Функциональное предназначение компонентов сети системы мобильной связи стандарта GSM

Кравченко В. И.

2017

План

I. Введение

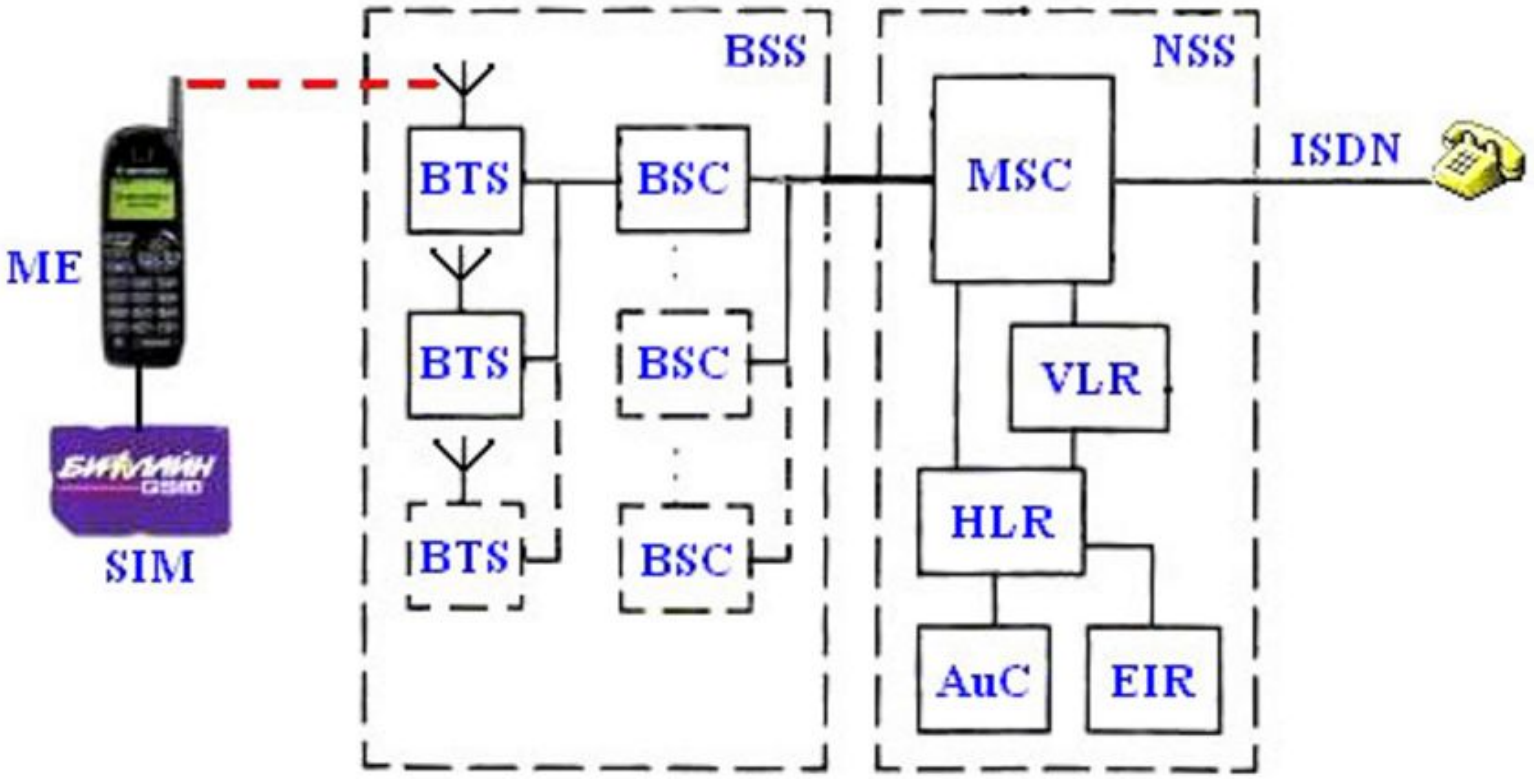
II. Упрощенная архитектура сети GSM
- 2.1. Мобильное устройство
- 2.2. Подсистема базовых станций
- 2.3. Подсистема сети и коммутации

III. Организация установки оборудования

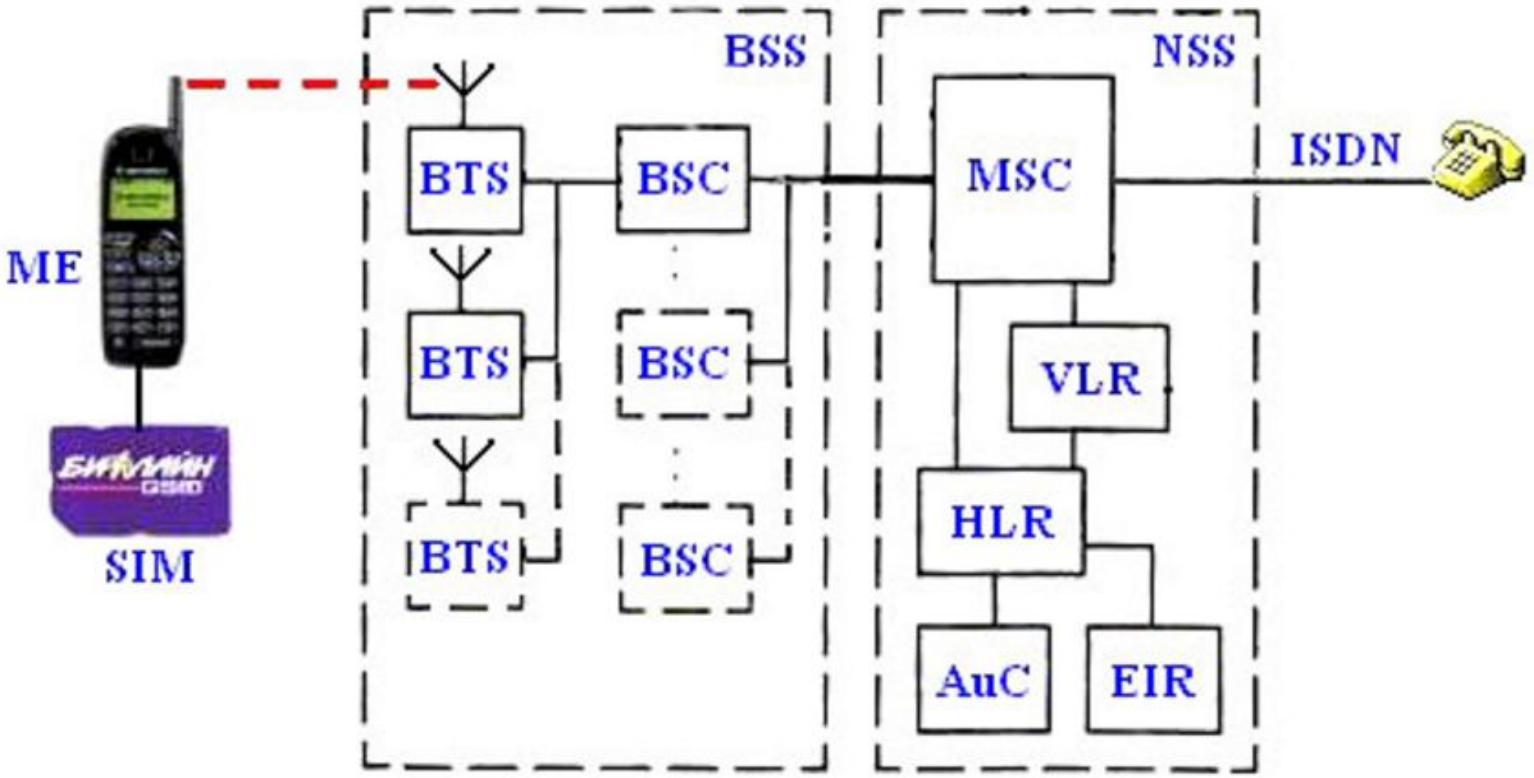
I. Введение

Системы мобильной связи, особенно системы сотовой мобильной связи, наряду с космическими, телевизионными и компьютерными системами, являются одними из важнейших достижений человечества в XX веке в области информационных систем и технологий. Сотовая мобильная связь, появившаяся на уровне идеи в проектах компании Bell System в конце 40-х годов и к 1978 году реализованная в виде первой опытной сети (Chicago, 2000 абонентов), к 2004 году лавинообразно завоевала одну из ключевых позиций в области информационных технологий: на 2004 год во всём мире сотовой мобильной связью было охвачено свыше 1,5 миллиарда пользователей.

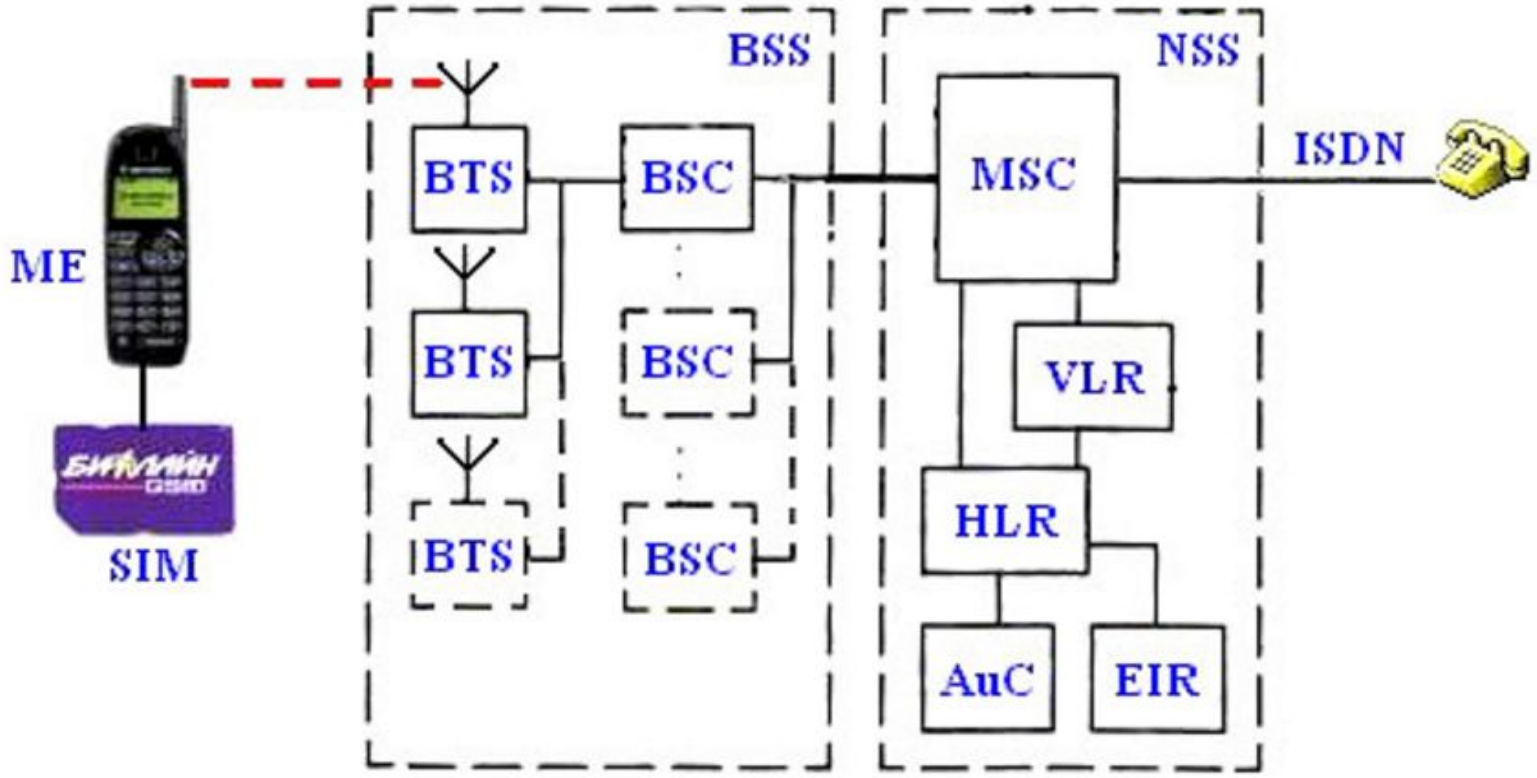
II. Упрощенная архитектура сети GSM



ME (Mobile Equipment) - мобильное устройство.
IMEI (International Mobile Equipment Identity) - международный идентификатор мобильного устройства
SIM (Subscriber Identity Module) - модуль идентификации абонента

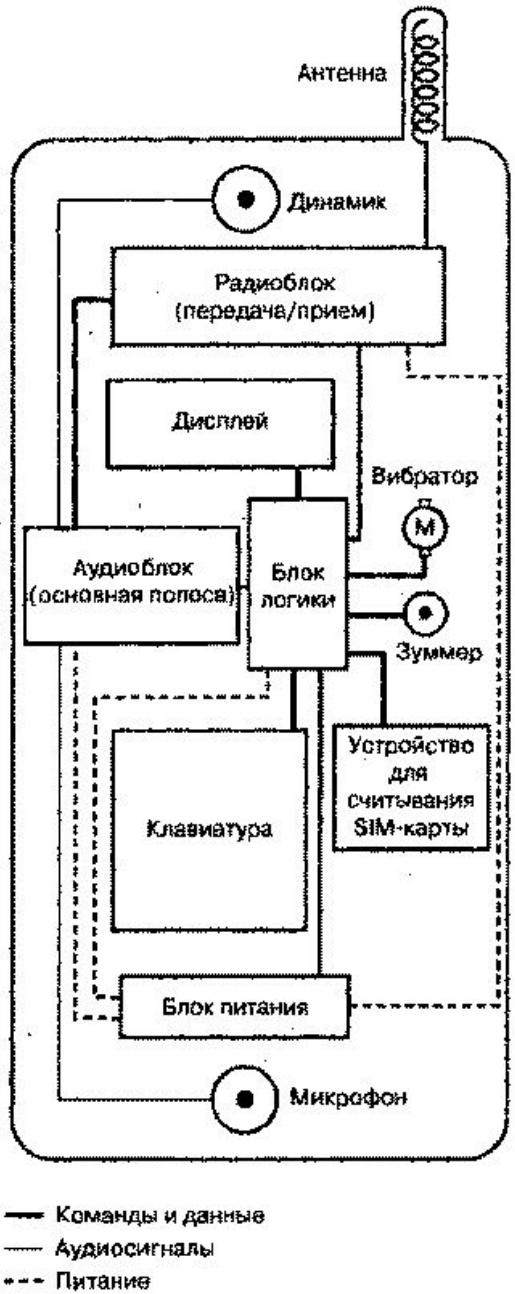


BSS (base station subsystem) - Подсистема базовых станций
BTS (Base Transceiver Station) – базовая станция
BSC (Base Station Controller) - Контроллер базовых станций

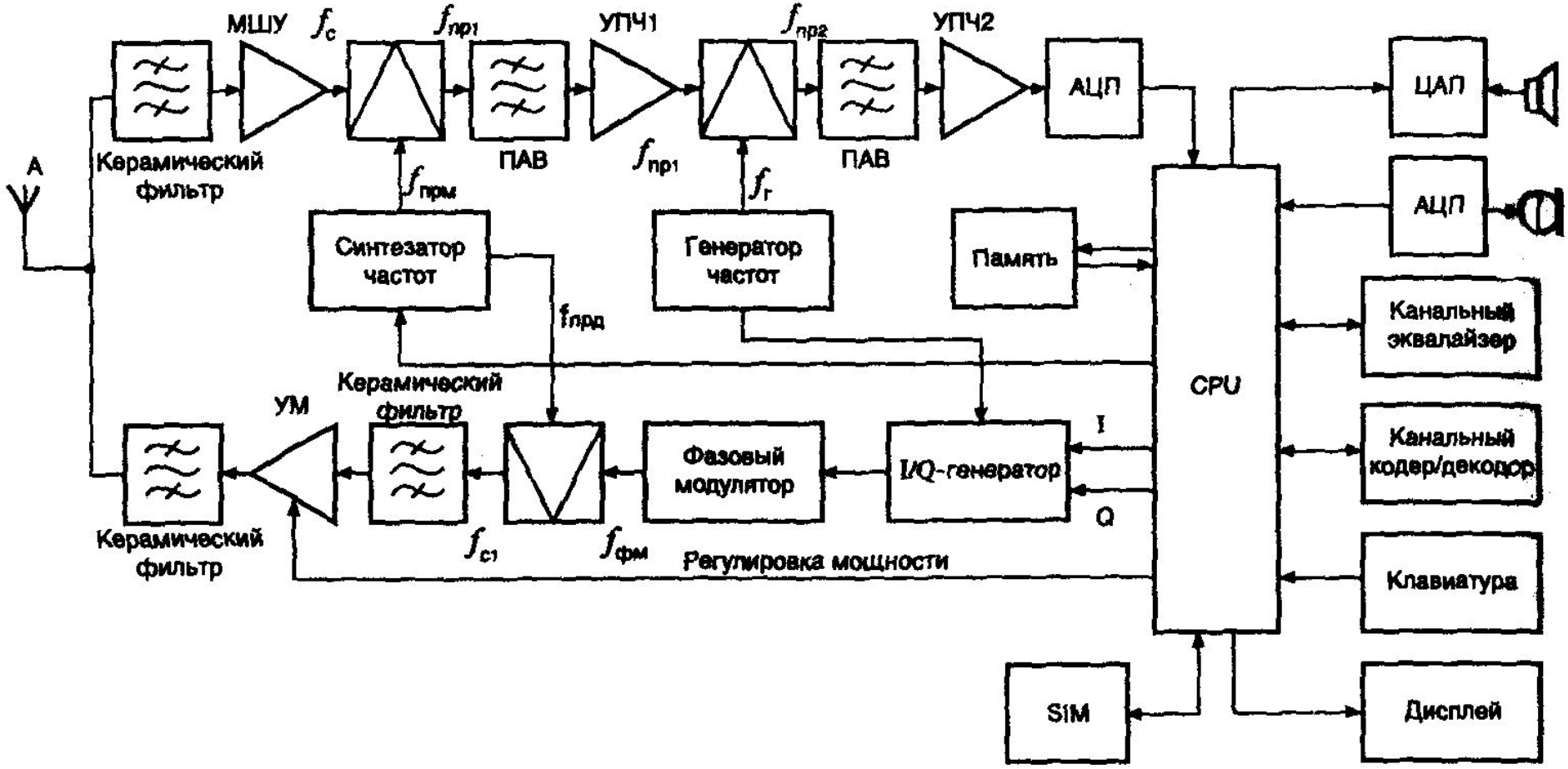


NSS (Network and Switching Subsystem) - подсистема сети и коммутации
MSC (Mobile services Switching Center) - центр коммутации
VLR (Visitor Location Register) - реестр перемещений («временных» абонентов)
HLR (Home Location Register - реестр собственных абонентов)
AuC (Authentication Center) - центр аутентификации
EIR (Equipment Identity Register) - реестр идентификации оборудования

2.1. Мобильное устройство



Структурная схема мобильного телефона системы GSM



Структурная схема цифрового радиотелефона

Основные производители мобильных процессоров:

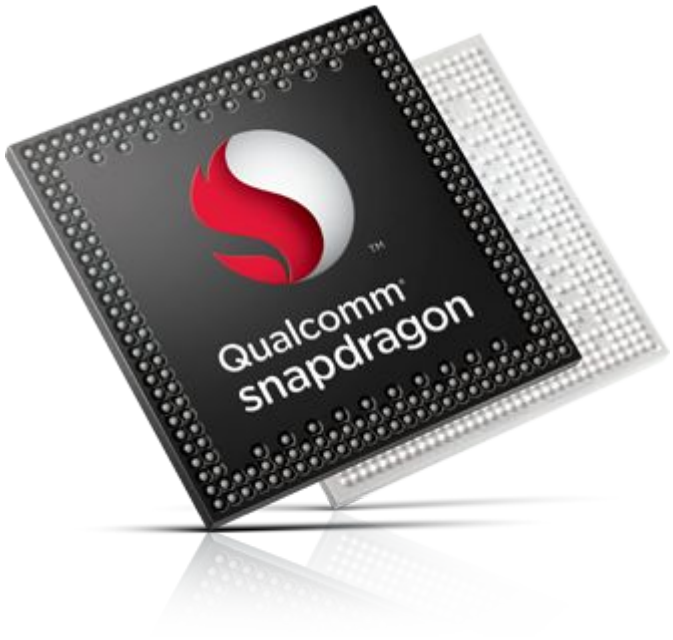
1. Qualcomm
2. MediaTek
3. Apple

Qualcomm Inc.— компания по разработке и исследованию беспроводных средств связи, а также SoC
Компания основана в 1985 году.
Производство: CDMA Chipsets, BREW, Eudora, OmniTRACS, MediaFLO, QChat, uiOne.

В 2005 году, лицензировав у компании ARM её процессорное ядро Cortex A8, компания Qualcomm разработала на его основе собственный микропроцессор для мобильных телефонов на ядре Scorpion. Чип полностью поддерживает набор инструкций ARMv7, используемый в Cortex A8, но является доработанным по сравнению с базовым ядром ARM. Scorpion работает на более высокой частоте, 1 ГГц и потребляет при этом вдвое меньше электроэнергии. Процессор выпускается по технологии 65 нм.

Характеристики передового процессора компании Snapdragon 830:

Техпроцесс: 10-нм FinFET Samsung
Ядра: Kryo 200
GPU: Adreno 540, частота 670 МГц
Память LPDDR4X 2133 МГц
Цифровой сигнальный процессор Hexagon 780 QDSP6 V7, 4-потоковый, с частотой потока 550 МГц или 600 МГц
Модем X16 LTE. Максимальная скорость передачи данных составляет 980 Мбит/с.
Технология быстрой зарядки Qualcomm Quick Charge 4.0



MediaTek Inc. — бесфабричная полупроводниковая компания, занимающаяся разработкой компонентов для беспроводной связи, оптических систем хранения данных, GPS, HDTV, DVD. Компания основана 28 мая 1997 года. Штаб-квартира расположена в Индустриальном и научном парке Синьчжу (Тайвань); подразделения существуют в Китае, Дании, ОАЭ, Индии, Японии, Южной Корее, Сингапуре, Великобритании, США и Швеции.

Они первые разработали 10-ядерный процессор под названием Xelio X20. На данный момент — это самая мощная однокристальная система в мире.

Характеристики передового процессора компании Helio X30 MT6799:

Техпроцесс: 10 нм FinFET

Десятиядерный2 ядра Cortex-A73 2,5ГГц
4 ядра Cortex-A53 2,2ГГц
4 ядра Cortex-A53 1.9ГГц

GPU: PowerVR 7400XT MP4 800 МГц
Память: LPDDR4X 1866МГц
Переферия: Камеры до 28 Мп (с двумя ISP с Imagiq 2.0) Макс. разрешение записи видео: 4K 3840×2160 Дисплей с разрешением до 2560x1600 точек LTE Cat. 10 с агрегацией частот 3CA Hi-Fi & 4-Mic ANC Audio Codec

Установлен в: Meizu Pro 7

Apple Inc. — американская корпорация, производитель персональных и планшетных компьютеров, аудиоплееров, телефонов, программного обеспечения. Один из пионеров в области персональных компьютеров и современных многозадачных операционных систем с графическим интерфейсом. Штаб-квартира — в Купертино, штат Калифорния.

Характеристики передового процессора компании Apple A10 Fusion:

Техпроцесс: 16 нм
64-битный 4-ядерный ARM-микропроцессор с архитектурой ARMv8-A

GPU: PowerVR GT7600

Технология памяти:
2 ГБ LPDDR4 у iPhone 7 и 3 ГБ LPDDR4 у iPhone 7 Plus

Установлен в: iPhone 7, iPhone 7 Plus

Сотовый телефон - сложное высокотехнологичное электронное устройство, включающее в себя: приёмопередатчик на поддиапазоны 1-2 ГГц (GSM) и 2-4 ГГц (UMTS) СВЧ-диапазона, специализированный контроллер управления, дисплей, интерфейсные устройства, аккумулятор.

IMEI - это уникальный серийный номер каждого телефона формата GSM, который автоматически передается аппаратом в сеть оператора при подключении. То есть если в ваш украденный сотовый телефон кто-то вставит свою сим-карту и сделает хотя бы один звонок, силовые структуры через оператора связи могут узнать, на кого оформлена сим-карта, и изъять телефон. Однако перед этим он может пылиться в витринах какого-нибудь магазина месяцами.

Код IMEI состоит из 15-и цифр

Первые 6 цифр
TAC (Type Approval Code) - утвержденный код типового образца, модели телефона (первые 2 цифры - код страны).
Далее 2 цифры
FAC (Final Assembly Code) - код страны финальной сборки:
6 цифр
SNR (Serial Number) - серийный номер
1 цифра
SP (Spare) - запасной, практически всегда = 0.

С 1 января 2003 года была принята новая структура IMEI. Современная структура IMEI

TAC — Type Allocation Code		Serial No	Check Digit
Reporting Body Identifier	Type Identifier	Serial number	Check Digit
NN	XXXX XX	ZZZZZZ	A
Типовой код распределения		Серийный номер	Проверочный код

SIM-карта - идентификационный модуль абонента, применяемый в мобильной связи.

Основная функция SIM-карты — хранение идентификационной информации об аккаунте, что позволяет абоненту менять сотовые аппараты, не меняя при этом свой аккаунт.

SIM-карта включает в себя микропроцессор с ПО и данные с ключами идентификации карты (IMSI, Ki и т. д.), записываемые в карту на этапе её производства, используемые на этапе идентификации карты (и абонента) сетью GSM.

Также SIM-карта может хранить дополнительную информацию, например:

- телефонную книжку абонента
- списки входящих/исходящих/пропущенных телефонных звонков
- текст входящих/исходящих SMS.

SIM-карта содержит микросхему памяти, поддерживающую шифрование. Существуют карты различных стандартов, с различным размером памяти и разной функциональностью. Есть карты, на которые при производстве устанавливаются дополнительные приложения (апплеты), такие как SIM-меню, клиенты телебанка, и т. д.

На самой карте телефонный номер абонента (MSISDN) в явном виде не хранится, он присваивается сетевым оборудованием оператора при регистрации SIM-карты в сети на основании её IMSI. По стандарту при регистрации одной SIM-карты в сети оператор может присвоить ей несколько телефонных номеров. Однако эта возможность требует соответствующей поддержки инфраструктурой оператора (и соответствующих затрат с его стороны), поэтому чаще всего не применяется.

Контакты SIM-карты

Используемые контакты:

C1 — Vcc — питание;

C2 — Reset – контакт управления картой;

C3 — CLK — Clock – тактовая частота;

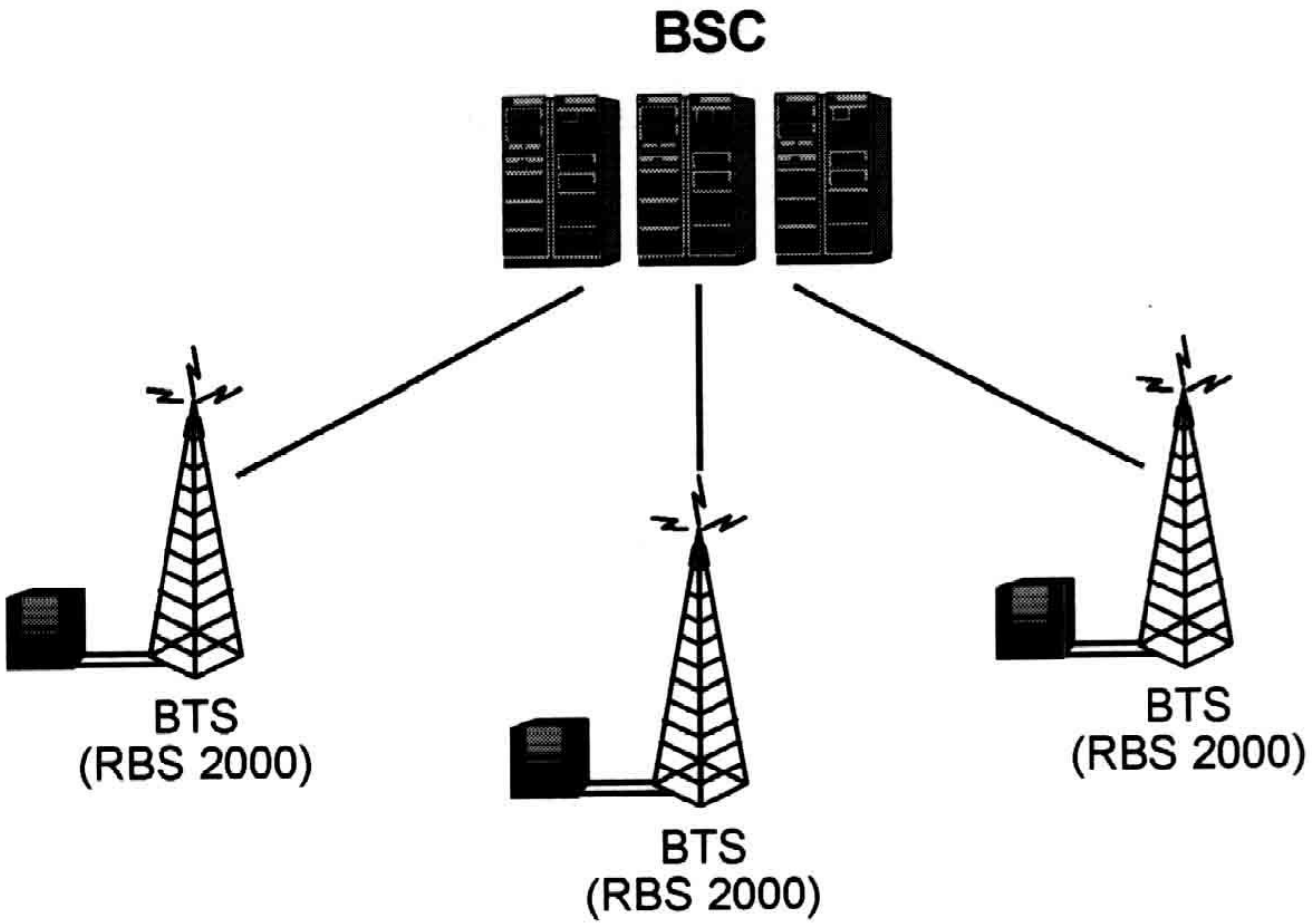
C5 — общий («земля»);

C6 — Vpp – напряжение программирования, которое используется при записи служебной информации

C7 — I/O – линия последовательного интерфейса ввода/вывода.

2.2. Подсистема базовых станций

BSS - один из основных элементов системы подвижной радиотелефонной связи, ответственный за передачу голосового и сигнального трафика между мобильным терминалом абонента и подсистемой сети и коммутации, GSM core network. ПБС занимается кодировкой голосовых каналов, назначением радиоканалов телефонным терминалам, функциями пейджинга, контролем качества передачи данных, осуществляет приём и передачу сигналов в воздушной среде и выполняет множество других задач, связанных с функционированием сети.



Базовая станция

Включает в себя приёмо-передающие антенные устройства, оборудование для ретрансляции радиосигнала (Трансивер), блоки шифрования данных. БС обслуживает отдельный участок сети с помощью нескольких нацеленных в различные участки сектора трансиверов (TRX), осуществляющих вещание на разных частотах.


TMU
PSU
PMU

Функции:

Обеспечение связи с контроллером базовых станций BSC по интерфейсу Abis

Радиоинтерфейс с MS (интерфейс Um)

Управление радиоканалами

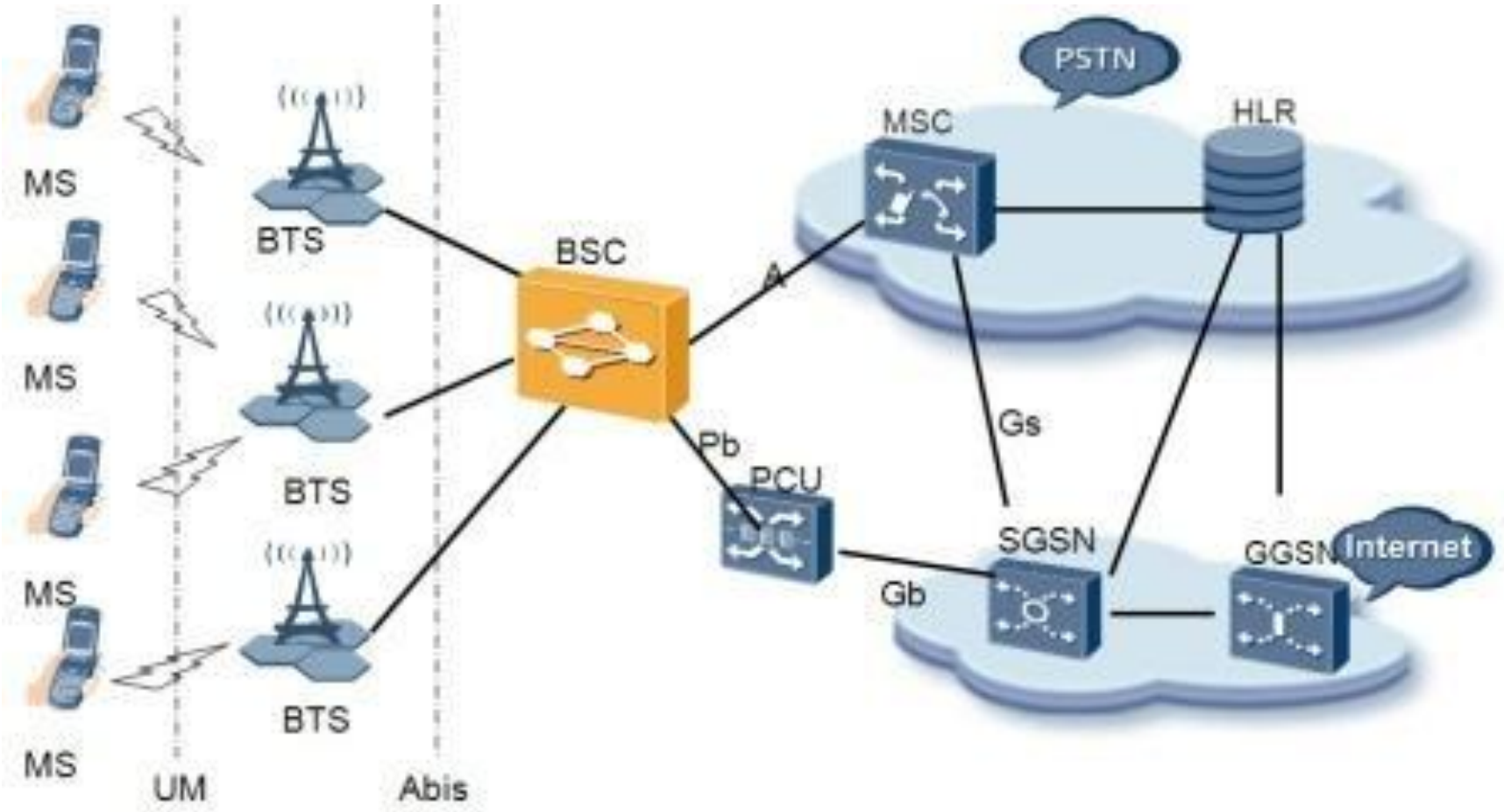
Обработка речевого сигнала

Управление звеном сигнализации

Техническое обслуживание

Синхронизация

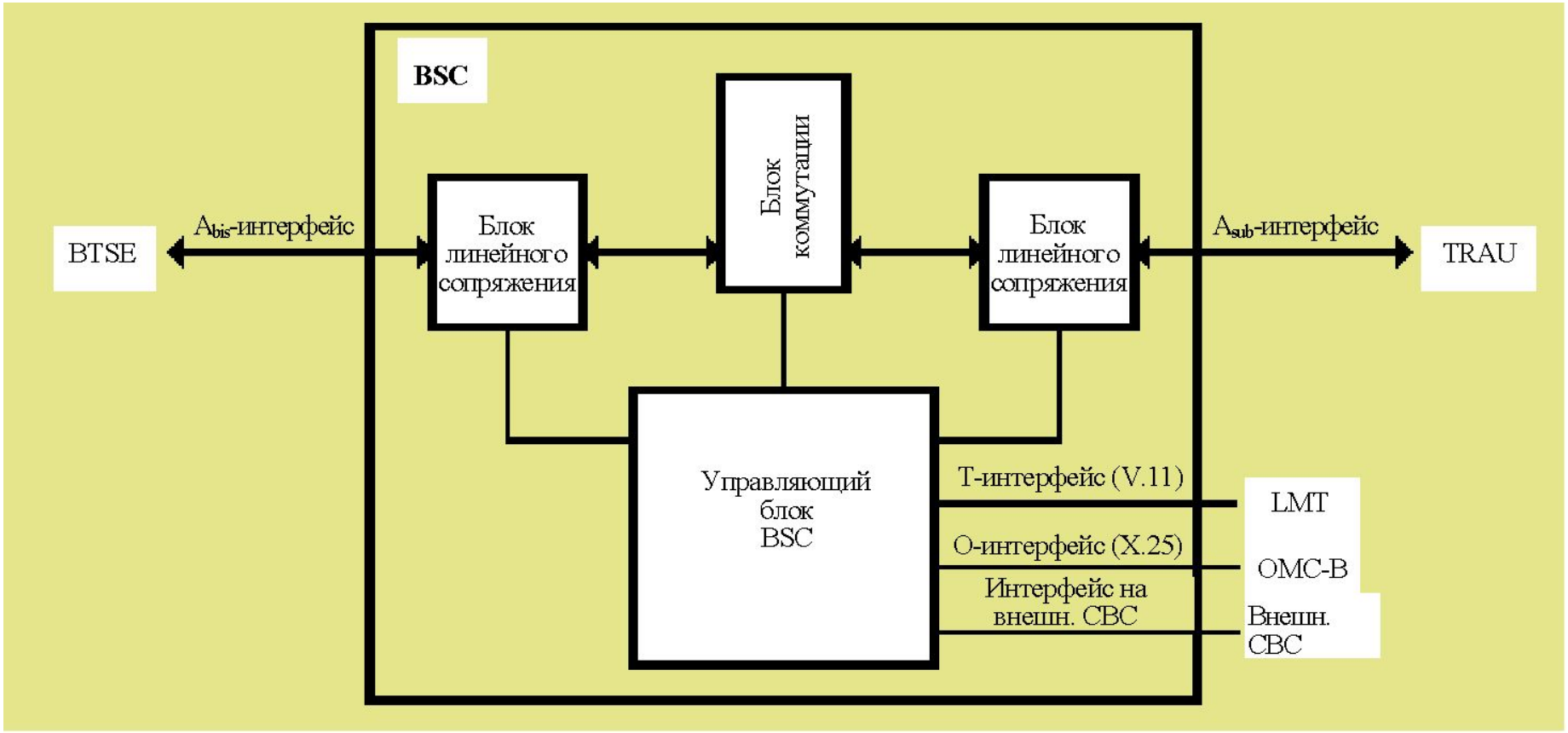
Контроллер базовых станций



Функции:

1. Переключение и освобождение разговорных каналов между MSC (коммутатором) и BTS (базовой станцией).
2. Управление процедурой Frequency hopping (перескоки разговорного канала по частоте в радиоинтерфейсе).
3. Уведомление мобильной станции о поступившем вызове (Paging).
4. Управление уровнями излучаемой мощности мобильной и базовой станции во время разговора при изменении условий приёма.
5. Наблюдение за качественными характеристиками радиосигнала во время разговора (качество, уровни приёма, интерференция и др.).
6. Управление эстафетной передачей разговора от одной базовой станции к другой при перемещении абонента либо при изменении радиообстановки без прерывания разговора (Handover control).
7. Обслуживание BTS / BSC / TCSM — установка и обновление ПО на элементы BSS, мониторинг и устранение аварийных ситуаций, изменение логического состояния элементов, тестирование оборудования BSS.
8. Поддержка интерфейсов на NMS / BTS / TCSM / SGSN.

BSC поддерживает полноскоростной и полускоростной режим работы. Модернизация для обеспечения полускоростного режима работы влияет на все основные функциональные компоненты BSC.

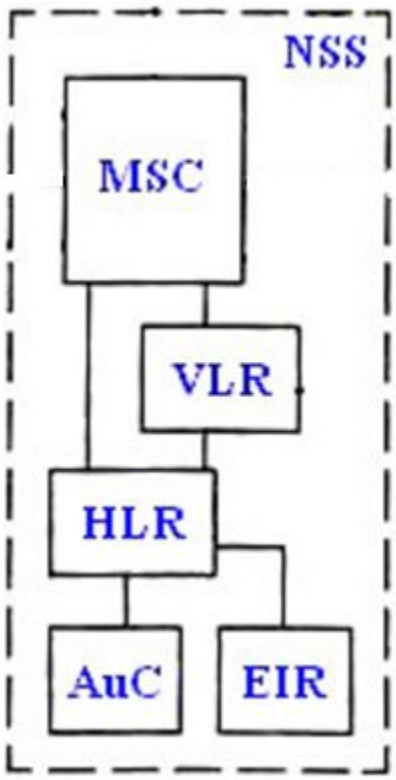


Функциональная структура BSC.

BSC состоит из:

- управляющего блока
- устройства линейного сопряжения
- блока коммутации

Подсистема сети и коммутации



Функции центра коммутации подвижной связи (MSC)
MSC является программно-управляемым цифровым коммутатором. MSC – это коммутатор PLMN в системе GSM, который:

– выполняет обработку вызовов
– выступает в качестве шлюза по отношению к другим сетям,
– подключаем к другим центрам MSC в сетях PLMN стандарта GSM,
– соединяет сетевые элементы SSS с сетевыми элементами BSS в зоне обслуживания PLMN стандарта GSM.

MSC имеет функции, которые присущи коммутаторам в фиксированных сетях, и специальные функции, которые не являются обязательными для коммутаторов фиксированных сетей. Специальные функции подвижной связи связаны с мобильностью абонента.

Основными функциями MSC являются, например:

– выбор маршрутов

(среди прочих функция "резервирования соединительной линии" позволяет резервировать каналы передачи для маршрутизации вызовов служб экстренной помощи, посылаемых в центры вызова служб экстренной помощи)

– установление соединений по каналу трафика и сигнализации
– контроль соединений
– учет сообщений
– управление данными по трафику (например, измерение трафика)
– управление перегрузкой
– дополнительные телекоммуникационные услуги
– санкционированное прослушивание (перехват)
– учет начисления платы

Расширенными функциями маршрутизации вызовов, тарификации и информации о пользователях, например, являются:

– гибкая маршрутизация вызовов в подсистеме коммутации (по номеру)
– маршрутизация по IMSI/MSISDN
– маршрутизация по данным абонента GSM
– генерация данных о начислении платы для абонентов GSM
– многоязычные объявления

Специальными функциями подвижной связи центра MSC являются:

– расширение базовых функций сети PLMN стандарта GSM (например, сотовоориентированная маршрутизация служебных номеров; маршрутизация служебных номеров, связанная с абонентом GSM)

– управление мобильностью:

опрос,

персональный вызов,

эстафетная передача,

корректировка местоположения

– управление ресурсами (например, поддержка полускоростного режима передачи, установление соединения без занятия радиоканала и т.п.)

– объединение средств для выделения канала на A-интерфейсе

– доступ к базам данных PLMN стандарта GSM (VLR, GCR, HLR, EIR)

– специальные функции обеспечения безопасности (например, проверка IMEI)

– управление постановкой в очередь по уровням приоритета для BSS

– функция межсетевого взаимодействия (IWF) для информационных услуг системы GSM

– функции защиты от несанкционированного пользования

– функции расширения емкости

Функции визитного регистра положения (VLR)

VLR (англ. *Visitors Location Register*) — временная база данных абонентов, которые находятся в зоне действия определённого центра мобильной коммутации. Каждая базовая станция в сети приписана к определённому VLR, так что абонент не может присутствовать в нескольких VLR одновременно.

В регистре VLR осуществляется регистрация всех абонентов GSM, находящихся в зоне его обслуживания. Пока абонент GSM находится в пределах зоны обслуживания, VLR содержит все параметры абонента GSM, необходимые для выполнения функций по управлению вызовами.

Функции по управлению вызовами

Функции по управлению вызовами включают адресацию и идентификацию.

Адресация и идентификация выполняется посредством следующих идентификаторов:

– международный идентификатор подвижного абонента (IMSI)
– местный идентификатор подвижного абонента (LMSI)
– номер подвижной станции в роуминге (MSRN)
– временный идентификатор подвижного абонента (TMSI) вместе с идентификатором зоны расположения (LAI)

Обеспечение конфиденциальности идентификации подвижного абонента не позволяет постороннему лицу идентифицировать подвижного абонента GSM и установить его местоположение с помощью процедуры радиоперехвата. В этих целях VLR создает TMSI, соответствующий IMSI, который является уникальным для VLR и передается по радиоинтерфейсу.

Установление соединения

В MSC функция установления соединения инициируется MS через MSC, чтобы отыскать необходимые параметры подвижного абонента GSM из VLR. Подвижный абонент GSM идентифицируется по IMSI или TMSI.

Регистрация местоположения

Функция регистрации местоположения включает процедуры для:

– корректировки местоположения
– отмены местоположения

Процедура корректировки местоположения инициируется MS через MSC при изменении зоны расположения MS или по истечении заданного времени. Эта процедура определяет местоположение абонента GSM (адрес VLR) для HLR и параметры аутентификации абонента GSM для соответствующего VLR.

Процедура отмены местоположения инициируется HLR, если абонент GSM покидает зону обслуживания VLR. Оператор также имеет возможность стереть информацию об абоненте GSM в VLR с помощью команд MML.

HLR (англ. Home Location Register) — база данных, которая содержит информацию об абоненте сети GSM-оператора.

HLR содержит данные о SIM-картах данного оператора мобильной связи. Каждой SIM-карте сопоставлен уникальный идентификатор, называемый IMSI, который является ключевым полем для каждой записи в HLR.

К основным функциям HLR относятся:

· **Управление базой данных, содержащей всю информацию об абонировании абонентов**. Поскольку HLR является базой данных, он должен располагать способностью в ответ на запрос на предоставление данных обрабатывать данные с большой скоростью, а также обновлять запросы от других сетевых узлов. По этой причине HLR действует как система управления базой данных. Каждая абонентская запись содержит большое количество важных параметров.

· **Связь с MSC**. HLR должен быть способным при установлении соединения с MS связываться с MSC, обслуживающим данную MS, для получения необходимой информации о маршрутизации вызова. MSC путем анализа MSISDN узнает о том, с каким именно HLR, находящимся в любой точке глобальной сети GSM, необходимо связаться для получения информации об абоненте.

· **Связь с GMSC.**GMSC в процессе установления соединения с MS запрашивает из HLR информацию о местонахождении MS, HLR предоставляет эту информацию в форме информации для маршрутизации вызова. Если MS находится в отключенном состоянии (DETACHED), HLR проинформирует GMSC о том, что нет необходимости осуществлять дальнейшую маршрутизацию вызова. Посредством анализа IMSI, GMSC знает, какой HLR из всей мировой сети, контролирует данную MS.

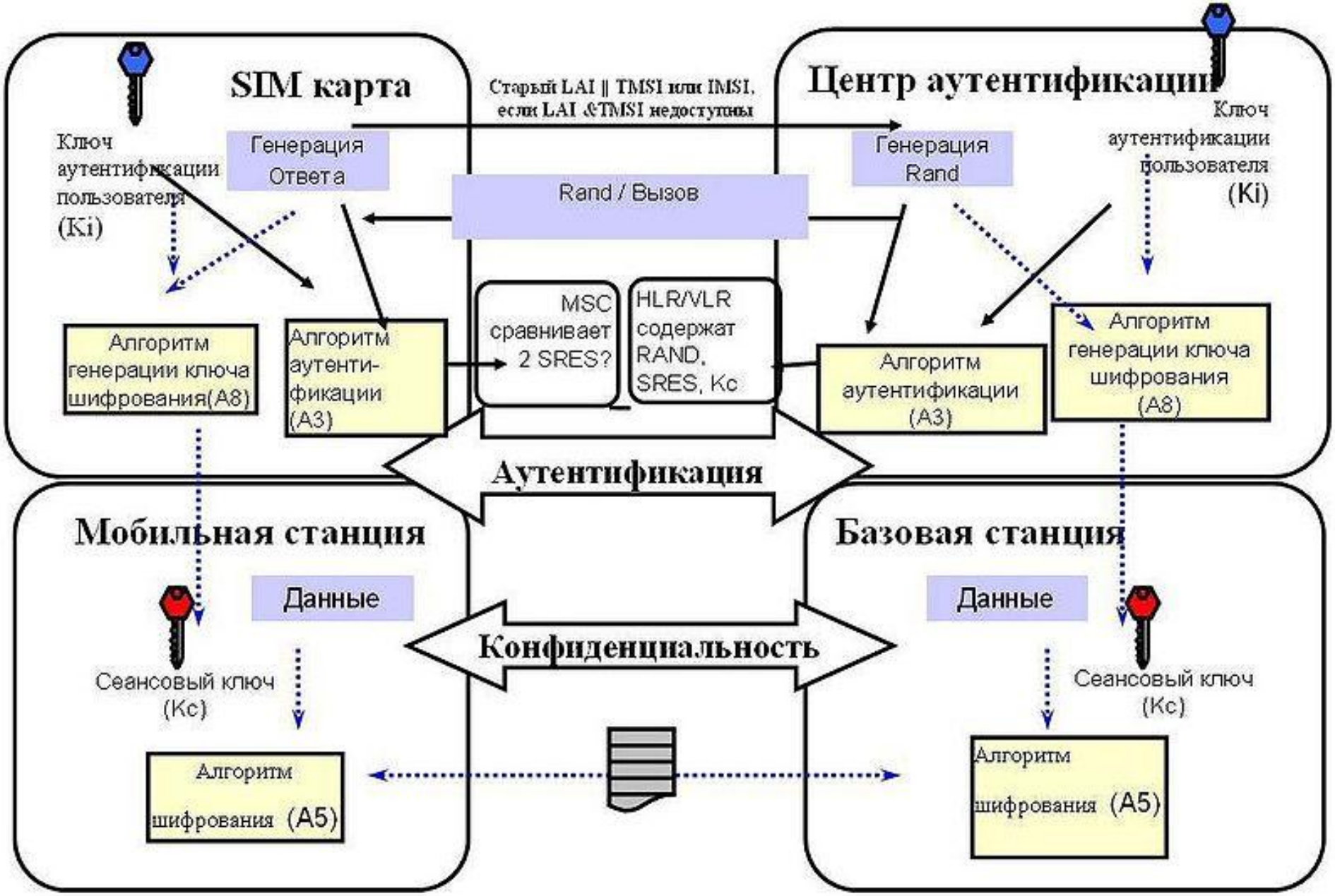
· **Связь с AUC**. HLR до того, как будет предпринято какое-либо действие по использованию абонентской информации или по внесению в нее изменений, должен получить новые аутентификационные параметры из AUC.

· **Связь с VLR/ILR.**Когда MS входит в зону обслуживания нового MSC, отвечающий за эту зону обслуживания VLR осуществляет запрос информации о MS из HLR, в котором хранятся данные абонента, использующего эту MS. HLR обеспечивает VLR копией информации об абоненте, обновляет у себя информацию о местонахождении абонента и инструктирует VLR, в котором ранее хранилась информация об абоненте, о необходимости удаления информации об этом абоненте.

HLR может быть реализован в том же сетевом узле, что и MSC/VLR, а может быть реализован в качестве отдельного аппаратного узла. Конкретная реализация зависит от емкости сети.

Центр аутентификации (*AuC*, англ. *Authentification Center*) предназначен для аутентификации каждой SIM карты которая пытается присоединиться к GSM-сети (обычно когда телефон включается). Как только аутентификация успешно завершается, HLR может управлять сервисами, на которые подписался абонент (SIM). Также генерируется шифровальный ключ который периодически используется для шифрования беспроводного соединения (голосового, SMS) между мобильным телефоном и базовой сетью.
Если аутентификация проходит неудачно, для данной SIM-карты услуги в данной сети предоставляться не будут. Возможна дополнительная идентификация мобильного телефона по его серийному номеру (IMEI) с помощью EIR (англ. *Equipment Identification Register* — реестра идентификации оборудования), но это уже зависит от настроек аутентификации в AuC.

Первичной функцией AUC является предоставление информации, которая будет использоваться MSC/VLR для выполнения аутентификации абонента и выполнения процедур кодирования информации, передаваемой по радиоканалу между сетью и MS.


SIM карта
Старый LAI || TMSI или IMSI, если LAI &TMSI недоступны
Центр аутентификации
Ключ аутентификации пользователя (Ki)
Генерация Ответа
Rand / Вызов
Генерация Rand
Ключ аутентификации пользователя (Ki)
Алгоритм генерации ключа шифрования(A8)
Алгоритм аутенти-фикации (A3)
MSC сравнивает 2 SRES?
HLR/VLR содержат RAND, SRES, Kc
Алгоритм аутентификации (A3)
Алгоритм генерации ключа шифрования (A8)
Аутентификация
Мобильная станция
Базовая станция
Данные
Данные
Конфиденциальность
Сеансовый ключ (Kc)
Сеансовый ключ (Kc)
Алгоритм шифрования (A5)
Алгоритм шифрования (A5)

На данном рисунке схематично представлены следующие шаги:
Телефон оператора подключается к сети.
Для подтверждения своей подлинности телефон посылает специальный идентификационный код, называемый TMSI(Temporary Mobile Subscriber Identity).
Центр Аутентификации(ЦА) генерирует 128-битное случайное число RAND и посылает его на Мобильную Станцию(МС).
МС зашифровывает полученное число RAND, используя свой секретный ключ K_i и алгоритм аутентификации A3.
МС берет первые 32 бита из последовательности, полученной на предыдущем шаге (назовем их SRES(signed response)) и отправляет их обратно на ЦА.
ЦА проделывает ту же операцию и получает 32 битную последовательность XRES(expected response).
После чего ЦА сравнивает SRES и XRES. В случае, если оба значения равны, телефон считается аутентифицированным.
МС и ЦА вычисляют сессионный ключ шифрования, используя секретный ключ K_i и алгоритм формирования ключа A8 $K_c=A8_{ki}(RAND)$

В EIR хранятся три списка (белый, серый и черный) с IMEI (international mobile equipment identity) - идентификаторами оборудования абонентов. Наличие IMEI в белом списке разрешает доступ в сеть безоговорочно. Оборудование из серого списка будет допущено в сеть, но будет непрерывно отслеживаться во время его нахождения в сети. Черный список предназначен для хранения IMEI аппаратов, которым в сеть доступ запрещен. Исходя из этого, назначение EIR очевидно: оказать помощь правоохранительным органам в поиске и отслеживании абонентов и украденного оборудования.

Во всем мире лишь один оператор установил EIR на своей сети. Причина такой непопулярности заключается в высокой стоимости оборудования, что, естественно, не выгодно операторам сотовой связи. Попытки обязать операторов устанавливать EIR предпринимались в разных странах, однако остались тщетными. Еще одной причиной, почему EIR не используется в нашей и большинстве других стран – это установка на сеть другого специализированного оборудования, получившего в русском языке название СОРМ (система оперативно-розыскных мероприятий). Этот элемент никак не описан в телекоммуникационных спецификациях 3GPP, IMT и т.п., и стандартизируется специальными отраслевыми документами. СОРМ предоставляет гораздо больше возможностей по слежению за абонентами для правоохранительных служб. Его установка в России обязательна для всех операторов сотовой связи.

III. Организация установки оборудования


GSM五期
仕版
cell 1
N120°
下傾6°
2006.3.21.


13/10/2014 12:40