подключении которой звонок будет сразу переведен на другой номер, вне зависимости от доступности изначально вызываемого абонента.

**C-MSISDN (Correlation MSISDN)** – номер корреляции, используемый для увязки между собой транзакций в рамках процедуры SRVCC.

**Call Center** – услуга, в которой пользователь может создать очередь входящих вызовов, настроить информирование абонентов о времени ожидания и контролировать работу сотрудников.

**Call Forwarding Busy** – услуга, при подключении которой звонок будет переадресован, если вызываемый абонент занят.

**Call Forwarding Selective** – услуга, которая позволяет выборочно переадресовывать вызовы в зависимости от номера, звонящего и расписания (рабочее/нерабочее время).

**Call Forwarding Unconditional** – предоставляет возможность переадресовывать входящие вызовы вне зависимости от расписания и входящего номера.

**Call Forwarding Unreachable** – услуга, при подключении которой всегда будет совершена попытка подключить ваши звонки в обычном режиме, и, если это не удастся, то они автоматически будут переадресованы на указанный номер. Если телефон станет доступен, звонки будут подключаться в обычном режиме.

**Call Hold/Music On Hold** – услуга, при подключении которой при постановке звонка на удержание может проигрываться выбранная мелодия.

**Call Recording** – услуга, в которой пользователь может включить или отключить запись телефонных разговоров для выбранных номеров. Система сохраняет записи в облачное хранилище, из которого пользователь имеет быстрый и удобный доступ к записям.

**Call Pickup** – прием вызова.

**Call-me-now** – услуга «Позвони мне сейчас», позволяет заказать звонок с веб-сайта при переходе по ссылке.

**Caller ID** – ID абонента А (совершающего вызов).

**Callrecord** – модуль, отвечающий за передачу полученных файлов в Портал ОАТС (записи разговоров, факсы, голосовая почта).

**CB (Communication Barring)** – услуга блокировки связи.

**CDIV (Communication Diversion)** – услуга переадресации вызовов.

**CH (Communication Hold)** – услуга удержания вызова.

**Cloud PBX (Облачная АТС)** – комплекс сервисов офисной АТС, необходимых для обеспечения бизнес-коммуникаций сотрудников.

**CS (Circuit Switched)** – коммутация каналов.

**CSCF (Call Session Control Function)** – функция управления сеансом связи сети IMS.

**CSFB (CS Fallback)** – технология перевода вызова в сети 2G/3G.

**CW (Communication Waiting)** – услуга ожидания вызова.

## D

**Dedicated bearer** – выделенное виртуальное соединение, ассоциированное с пакетными фильтрами восходящего канала (UL) в UE и пакетными фильтрами нисходящего канала (DL) в PDN-GW. Данные фильтры выделяют поток абонентских данных, которым необходим специфический уровень QoS.

**Default bearer** – виртуальное соединение по умолчанию (дефолтное виртуальное соединение). Создается при установке каждого нового соединения пользовательского терминала (UE) с пакетной сетью и остается неизменным на протяжении всего времени жизни данного соединения. Виртуальное соединение по умолчанию является виртуальным соединением без гарантированной скорости (non-GBR bearer). Каждое соединение UE с пакетной сетью характеризуется именем точки доступа (APN).

**DRX (Discontinuous Reception)** – режим прерывистого приема.

## E

***E-CSCF (Emergency CSCF)*** – узел обслуживания экстренных служб сети IMS.

***E-RAB (E-UTRAN Radio Access Bearer)*** – данный термин определяет виртуальное соединение (bearer), переносящий абонентский трафик в сети радиодоступа E-UTRAN. E-RAB включает в себя виртуальное соединение на радиоинтерфейсе (data radio bearer) и виртуальное соединение на S1 интерфейсе (S1 bearer). В свою очередь E-RAB является частью EPS-bearer. Соответственно, существует однозначный мапинг между E-RAB и EPS-bearer. В полном соответствии с EPS-bearer E-RAB может быть дефолтным (default) или выделенным (dedicated).

***E-RAB ID*** – уникальный идентификатор в диапазоне от 0 до 15, определяющий E-RAB для конкретного пользовательского терминала (UE) внутри S1 соединения. E-RAB ID сохраняется неизменным в течении всего времени жизни E-RAB (даже при освобождении S1 соединения или выполнения S1 хэндовера).

***E-TAS*** – система для оказания различных услуг связи, таких, как: облачная АТС, облачный контакт-центр, сервисы IVR, сервисы исходящего оповещения и информирования, сервисы, использующие распознавание и синтез речи (с использованием внешних движков), услуги технологического соединения абонентов с различной подменой номеров и технических параметров связи, сервисы web-вызовов, конвергентные услуги связи, сервисы с поддержкой HD Voice.

***E-UTRAN (Evolved UMTS Terrestrial Radio Access Network)*** – новое поколение сети радиодоступа стандарта LTE.

***ECT (Explicit Communication Transfer)*** – услуга перевода вызова.

***Emergency numbers*** – номера экстренного вызова.

***EMM (EPS Mobility Management)*** – процедуры для управления мобильностью пользовательского терминала (UE) в сети E-UTRAN. Также EMM обеспечивает управление безопасностью NAS протокола.

**EMM context** – блок информации, устанавливаемый локально в пользовательском терминале (UE) и модуле управления мобильностью (MME) при успешном завершении процедуры регистрации в сети (attach) и включающий в себя в т. ч. глобальный идентификатор UE (GUTI), временные и постоянные идентификаторы UE (P-TMSI, IMSI, IMEI, IMEISV), список идентификаторов зон местоположения (TAI list), таймер периодического обновления местоположения (T3412) и т.д.

**EPC (Evolved Packet Core)** – ядро пакетной сети нового поколения.

**EPS (Evolved Packet System)** – пакетная система нового поколения, включающая в себя ядро пакетной сети нового поколения (EPC - Evolved Packet Core) и сеть радиодоступа нового поколения (E-UTRAN - Evolved Universal Terrestrial Radio Access Network).

**EPS AS security context** – блок информации, включающий в себя в т.ч. криптографические ключи (KeNB, KRRCinc, KRRCenc, KUPinc, KUPenc), параметры Next Hop (NH) и Hop Chaining Counter (NCC), а также идентификаторы используемых алгоритмов для AS шифрования и контроля целостности. EPS AS security context существует только если конфигурация сети предполагает криптографическую защиту на сети радиодоступа.

**EPS NAS security context** – блок информации, включающий в себя KASME, описание возможностей системы безопасности пользовательского терминала (UE), а также uplink и downlink NAS COUNT значения. EPS NAS security context может дополнительно содержать ключи KNASint и KNASenc, а также идентификаторы используемых алгоритмов для NAS шифрования и контроля целостности.

**EPS security context** – блок информации, устанавливаемый локально в пользовательском терминале (UE) и модуле управления мобильностью (MME), и включающий в себя EPS NAS security context и EPS AS security context.

**EPS сервис** – сервис, предоставляемый пакетной сетью (синоним термина GPRS сервис).

**ESM (EPS Session Management)** – процедуры для управления IP связанностью и виртуальными соединениями (bearer) пользовательского терминала (UE).

**etas\_icf** – модуль, который реализует функционал запроса логики обработки вызова из Портала OATC, при подключенной услугой ICF (Intellectual Call Forward).

***EVS (Enhanced Voice Services)*** – кодек с технологией повышения качества передачи голоса.

## F

***FAX (Факс)*** – услуга, которая позволяет принимать документы по факсу. Уведомления обо всех новых факсах приходят по электронной почте с копией факса, а также сохраняются в Облачном хранилище. Формат сохраненного файла tiff.

***Forking*** – это ветвление или распределение одного входящего вызова на несколько зон, чтобы доставить звонок на DEF номер и SIPDef номер одновременно.

## G

***GBR bearer*** – виртуальное соединение (bearer), использующее выделенный сетевой ресурс с гарантированной битовой скоростью (Guaranteed Bit Rate - GBR).

***gRPC*** – это протокол удаленного вызова функций (процедур).

***GRUU (Globally Routable User agent URI)*** – глобальный идентификатор пользовательского устройства в сети IMS.

## H

***Hierarchical call barring*** – позволяет запретить абоненту осуществление исходящих вызовов на определенные направления (by location, by outgoing dial plan).

***HSS (Home Subscriber Server)*** – домашний сервер базы данных пользователя.

***Hunt Group*** – услуга реализует распределение вызова внутри группы, состоящей из нескольких телефонных номеров, по определенному алгоритму.

## I

***I-CSCF (Interrogating CSCF)*** – запрашивающий узел сети IMS. I-CSCF является точкой в сети оператора для всех входящих соединений к абонентам данного оператора. Основная задача, выполняемая I-CSCF – назначение S-CSCF, основываясь на данных, полученных из HSS.

**IBCF (Interconnection Border Control Function)** – узел управления пограничным взаимодействием сети IMS.

**ICS (IMS Centralized Services)** – централизованные сервисы IMS.

**ICSI (IMS Communication Service Identifier)** – идентификатор IMS сервиса электросвязи.

**IM-MGW (IP Multimedia Media Gateway)** – медиашлюз, обеспечивающий передачу данных между подсистемой IMS и доменами с коммутацией каналов сети IMS.

**IMS (IP Multimedia Subsystem)** – IP-мультимедиа подсистема. Спецификация стандартной архитектуры по управлению мультимедийными услугами на основе IP-протокола для сетей следующего поколения (NGN), обеспечивающая конвергенцию услуг передачи речи и данных, предоставляемых различными поставщиками, через общую инфраструктуру IP-сети, а также через различные типы мобильных и фиксированных сетей доступа.

**IMS Core** – ядро IMS, выполняет основную функцию коммутации вызовов.

**IMS-AGW (IMS Access Gateway)** – шлюз доступа сети IMS.

**IMS-AKA (IMS Authentication and Key Agreement)** – процедура аутентификации и согласования секретных ключей.

**IMSI (International Mobile Subscriber Identity)** – международный идентификатор абонента мобильной связи.

**Initial NAS message** – исходное NAS сообщение, устанавливающее NAS сигнальное соединение между UE и MME. Для примера, сообщение ATTACH REQUEST является initial NAS message.

**Intellectual call forwarding (ICF)** – переадресация вызовов в зависимости от условий. В качестве условия переадресации вызова может использоваться день недели, время суток, принадлежность вызываемого абонента к определенному региону, загруженность номеров переадресации и многое другое.

**IP-SM-GW (IP Short Message Gateway)** – узел взаимодействия с SMS сети IMS.

**ISIM (IM Services Identity Module)** – модуль идентификации мультимедийных услуг.

## M

**Media Gateway Control Function (MGCF)** – функция управления шлюзами в подсистеме IMS. Обеспечивает доступ из 2g, 3g сетей в сеть IMS.

**MGCF (Media Gateway Control Function)** – узел управления медиашлюзами IM-MGW сети IMS.

**MMTel (Multimedia Telephony)** – услуга мультимедийной телефонии.

**Mobile Origination (UE-TAS)** – вызывающая сторона. Вызов, адресованный от стороннего пользовательского терминала в сторону абонента oATC.

**Mobile Termination (TAS-UE)** – принимающая сторона. Вызов, адресованный от абонента oATC в сторону какого-либо пользовательского терминала.

**MRFC (Media Resource Function Controller)** – контролер мультимедийных ресурсов сети IMS.

**MRFP (Media Resource Function Processor)** – процессор мультимедийных ресурсов сети IMS.

**MSISDN (Mobile Subscriber ISDN Number)** – мобильный международный номер абонента в сети ISDN.

## N

**non-EPS сервис** – сервис, предоставляемый сетью с коммутацией каналов (CS).

## O

**OCI-P (Open Client Interface - Provisioning)** – основанный на XML протокол запроса-ответа, который позволяет сторонним приложениям выполнять все системные, ресурсные и абонентские действия по предоставлению доступа к VoIP-системе на базе BroadWorks.

**OCS (Online Charging System)** – система тарификации в режиме реального времени.

*OOTB (out of the blue)* – инициация сеанса самой платформой.

## P

*P-CSCF (Proxy CSCF)* – прокси узел сети IMS.

*P-GW (Packet Data Network Gateway)* – шлюз взаимодействия с пакетными сетями.

*PCEF (Police and Charging Enforcement Function)* – узел применения политик сети и правил тарификации.

*PCRF (Police and Charging Rules Function)* – узел функций политик сети и правил тарификации.

*PS (Packet Switched)* – коммутация пакетов.

## Q

*QCI (Quality of Service Class Indicator)* – идентификатор качества передачи пакетов данных.

## R

*RSRP (reference symbol received power)* – уровень мощности референсных символов сети радиодоступа E-UTRAN.

*RSRQ (reference signal received quality)* – уровень качества референсных символов сети радиодоступа E-UTRAN.

*RTCP (RTP Control Protocol)* – протокол управления передачей пакетов данных в реальном времени

*RTP (Real Time Protocol)* – протокол передачи пакетов данных в реальном времени.

## S

*S-GW (Serving Gateway)* – обслуживающий шлюз.

**SAE (System Architecture Evolution)** – архитектура базовой пакетной сети нового поколения.

**SCC-AS (Service Centralisation and Continuity AS)** – сервер централизации и продолжения сервиса. Исполняет функциональность якоря сессии в IMS домене для обеспечения возможности в будущем передачи сессии в домен с коммутацией каналов.

**S-CSCF (Serving CSCF)** – обслуживающий узел сети IMS. S-CSCF является центральной точкой IMS. Он обеспечивает выполнение процедуры регистрации, принятие решение о маршрутизации, управление машиной состояний сессии, хранение профиля пользователя.

**SDP (Session Description)** – протокол, предназначенный для описания сессии передачи потоковых данных, включая телефонию.

**SIP (Session Initiation Protocol)** – протокол инициирования сессий.

**SMSC (Short Message Service Center)** – центр службы коротких сообщений.

**SMSoIP (SMS over IP)** – технология передачи коротких текстовых сообщений через IP сеть.

**SR-VCC (Single Radio Voice Call Continuity)** – технология организации голосовых вызовов, обеспечивающая поддержку непрерывной мобильности пользователя.

**STN-SR (Session Transfer Number for SRVCC)** – номер маршрутизации, идентифицирующий SCC-AS, и используемый для передачи сессии из PS домена в CS домен в рамках процедуры SRVCC; имеет формат E164, включается в абонентский HSS профиль и загружается MME при регистрации пользователя в сети (E-UTRAN attach).

## **T**

**TAI list** – список идентификаторов зон местоположения (Tracking Area Identity) пользовательского терминала (UE), в которых UE может находиться без выполнения процедуры обновления местоположения (tracking area updating). Список зон местоположения (TAI) в TAI list для UE назначает MME.

**TAS (Telephony Application Server)** – сервер телефонных приложений сети IMS.

*TrGW (Transition Gateway)* – транзитный шлюз сети IMS.

## U

*UE (User Equipment)* – пользовательский терминал.

*UICC (Universal Integrated Circuit Card)* – расширенный стандарт микропроцессорной карты.

*UE's usage setting* – индикация возможностей пользовательского терминала (UE) для голосовых сервисов (voice) и сервисов передачи данных (data). Если значение UE's usage setting соответствует "data centric", то пользовательскому терминалу (UE) требуется доступ к сервисам передачи данных и опционально – к голосовым сервисам. Если значение UE's usage setting соответствует "voice centric", то пользовательскому терминалу (UE) требуется доступ к голосовым сервисам и опционально – к сервисам передачи данных.

*UE-ассоциированное логическое S1 соединение* – логическое соединение на S1 интерфейсе, ассоциированное с конкретным пользовательским терминалом UE, и используемое для переноса сигнального трафика S1AP данного терминала. Соединение определяется парой идентификаторов "MME UE S1AP ID" и "eNB UE S1AP ID". Идентификатор "MME UE S1AP ID" используется MME для однозначного сопоставления принятого сообщения конкретному UE. Аналогичным образом используется идентификатор "eNB UE S1AP ID" на базовой станции. Соединение устанавливается при обмене первым S1AP сообщением между сетевыми узлами и может существовать до того, как UE context загружен в eNodeB.

*USSD (Unstructured Supplementary Service Data)* – услуга, позволяющая организовать интерактивное взаимодействие между абонентом сети и сервисным приложением в режиме передачи коротких сообщений.

## V

*VoIP (Voice Over IP)* – семейство технологий, позволяющих обеспечить голосовую связь через IP сеть.

## X

*XCAP (XML Configuration Access Protocol)* – протокол доступа к конфигурации XML.

*XML (eXtensible Markup Language)* – язык для текстового выражения структурированной информации в стандартном виде.