МИНИСТЕРСТВО ПО РАЗВИТИЮ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И КОММУНИКАЦИЙ РЕСПУБЛИКИ УЗБЕКИСТАН

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ИМЕНИ МУХАММАДА АЛ-ХОРАЗМИЙ

Ибраимов Р.Р., Пулатов Ш.У., Хатамов А.П., Мадаминов Х.Х.

Учебник по курсу

GSM и управление мобильностью

для специальности 5А350901 –Мобильные системы связи

Ташкент 2020

УДК: 621. 396. 218: 004.738. 5 (075) С 748

Авторы: Ибраимов Р.Р., Пулатов Ш.У., Хатамов А.П., Мадаминов Х.Х.

Учебник по курсу «GSM и управление мобильностью». Для специальности 5А350901 –Мобильные системы связи / ТУИТ. Ташкент 2020.

Рассматриваются основы построения и архитектура сети связи стандарта GSM. Приводятся основные понятия, термины, параметры сети связи, процедуры управления мобильностью, задачи системы сетевого планирования, идентификаторы, варианты сценариев обслуживания вызовов, аспекты безопасности, протоколы сети, частотный план и структура кадров в стандарте GSM. Также рассматриваются методы обработки речи и проблемы, возникающие при передаче радиосигналов. Отмечены выборы видов мобильных приложений и их применение в стандарте GSM.

Учебник предназначен для магистрантов, обучающихся по специальности 5А350901 –Мобильные системы связи, а также он может быть полезен для инженерно-технических работников, специализирующихся в области беспроводных систем связи.

GSM aloqa tarmog'i arxitekturasi va qurilish tamoyillari ko'rib chiqilgan. GSM standartida asosiy tushunchalar, atamalar, aloqa tarmog'ining parametrlari, mobillikni boshqarish jarayonlari, tarmoqni loyihalashtirish tizimining vazifalari, identifikatorlar, qo'ng'iroqlar bilan ishlash ssenariylari, xavfsizlik jihatlari, tarmoq protokoli, chastotani loyihalashtirish va kadrlar tuzilishi berilgan. Shuningdek, nutqni qayta ishlash usuli va radiosignallarini uzatishdagi muammolari muhokama qilinadi. Mobil ilovalarning turlarini tanlash va ulardan GSM standartida foydalanish qayd etilgan.

Darslik 5A350901 - Mobil aloqa tizimlari mutaxassisligi bo'yicha tahsil olayotgan magistrlar uchun mo'ljallangan, shuningdek simsiz aloqa tizimlariga ixtisoslashgan muhandis va texnik xodimlar uchun ham foydali bo'lishi mumkin.

The fundamentals of construction and architecture of a GSM standard communication network are considered. The basic concepts, terms, parameters of the communication network, mobility management procedures, tasks of the network planning system, identifiers, scenarios of call servicing, security aspects, network protocols, frequency plan and frame structure in the GSM standard are given. It also discusses speech processing techniques and problems encountered in transmitting radio signals. Elections of types of mobile applications and their application in the GSM standard are noted.

The textbook is intended for undergraduates studying in the specialty 5A350901 - Mobile communication systems, and it can also be useful for engineering and technical workers specializing in the field of wireless communication systems.

Рецензенты:

Профессор кафедры «РТУиС»,
д.т.н. ТашГТУ имени И. Каримова — А.М. Назаров

Доцент кафедры «ТМС»,
к.т.н. ТУИТ имени Мухаммада аль-Хорезмий — А.Х.Абдукадыров

Редактор:

Профессор кафедры «ТМС»,
академик Уз.А.Н, д.ф.м.н..
ТУИТ имени Мухаммада аль-Хорезмий — Т.Д. Раджабов

Ташкентский университет информационных технологий
имени Мухаммада ал-Хоразми, 2020

СОДЕРЖАНИЕ

Mundarija

ПРЕДИСЛОВИЕ

Учебник состоит из введения, 6 глав, заключения, глоссария терминов по мобильным системам связи и списка использованной литературы. В первой главе читатель знакомится с основными компонентами, принципами построения и характеристики стандарта GSM, во второй с особенностями управления мобильностью, приводятся варианты сценариев обслуживания вызовов. В третьей главе рассмотрены аспекты безопасности, протоколы сети, частотный план и структура кадров в стандарте GSM. Четвертая глава посвящена обработке речи в стандарте GSM и проблемам, возникающим при передаче радиосигналов. В пятой главе показывается, как происходит управление сетями связи в стандарте GSM и в шестой обсуждается мобильное приложение, разработанное для стандарта GSM, и приводятся примеры их использования.

Предназначается для магистров по специальности А5350901студентов, изучающих соответствующий курс, а также может быть полезен для инженерно-технических работников, специализирующихся в системах мобильной радиосвязи.

ВВЕДЕНИЕ

Характерная черта современного мира — широкое использование подвижной связи. В настоящее время в большинстве стран количество абонентов подвижной связи превосходит количество абонентов стационарной сети. Уже многие абоненты отказываются от стационарной связи, несмотря на то, что пока она имеет некоторые преимущества по надежности и качеству услуг, в основном в части широкополосной сети и возможностей мультимедиа.

Надежность сотовой связи и ее качество в настоящее время зависит от местности, погодных и радиоэлектромагнитных условий. Поэтому абонент не всегда может быть уверен, что связь будет предоставлена в любом месте и в любое время.

Потребность в совершенствовании качества информационных услуг и телекоммуникационных систем в период экономического роста возрастает. Этому также свидетельствует ряд Указов и Постановлений Президента Республики Узбекистан, в том числе Указ президента Республики Узбекистан №УП-4947 от 07.02.2017 г., Указ президента Республики Узбекистан №УП-5349 «О стратегии действий по дальнейшему развитию Республики Узбекистан». «О мерах по дальнейшему совершенствованию технологий и коммуникаций» от 19.02.2018 г., и другие нормативно-правовые документы, принятые в данной сфере [1-4].

В настоящее время стандарт мобильной связи GSM является наиболее распространенной системой в Европе и странах СНГ. В США имеется модификация этой системы. Ее сторонники подчеркивают хорошее качество речи, наличие службы коротких сообщений (SMS), работу в сложных метеоусловиях, в условиях многолучевого распространения и минимального отношения сигнал-помеха.

Одна из основных функций сетей GSM является управление мобильностью, в задачу которой входит функция отслеживания местонахождения абонентов, для направления к ним звонков. Без этой функции абоненты сетей, построенные в любой стране мира на основе стандарта GSM, не смогут использовать свои телефонные аппараты для получения услуг в соответствующих зонах обслуживания. К таким услугам относятся как высокоскоростная передача данных, передача коротких сообщений (SMS), услуги Интеллектуальной сети (IN), например, услуга мобильной виртуальной корпоративной сети (MVPN).

Технические спецификации GSM разработаны с учетом возможности взаимодействия с другими стандартами, то есть они гарантируют наличие интерфейсов с сетями мобильной связи других стандартов. Следует также отметить, то ключевым аспектом GSM является то, что спецификации могут быть модифицированы, они являются «открытыми», то есть не являются законченными в смысле развития и могут дорабатываться с целью удовлетворения будущих потребностей [5].

К стандарту GSM разработаны разнообразные приложения. Как известно охрана домов, дач, квартир и гаражей является достаточно сложной задачей, для эффективного решения которой возникает потребность в применении различных защитных систем. Наиболее эффективным охранным комплексом, отличающимся широкими функциональными возможностями и высоким уровнем безопасности, является GSM сигнализация. Здесь важным является также и то, что для передачи сигналов об опасности используются высокочастотные каналы сотовой связи, а не проводные магистрали, которые могут легко повредить злоумышленники.

Существуют большое разнообразие GSM-модулей, позволяющие управлять дистанционно любой автоматикой, принимая сигнал с телефона, работающего в диапазоне GSM, и осуществляя включение/выключение подсоединенной аппаратуры. Применяется он для открытия распашных и откатных ворот, шлагбаума на паркингах, автостоянках, в дачных и

гаражных кооперативах, частных домах, удаленного управления инженерными системами полива, освещения, отопления, перезагрузки серверов и роутеров. Наиболее широкое распространение получили GSM-модули как надежный и бюджетный контроллер для управления групповым доступом на объект и многие другие.

Целью данного учебника является изложение общих принципов организации и работы мобильных систем связи стандарта GSM, а также особенностей управления мобильностью.

ГЛАВА 1. СОТОВАЯ СВЯЗЬ СТАНДАРТА GSM

1.1. Принципы построения и основные характеристики стандарта GSM

Классификация мобильных систем связи. Системы радиосвязи с подвижными объектами, потребность в которых с каждым годом все более возрастает, условно подразделяются следующим образом [5]:

- системы персонального радиовызова (Paging Systems);
- профессиональные (частные) системы подвижной радиосвязи (PMR,PAMR);
- системы сотовой подвижной радиосвязи (ССПС – Cellular Radio Systems);
- системы беспроводных телефонов (Cordless Telephony);
- системы персональной связи с использованием ИСЗ.

Принципы построения сотовых систем радиосвязи. Одной из первых систем персональной мобильной связи можно считать систему персонального вызова «Мультитон». В этой системе диспетчер вызывает сотрудника по персональному приемнику. По получению акустического вызова сотрудник находит ТЛФ и звонит диспетчеру.

Следующий уровень сервиса, сотрудник не только получает вызов, но и на дисплее индивидуального приемника видит номер ТЛФ вызывающего абонента, но связаться с ним может только со стационарного ТЛФ (Paiging Systems).

Высший уровень подобной системы позволяет производить переговоры с индивидуального радиотелефона внутри системы и выходить в общественную ТЛФ сеть через диспетчера. Подобными системами оборудуются предприятия, больницы, промышленные комплексы и др. (PMR и PAMR). PMR понимают как частные системы подвижной радиосвязи, которые не обеспечивают непрерывности связи при пересечении абонентами границ зон радиопокрытия, не имеют автоматического роуминга, не гарантируют абонентам других систем одинаковый набор имеющихся услуг

связи, включая вопросы оплаты. PAMR в отличие от PMR обеспечивает автоматическое соединение подвижных абонентов с абонентами телефонных сетей общего пользования.

Основные усилия при проектировании подвижных систем были сосредоточены на обеспечении высокой помехоустойчивости приема радиотелефонных сообщений, поэтому в этом направлении были достигнуты определенные успехи, которые приблизили подвижную связь по качеству принимаемой информации к уровню проводной ТЛФ связи. Это привело к тому, что частотный ресурс, выделенный подвижной связью, был исчерпан ввиду массового притока радиоабонентов, что побудило разработчиков к поведению интенсивных исследований в области создания систем с высокой пропускной способностью и эффективного использования спектра частот.

В этом отношении наиболее перспективными были признаны сотовые системы подвижной связи (ССПС), имеющие принципиально новую структуру построения и организации связи, а именно множество базовых станций (BTS) соединяются в единую сеть. В процессе передвижения абонентская станция (MS) «эстафетно передается» от одной BTS к другой, автоматически переключаясь по командам последних на нужный частотный канал, что и обеспечивает непрерывность связи. В ССПС выделенные частотные каналы многократно используются абонентами в ячейках, разнесенных друг от друга на необходимое защитное расстояние. При таком принципе построения число активных частотных каналов возрастает, что обеспечивает высокую пропускную способность и более эффективное использование спектра частот.

История развития сотовой связи. Первая система радиотелефонной связи, предлагавшая услуги всем желающим, начала свое функционирование в 1946 г. в г. Сент-Луис (США). Радиотелефоны, применявшиеся в этой системе, использовали обычные фиксированные каналы. Если канал связи был занят, то абонент вручную переключался на другой – свободный канал. Аппаратура была громоздкой и неудобной в использовании. Центральный

радио узел передавал высокочастотные сигналы огромной мощности на расстояние 100 км. Обслуживание, в лучшем случае, было соответствующим. Телефонная система предоставляла 11 каналов, работавших по принципу частотной модуляции, с шириной полосы частот 40 МГц. Затем последовали две улучшенные системы (IMTS-MJ и –MK), занимающие 11 и 12 каналов с шириной полосы частот 152- и 454 МГц соответственно. Технология и использование частотной модуляции были усовершенствованы, радиоканалы стали более узкими. Самым ранним мобильным телефонам был необходим спектр частот в 120 кГц, чтобы передать голосовой сигнал в 3 кГц.

С развитием техники системы радиотелефонной связи совершенствовались: уменьшались габариты устройств, осваивались новые частотные диапазоны, улучшалось базовое и коммутационное оборудование, в частности, появилась функция автоматического выбора свободного канала (trunking). Однако при огромной потребности в услугах радиотелефонной связи возникали и проблемы.

Главная из них – ограниченность частотного ресурса: число фиксированных частот в определенном частотном диапазоне не может бесконечно увеличиваться, поэтому радиотелефоны с близкими по частоте рабочими каналами начинают создавать взаимные помехи.

Ученые и инженеры разных стран пытались решить эту проблему. И вот в середине 40-х годов исследовательский центр Bell Laboratories американской компании AT&T предложил идею разбиения всей обслуживаемой территории на небольшие участки, которые стали называться ***сотами,*** (англ. *Cell* - ячейка). Каждая сота должна была обслуживаться передатчиком с ограниченным радиусом действия и фиксированной частотой. Это позволило бы без всяких взаимных помех использовать ту же самую частоту повторно в другой ячейке. Однако прошло более 30 лет, прежде чем такой принцип организации связи был реализован на аппаратном уровне. Причем в эти годы разработка принципа сотовой связи велась в различных странах мира по разным направлениям.

Усилия по созданию безопасности мобильной телефонии и PMR (private dispatched mobile radio - персональная мобильная радиосвязь) были возложены на Федеральную Комиссию Связи (FCC), которая рассматривала ряд радиовещательных служб как наиболее социально ответственных. Политические веяния способствовали росту популярности мобильной телефонии и в 1968 году комиссия согласилась рассмотреть возможность использования высокочастотных телеканалов 70-83 (ширина полосы частот 800 МГц) для нужд PMR. К тому времени в США уже насчитывалось около 70 000 пользователей мобильных телефонов.

В 1971 году в AT&T Bell Laboratories, Murray Hill, N.J., предложили концепцию сотовой системы и как более предпочтительную архитектуру мобильной телефонной системы AMPS. Идея была интригующей и призывала поместить основную станцию на большую высоту над городом, а ее менее мощные копии поближе к земле на обширном пространстве. Каждая ячейка была копией основной радиоустановки и управлялась через переключающий центр и управляющую функцию основной станции.

Уменьшение области действия каждой ячейки позволили повторять частоты при условии, что они располагались на достаточном расстоянии друг от друга. Известно, что влияние ячеек пропорционально не расстоянию между ними, а коэффициенту отношения этого расстояния к радиусу ячейки. В свою очередь радиус ячейки пропорционален мощности передатчика, что дает возможность увеличивать число радиоканалов в системе простым уменьшением мощности передатчика ячейки, а уменьшение размера ячейки позволяет заполнить свободные области новыми ячейками.

В конце 70-х годов начались работы по созданию единого стандарта сотовой связи для 5 североевропейских стран: Швеции, Финляндии, Исландии, Дании и Норвегии, который получил название NMT-450(Nordic Mobile Telephone) и предназначался для работы в диапазоне 450 МГц. Эксплуатация первых систем NMT-450началась в 1981 г., но еще на месяц

раньше система сотовой связи стандарта NMT-450 вступила в эксплуатацию в Саудовской Аравии.

Сети на основе стандарта NMT-450 и его модифицированные версии стали широко использоваться в Австрии, Голландии, Бельгии, Швейцарии, а также в странах Юго-Восточной Азии и Ближнего Востока. На базе этого стандарта в 1985 г. был разработан стандарт NMT-900 диапазона 900 МГц, который позволил расширить функциональные возможности системы и значительно увеличить абонентскую емкость системы.

В1983 г. в США, после ряда успешных полевых испытаний вступила в коммерческую эксплуатацию сеть стандарта AMPS (Advanced Mobile Phone Service), разработанная в исследовательском центре Bell Laboratories.

В 1985 г. в Великобритании был принят в качестве национального стандарт TACS (Total Access Communications System), разработанный на основе американского стандарта AMPS. В 1987 г. в связи с резким увеличением числа абонентов сотовой связи была расширена рабочая полоса частот. Новая версия этого стандарта сотовой связи получила название ETACS (Enhanced TACS).

Во Франции, в отличие от других европейских стран, в 1985 г. был принят стандарт Radiocom-2000. С 1986 г. в скандинавских странах начал применяться стандарт NMT-900.

Все вышеперечисленные стандарты являются аналоговыми и относятся к первому поколению систем сотовой связи. Использование различных стандартов сотовой связи и большая перегруженность выделенных частотных диапазонов стали препятствовать ее широкому применению. Иногда по одному и тому же телефону было невозможно из-за взаимных помех разговаривать даже абонентам, находящимся в двух соседних странах (особенно в Европе). Увеличить число абонентов можно было лишь двумя способами: расширив частотный диапазон (как, например, это было сделано в Великобритании – ETACS) или, перейдя к рациональному частотному

планированию, позволяющему гораздо чаще использовать одни и те же частоты.

Использование новейших технологий и научных открытий в области связи и обработки сигналов позволило подойти к концу 80-х годов к новому этапу развития систем сотовой связи – созданию систем второго поколения, основанных на цифровых методах обработки сигналов, к которому относится и стандарт GSM.

История развития GSM. С целью разработки единого европейского стандарта цифровой сотовой связи для выделенного в этих целях диапазона 900 МГц в 1982 г. Европейская Конференция Администраций Почт и Электросвязи (CEPT) – организация, объединяющая администрации связи 26 стран, создала специальную группу Groupe Special Mobile**.** Аббревиатура GSM и дала название новому стандарту (позднее, в связи с широким распространением этого стандарта во всем мире, GSM стали расшифровывать как Global System for Mobile Communications. Результатом работы этой группы стали опубликованные в 1990 г. требования к системе сотовой связи стандарта GSM, в котором используются самые современные разработки ведущих научно-технических центров [6].

В полном масштабе на территории Европы система начала действовать в канун 1993 года, а введение новых зон обслуживания продолжалось в течение 1995 года. Также в 1986 году GSM взяла на себя общую ответственность за координацию развития всего комплекса спецификаций.

Оставалось подключить к работе потенциальных операторов, иными словами, будущих разработчиков и владельцев сетей. Этот вопрос решился в сентябре 1987 года, в момент подписания в Копенгагене операторами из 13 стран "Меморандума о взаимопонимании" MoU (Memorandum of Understanding), что соответствовало намерениям в пользу осуществления проекта. Тем временем во Франции началось тестирование восьми или девяти различных способов передачи радиосигнала, в результате чего неоспоримый выбор пал на метод многостанционного доступа с временным

разделением каналов TDMA (Time Division Multiple Access), иными словами, временного уплотнения (мультиплексирования). Стоит отметить, что решающую роль в разработке данного метода сыграл исследовательский институт CNET, который впоследствии был преобразован во France Telecom.

К февралю 1988 года надежность системы была достаточно доказана, чтобы можно было официально пригласить всех операторов, подписавших "Меморандум о взаимопонимании" для участия в проекте. Но необходимо было довести до конца огромную работу по разработке и тестированию окончательных спецификаций, которые к 1997 году должны были достичь уже 6000 страниц. Очень скоро стало ясно, что этот титанический труд имеет такой размах и сложность, что дата введения системы в эксплуатацию, назначенная на 1 июля 1991 года, начала ставиться под очень большое сомнение со всеми вытекающими из этого катастрофическими последствиями. Принимая во внимание сложившуюся ситуацию, было решено разбить проект на две фазы, дающие возможность запустить систему поэтапно, с некоторым промежутком, хотя на первых порах и не в полном объеме, но вполне функционирующую.

Передача ответственности в 1989 году от группы GSM Европейскому институту стандартов по телекоммуникациям ETSI (European Telecommunications Standards Institute), созданному во Франции, активизировала деятельность, направленную на взаимодействие между административными органами, операторами и производителями, одновременно поставленными в равные условия. В результате "Фаза 1" спецификации GSM была опубликована в 1990 году и принята для разработанной в Великобритании системы DCS 1800 (диапазон 1800 МГц).

В дальнейшем эта система была переименована в GSM 1800 и на выставке TELECOM 91, проходившей в Женеве, был представлен опытный образец сети. Однако на рынке еще не было телефонов GSM из-за нерешенных вопросов совместимости и стандартизации. Надо отметить, что эти телефоны входили в число первого телекоммуникационного оснащения,

которое прошло испытания на соответствие единому общеевропейскому стандарту, а не принималось по очереди в каждой стране. Но к 1991 году процедура согласования и стандартизации еще не была разработана. Наконец, в апреле 1992 года была установлена временная процедура типовых испытаний на соответствие стандарту, позволившая начать массовый выпуск первых сотовых телефонов, что мгновенно стимулировало деятельность операторов. Все встало на свои места, снежный ком завертелся, и более ничто не могло его остановить. В июне 1992 года было подписано первое соглашение по роумингу, давшее возможность английским абонентам пользоваться их сотовыми телефонами в Финляндии, а финским абонентам - в Англии. Общеевропейская сеть заработала. К концу 1993 года насчитывалось уже свыше миллиона абонентов. А после того, как австралийский оператор Telstra присоединился к остальным участникам Меморандума, система GSM вышла за границы Европы и завоевала весь мир. На сегодняшний день только во Франции уже более двадцати миллионов абонентов, которых обслуживают три оператора. Мобильные телефоны GSM могут использоваться более чем в сотне стран, разбросанных по всему миру, и даже спутниковые сотовые телефоны работают в соответствии со стандартом GSM.

В отличие от других, широко распространенных цифровых стандартов, GSM обеспечивает лучшие энергетические характеристики, более высокое качество связи, ее безопасность и конфиденциальность. Приемлемое качество принимаемых речевых сообщений в стандарте GSM обеспечивается при отношении сигнал/шум на входе приемника 9 дБ (для стандарта D-AMPS, например, это отношение составляет около 16 дБ), а энергетические затраты в реальных каналах связи (при замирании сигналов) на 6-10 дБ ниже, по сравнению со стандартом D-AMPS.

Предоставляемые услуги в стандарте GSM. Стандарт GSM предоставляет своим пользователям ряд услуг, которые не реализованы (или

реализованы не полностью) в других стандартах сотовой связи [3]. К ним относятся:

- Использование интеллектуальных SIM-карт для обеспечения доступа к каналу и услугам связи;
- Шифрование передаваемых сообщений;
- Закрытый от прослушивания радиоинтерфейс;
- Аутентификация абонента и идентификация абонентского оборудования по криптографическим алгоритмам;
- Использование служб коротких сообщений, передаваемых по каналам сигнализации;
- Автоматический роуминг абонентов различных сетей GSM в национальном и международном масштабах;
- Межсетевой роуминг абонентов GSM с абонентами сетей стандартов DCS1800, PCS1900, DECT, а также со спутниковыми сетями персональной радиосвязи (Globalstar, Inmarsat-P, Iridium).

Общие характеристики стандарта GSM. В соответствии с Рекомендацией CEPT 1980 г., касающейся использования частот подвижной связи в диапазоне 862-960 МГц, стандарт GSM цифровой общеевропейской сотовой системы наземной подвижной связи предусматривает работу передатчиков в двух диапазонах частот [7]. Полоса частот 890-915 МГц используется для передачи сообщений с подвижной станции на базовую, а полоса частот 935-960 МГц - для передачи сообщений с базовой станции на подвижную (абоненту). Причем при переключении каналов во время сеанса связи разность между этими частотами постоянна и равна 45 МГц. Разнос частот между соседними каналами связи составляет 200 кГц. Таким образом, в отведенной для приема/передачи полосе частот шириной 25 МГц размещается 124 канала связи.

В стандарте GSM используется узкополосный многостанционный доступ с временным разделением (TDMA), что позволяет на одной несущей частоте разместить 8 речевых каналов одновременно. В качестве

речепреобразующего устройства используется речевой кодек RPE - LTP с регулярным импульсным возбуждением и скоростью преобразования речи 13 Кбит/с.

Обработка речи в данном стандарте осуществляется в рамках принятой системы прерывистой передачи речи DTX (Discontinuous Transmission), которая обеспечивает включение передатчика только тогда, когда пользователь начинает разговор, и отключает его в паузах и в конце разговора. Система DTX управляет детектором активности речи VAD (Voice Activity Detector), который обеспечивает обнаружение и выделение интервалов речи с шумом и шума без речи даже в тех случаях, когда уровень шума соизмерим с уровнем речи.

Для защиты от ошибок, возникающих в радиоканалах, применяется блочное и сверточное кодирование с перемежением. Повышение эффективности кодирования и перемежения при малой скорости перемещения подвижных станций достигается медленным переключением рабочих частот в процессе сеанса связи (со скоростью 217 скачков в секунду).

Для борьбы с интерференционными замираниями принимаемых сигналов, вызванными многолучевым распространением радиоволн в условиях города, в аппаратуре связи используются эквалайзеры, обеспечивающие выравнивание импульсных сигналов со среднеквадратическим отклонением времени задержки до 16 мкс. Система синхронизации оборудования рассчитана на компенсацию (до 233 мкс) абсолютного времени задержки сигналов. Это соответствует максимальной дальности связи 35 км (радиус соты).

Для модуляции радиосигнала применяется спектрально-эффективная гауссовская частотная манипуляция с минимальным частотным сдвигом (GMSK). Такое называние обусловлено тем, что последовательность информационных бит до модулятора проходит через фильтр нижних частот с гауссовской амплитудно-частотной характеристикой, что дает значительное

уменьшение ширины полосы частот излучаемого сигнала. Формирование GMSK радио-сигнала происходит таким образом, что на интервале, соответствующем одному биту, фаза несущей изменяется на 90°. Это наименьшее изменение фазы, которое может быть обнаружено при данном типе манипуляции. Выходной сигнал с непрерывным изменением фазы аналогичен сигналу, полученному в результате частотной модуляции с дискретным изменением частоты.

В стандарте GSM используется модуляция с величиной нормированной полосы BT=0,3, где B - ширина полосы фильтра по уровню -3 дБ; T - длительность передачи одного бита. Основой формирователя GMSK-сигнала является квадратурный (I/O) модулятор, который состоит из двух умножителей и одного сумматора.

Модуляцию GMSK характеризуют следующие свойства:

- постоянная по уровню огибающая, позволяющая использовать передающие устройства с усилителями мощности класса С;
- узкий спектр на выходе усилителя мощности передающего устройства, обеспечивающий низкий уровень внеполосного излучения;
- хорошая помехоустойчивость канала связи.

В стандарте GSM достигается высокая степень безопасности передачи сообщений, которая осуществляется шифрование сообщений по алгоритму шифрования с открытым ключом (RSA).

В целом система связи, действующая в стандарте GSM, рассчитана на ее использование в различных сферах. Она предоставляет пользователям широкий диапазон услуг и возможность применять разнообразное оборудование для передачи речевых сообщений и данных, вызывных и аварийных сигналов; подключаться к телефонным сетям общего пользования (PSTN), сетям передачи данных (PDN) и цифровым сетям с интеграцией служб (ISDN).

Основные характеристики стандарта GSM

Частоты передачи подвижной станции приема базовой станции-890-915 МГц;

Частоты приема подвижной станции и передачи базовой станции-935-960 МГц;

Дуплексный разнос частот приема и передачи -45 МГц;

Скорость передачи сообщений в радиоканале - 270, 833 кбит/с;

Скорость преобразования речевого кодека -13 кбит/с;

Ширина полосы канала связи - 200 кГц;

Максимальное количество каналов связи – 124;

Максимальное количество каналов, организуемых на базовой станции-16-20;

Вид модуляции – GMSK;

Индекс модуля BT - 0,3;

Ширина полосы предмодуляционного гауссовского фильтра - 81,2 кГц;

Количество скачков по частоте в секунду – 217;

Временное разнесение в интервалах TDMA кадра (передача/прием) для подвижной станции -2;

Вид речевого кодека - RPE/LTP;

Максимальный радиус соты -35 км;

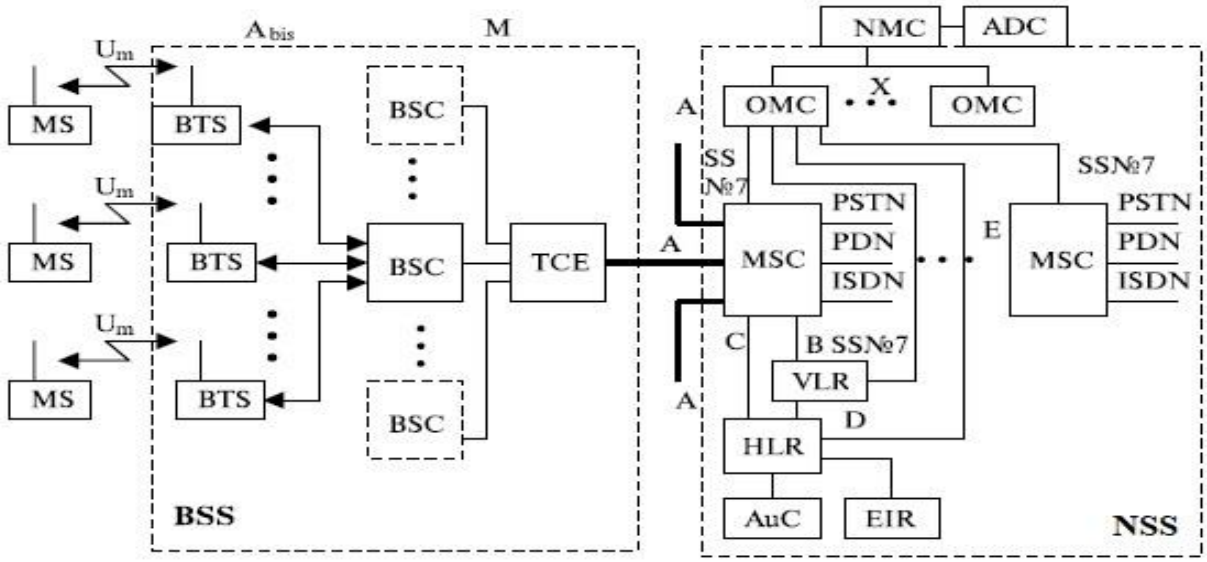
Схема организации каналов комбинированная - TDMA/FDMA.

В Узбекистане, в Ташкенте, впервые появилась система стандарта NMT-450 в 1993 году. Принятие в дальнейшем концепции развития сетей сухопутной подвижной связи стало мощным катализатором дальнейшего развития сотовой связи в национальном масштабе. И если с внедрением стандартов NMT, и затем AMPS Узбекистан отставал лет на десять, то провозглашение стандарта GSM в качестве республиканского, сократило этот временной разрыв примерно до трех лет.

Четкая ориентация на прогрессивные мировые технологии дала возможность Узбекистану не отставать от ведущих стран мира в развитии современных систем подвижной радиосвязи, однако основным стандартом, используемым абонентами, остается пока GSM.

1.2. Архитектура и основные принципы организации сети GSM

Сеть GSM состоит из нескольких функциональных объектов, функции и интерфейсы которых показаны на рисунке 1.1 [5-8].



ADC — Administration Center	Административный центр
AuC — Authentication	Центр аутентификации
BTS — Base Transceiver Station	Базовая приемо-передающая станция
BSC — Base Station Controller	Контроллер базововй станции
BSS — Base Station System	Подсистема базовой станции
EIR — Equipment Identification Register	Регистр идентификации оборудования
HLR — Home Location Register	Домашний регист местоположения
ISDN — Integrated Service Digital Network	Цифровая сеть с интеграцией служб
MS — Mobile Station	Мобильная станция
MSC — Mobile Switching Center	Цент коммутации мобильной связи
NMC — Network Management Center	Центр управления сетью
OMC — Operation and Maintenance Center	Центр эксплуатации и технического обслуживания
PDN — Packet Data Networks	Сеть пакетной коммутации
PSTN — Public Switched Telephone Network	Телефонная сеть общего пользования
NSS — Network Switching Subsystem	Коммутационная подсистема
TCE — Transcoder Equipment	Транскодер
VLR — Visit Location Register	Визитный регистр местоположения

Рис. 1.1. Архитектура сети и интерфейсы GSM

Сеть GSM включает три основные части:

- мобильные станции (MS), которые перемещаются с абонентом;
- подсистему базовых станций (BSS), которая управляет радиолинией связи с мобильной станцией;
- подсистему сети (NSS), главная часть которой — центр коммутации

мобильной связи (MSC) — выполняет коммутацию между мобильными станциями и между мобильными или стационарными сетевыми пользователями. MSC также управляет работой, связанной с передвижением абонента.

На рисунке 1.1. не показан центр обслуживания, который наблюдает за надежным функционированием и изменениями на сети. Мобильная станция (MS) и подсистема базовых станций (BSS) связываются по Um-интерфейсу, также известному как "воздушный *интерфейс*" или радиолиния связи. Подсистема базовых станций взаимодействует с центром коммутации мобильной связи по А интерфейсу.

Мобильная станция (MS) состоит из подвижной аппаратуры (терминал) и карты с интегральной схемой, включающей микропроцессор, которая называется модулем абонентской идентификации (SIM — Subscriber Identification Module). SIM-карта обеспечивает при перемещении пользователя доступ к оплаченным услугам независимо от используемого терминала. Вставляя SIM-карту в другой терминал GSM, пользователь может принимать вызовы, делать вызовы с этого терминала и получать другие услуги [5-8].

Подвижная аппаратура однозначно определяется с помощью международного опознавательного кода мобильного оборудования (*IMEI* — International Mobile Equipment Identity). SIM-карта содержит международный опознавательный код мобильного абонента (*IMSI* — International Mobile Subscriber Identity), используемый для идентификации абонента, секретный код для удостоверения подлинности и другую информацию. *IMEI* и *IMSI* независимы — это дает возможность обеспечить наиболее вероятное опознавание личности при передвижении абонента. SIM-карта может быть защищена против неправомочного использования паролем или личным номером.

Применяются три типа оконечного оборудования подвижной станции:

- MT0 (Mobile Termination 0) — многофункциональная подвижная станция, в состав которой входит терминал данных с возможностью передачи и приема данных и речи;
- MT1 (Mobile Termination 1) — подвижная станция с возможностью связи через терминал с ISDN;
- MT2 (Mobile Termination 2) — подвижная станция с возможностью подключения терминала для связи по протоколу МККТТ V-или X-серий.

Терминальное оборудование может состоять из оборудования одного или нескольких типов, такого как телефонная трубка с номеронабирателем, аппаратура передачи данных (*DTE*), телекс и т. д.

Различают следующие типы терминалов:

1. TE1 (Terminal Equipment — *терминальное оборудование*, обеспечивающее связь с ISDN;
2. TE2 (Terminal Equipment — *терминальное оборудование*, обеспечивающее связь с любым оборудованием через протоколы МККТТ V- или X-серий (связь с ISDN не обеспечивает). Терминал TE2 может быть подключен как нагрузка к MT1 (подвижной станции с возможностью связи с ISDN) через адаптер TA.

Упрощенная схема приемо-передатчика мобильной станции приведена на рисунке 1.2.

В состав передатчика и приемника входят следующие блоки.

В микрофоне речевой сигнал преобразуется в электрический, ширина спектра которого ограничена фильтром и составляет 4 КГц.

Аналого-цифровой преобразователь (АЦП) преобразует в цифровую форму сигнал с выхода микрофона и вся последующая обработка, и передача сигнала речи производится в цифровой форме, вплоть до обратного цифро-аналогового преобразования (ЦАП) на приеме.

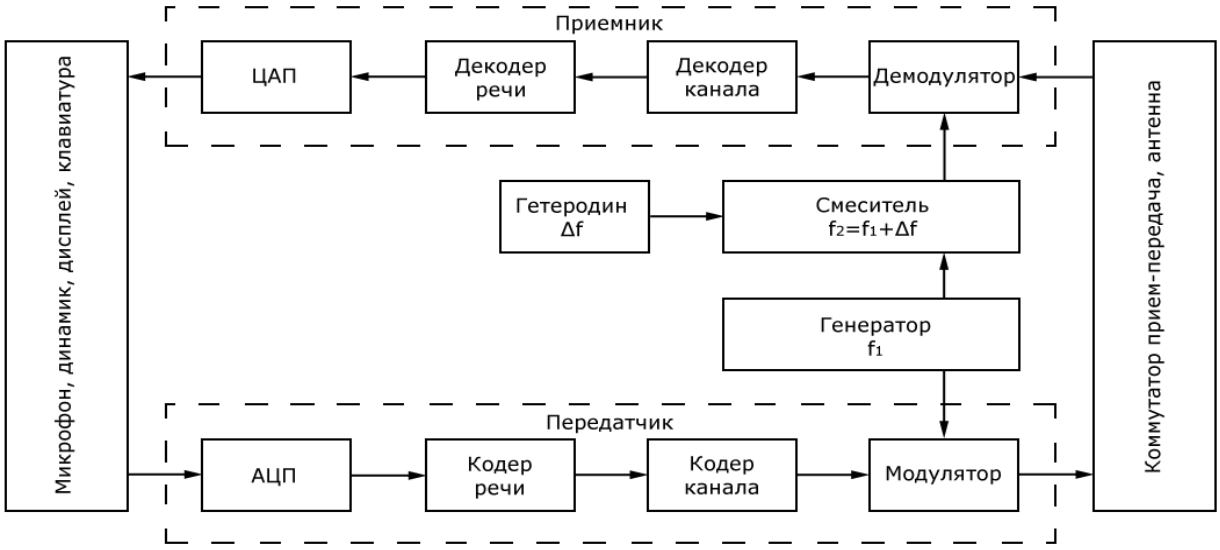


Рис.1.2. Упрощенная блок-схема приемо-передатчика мобильной станции

Кодер речи осуществляет кодирование сигнала речи в цифровой форме с целью сокращения объема информации, передаваемой по каналу связи. Декодер речи восстанавливает на приеме поступивший на него закодированный сигнал речи.

Кодер канала добавляет в сигнал закодированной речи дополнительную информацию, предназначенную для защиты от ошибок на радиоучастке. Декодер канала проверяет принятую информацию на наличие ошибок и выявленные ошибки по возможности исправляет.

Модулятор осуществляет перенос информации на несущую частоту. Демодулятор выделяет из модулированного радиосигнала несущую информацию.

Подробнее все этапы обработки будут рассмотрены в последующем изложении материала.

Подсистема базовых станций содержит два вида оборудования: базовая приемопередающая станция (*BTS* — Base *Transceiver* Station) и контроллер базовой станции (*BSC* — *Base Station* Controller) [5]. Они взаимодействуют через стандартизированный интерфейс A_{bis} (рис.1.1).

На базовой приемопередающей станции размещается приемопередатчик, который для одной определенной соты реализует

протоколы радиолинии с передвижной станцией. В большом городе обычно размещено большое количество *BTS*. Поэтому основные требования к *BTS* — прочность, надежность, портативность и минимальная стоимость.

Контроллер базовой станции управляет радиоресурсами для одного или более *BTS*: выбором и установлением соединения по радиоканалу, скачком частоты и хэндовером (переключением).

BSC подключается между базовой приемопередающей станцией (*BTS*) и центром коммутации мобильной связи (MSC).

Коммутационная подсистема сети. Центральный компонент подсистемы сети — *центр коммутации мобильной связи* (MSC) [5]. Он работает как обычный узел коммутации общедоступной телефонной сети (*PSTN* — Public Switched *Telephone Network*) или цифровой сети интегрального обслуживания (ISDN — Integrated Service *Digital Network*). Дополнительно обеспечивает все функциональные возможности мобильного абонента, такие как регистрация, аутентификация, обновление местоположения, передача соединения (хэндовер) и маршрутизация вызова при передвижении абонента. Эти функции обеспечиваются совместно несколькими функциональными объектами, которые вместе формируют подсистему сети. MSC обеспечивает подключение к фиксированным сетям (таким как общедоступная телефонная сеть *PSTN* или цифровая сеть интегрального обслуживания ISDN). Передача сигналов между функциональными объектами в подсистеме сети использует ОКС № 7 (*SS7*) — отдельный канал сигнализации, такой же, как применяется для обмена в ISDN и в сетях общего пользования.

Центр коммутации подвижной связи обслуживает группу сот и обеспечивает все виды соединений, в которых нуждается в процессе работы подвижная станция. MSC аналогичен ISDN коммутационной станции и реализует интерфейс между фиксированными сетями (*PSTN*, *PDN*, ISDN и т. д.) и сетью подвижной связи. Он обеспечивает маршрутизацию вызовов и функции управления вызовами. Кроме выполнения функций обычной ISDN

коммутационной станции на MSC возлагаются функции коммутации радиоканалов. К ним относятся "эстафетная передача", в процессе которой достигается непрерывность связи при перемещении подвижной станции из соты в соту, и переключение рабочих каналов в соте при появлении помех или неисправностях.

Каждый MSC обеспечивает обслуживание подвижных абонентов, расположенных в пределах определенной географической зоны (например, Ташкент и область). MSC управляет процедурами установления вызова и маршрутизации. Для телефонной сети общего пользования (*PSTN*) MSC обеспечивает функции сигнализации по протоколу ОКС №7, передачи вызова или поддержки других видов интерфейсов в соответствии с требованиями конкретного проекта.

MSC формирует данные, необходимые для выписки счетов за предоставленные сетью услуги связи, накапливает данные по состоявшимся разговорам и передает их в центр расчетов (биллинг- центр). MSC составляет также статистические данные, необходимые для контроля работы и оптимизации сети. Он же поддерживает *процедуры безопасности*, применяемые для управления доступами к радиоканалам.

MSC не только участвует в управлении вызовами, но также управляет процедурами регистрации местоположения и передачи управления, кроме передачи управления в подсистеме базовых станций (*BSS*). Регистрация местоположения подвижных станций необходима для обеспечения доставки вызова перемещающимся подвижным абонентам от абонентов телефонной сети общего пользования или других подвижных абонентов. Процедура передачи вызова позволяет сохранять соединения и обеспечивать ведение разговора, когда подвижная станция перемещается из одной зоны обслуживания в другую. Передача вызовов в сотах, управляемых одним контроллером базовых станций (*BSC*), осуществляется этим *BSC*. Когда передача вызовов происходит между двумя сетями, управляемыми разными *BSC*, то первичное управление осуществляется в MSC. В стандарте GSM

также предусмотрены процедуры передачи вызова между сетями (контроллерами), относящимися к разным MSC. Центр коммутации осуществляет постоянное слежение за подвижными станциями, используя домашний регистр местоположения (*HLR*) и визитный регистр местоположения (*VLR*).

Домашний регистр местоположения (*HLR* —Home Location Register). В *HLR* хранится та часть информации о местоположении какой-либо подвижной станции, которая позволяет центру коммутации доставить вызов определенной мобильной станции. Практически *HLR* представляет собой справочную базу данных о постоянно зарегистрированных в сети абонентах. В ней содержатся опознавательные номера и адреса, а также параметры подлинности абонентов, состав услуг связи, специальная информация о маршрутизации. Ведется регистрация данных об изменении местоположения и роуминге ("блуждании") абонента, включая данные о временном идентификационном номере подвижного абонента (TMSI — Temporary Mobile Subscriber Identity) и соответствующем визитном регистре местоположения (*VLR*). Регистр *HLR* содержит международный идентификационный номер подвижного абонента (*IMSI* — International Mobile Subscriber Identity), состав услуг связи, специальную информацию о маршрутизации. Он используется для опознавания подвижной станции в центре аутентификации (AUC — *Authentication Center*).

Домашний регистр местоположения (*HLR*) вместе с MSC обеспечивает маршрутизацию вызова и изменения местоположения (роуминг) мобильной станции и содержит всю административную информацию каждого абонента, зарегистрированного в соответствующей сети GSM, наряду с текущим местоположением мобильных станций. Местоположение мобильных станций находится обычно в форме адреса данной мобильной станции в *VLR*. Фактическая процедура маршрутизации будет описана позже. Логически существует только один *HLR* в сети GSM, хотя он может быть реализован как распределенная база данных. К данным, содержащимся в *HLR*, имеют

дистанционный доступ все MSC и *VLR* сети, и, если в сети имеются несколько *HLR*, в базе данных содержится только одна запись об абоненте, поэтому каждый *HLR* представляет собой определенную часть общей *базы данных сети* об абонентах. Доступ к базе данных об абонентах осуществляется по номеру *IMSI* (*IMSI* — International Mobile Station Identity) или по MSISDN-номеру подвижной станции в сети ISDN (MSISDN — Mobile Station ISDN Number). К базе данных могут получить доступ MSC или *VLR*, относящиеся к другим сетям, в рамках обеспечения межсетевого роуминга абонентов.

Визитный регистр местоположения (*VLR* — Visit Location Register). Второе основное устройство, обеспечивающее контроль над передвижением подвижной станции из зоны в зону, — визитный регистр местоположения *VLR*. С его помощью достигается функционирование подвижной станции за пределами зоны, контролируемой *HLR*. Когда в процессе перемещения подвижная станция переходит из зоны действия одного контроллера базовой станции *BSC*, объединяющего группу базовых станций, в зону действия другого *BSC*, она регистрируется новым *BSC*, и в *VLR* заносится информация о номере области связи, которая обеспечит доставку вызовов подвижной станции. Для сохранности данных, находящихся в *HLR* и *VLR*, в случае сбоев предусмотрена защита устройств памяти этих регистров.

VLR включает в себя такие же данные, как и *HLR*, однако эти данные содержатся в *VLR* только до тех пор, пока абонент находится в зоне, контролируемой *VLR*.

В сети подвижной связи GSM соты группируются в географические зоны (LA — Location Area), которым присваивается свой идентификационный номер (*LAC* — Location *Area Code*). Каждый *VLR* содержит данные об абонентах в нескольких LA. Когда подвижный абонент перемещается из одной LA в другую, данные о его местоположении автоматически обновляются в *VLR*. Если старая и новая LA находятся под управлением различных *VLR*, то данные на старом *VLR* стираются после их

копирования в новый *VLR*. Текущий адрес *VLR* абонента, содержащийся в *HLR*, также обновляется.

VLR обеспечивает также присвоение номера для услуг роуминга мобильной станции (MSRN — Mobile Station *Roaming* Number). Когда подвижная станция принимает входящий вызов, *VLR* выбирает его MSRN и передает его на MSC, который осуществляет маршрутизацию этого вызова к базовым станциям, находящимся рядом с подвижным абонентом.

Во время движения подвижная станция может покинуть зону, обслуживаемую одним MSC/VLR, и переместиться в зону, которую обслуживает другой MSC/VLR. В этом случае MSC/VLR участвует в передаче управления от одного MSC/VLR к другому. Он также присваивает новый временный мобильный опознавательный код станции TMSI (Temporary Mobile Subscriber Identity) и передает его в *HLR*. Новый MSC/VLR инициирует процедуру установления подлинности абонента и его оборудования. Кроме случая, когда подвижный абонент меняет зону местоположения, временный номер может периодически изменяться по решению оператора с целью защиты от злонамеренного перехвата номеров участников разговора. В этом случае процедура изменения идет также с использованием *VLR,* для доступа к *VLR* могут использоваться идентификационные номера *IMSI*, TMSI и MSRN.

В общем VLR можно считать локальной базой данных в данной зоне, которая содержит информацию о подвижном абоненте.

Применение *VLR* позволяет сократить число запросов *HLR*, и это снижает сетевой трафик и уменьшает время обслуживания.

Внутренние интерфейсы GSM.

- Интерфейс между MSC и BSS (A – интерфейс) обеспечивает передачу сообщений для управления BSS, передачи вызова, управления передвижением. A – интерфейс объединяет каналы связи и линии сигнализации. Последние используют протокол SS N7 МККТТ. Полная

спецификация A – интерфейса соответствует требованиям серии 08 Рекомендаций ETSI/GSM.

- Интерфейс между MSC и HLR совмещен с VLR (B – интерфейс). Когда MSC необходимо определить местоположение подвижной станции, он обращается к *VLR.* Если подвижная станция инициирует процедуру место определения с MSC, он информирует свой *VLR,* который заносит всю изменяющуюся информацию в свои регистры. Эта процедура происходит всегда, когда MS переходит из одной области место определения в другую. В случае, если абонент запрашивает специальные дополнительные услуги или изменяет некоторые свои данные, MSC также информирует *VLR*, который регистрирует изменения и при необходимости сообщает о них *HLR.*
- Интерфейс между MSC и *HLR* (C – интерфейс) используется для обеспечения взаимодействия между MSC и HLR. MSC может послать указание (сообщение) *HLR* в конце сеанса связи для того, чтобы абонент мог оплатить разговор. Когда сеть фиксированной телефонной связи не способна исполнить процедуру установления вызова подвижного абонента, MSC может запросить *HLR* с целью определения местоположения абонента для того, чтобы послать вызов MS.
- Интерфейс между *HLR* и *VLR* (D – интерфейс) используется для расширения обмена данными о положении подвижной станции, управления процессом связи. Основные услуги, предоставляемые подвижному абоненту, заключаются в возможности передавать или принимать сообщения независимо от местоположения. Для этого *HLR* должен пополнять свои данные. *VLR* сообщает *HLR* о положении MS, управляя ею и переприсваивая ей номера в процессе блуждания, посылает все необходимые данные для обеспечения обслуживания подвижной станции.
- Интерфейс между MSC (E – интерфейс) обеспечивает взаимодействие между разными MSC при осуществлении процедуры HANDOVER –

"передачи" абонента из зоны в зону при его движении в процессе сеанса связи без ее перерыва.

- Интерфейс между BSC и BTS (A - bis интерфейс) служит для связи BSC с BTS и определен Рекомендациями ETSI/GSM для процессов установления соединений и управления оборудованием, передача осуществляется цифровыми потоками со скоростью 2,048 Мбит/с. Возможно использование физического интерфейса 64 кбит/с.
- Интерфейс между BSC и OMC (O – интерфейс) предназначен для связи BSC с OMC, используется в сетях с пакетной коммутацией МККТТ X.25.
- Внутренний BSC-интерфейс контроллера базовой станции обеспечивает связь между различным оборудованием BSC и оборудованием транскодирования (TCE); использует стандарт ИКМ – передачи 2,048 Мбит/с и позволяет организовать из четырех каналов со скоростью 16 кбит/с или один канал на скорости 64 кбит/с.
- Интерфейс между MS и BTS (Um - радиоинтерфейс) определен в сериях 04 и 05 Рекомендаций ETSI/GSM.
- Сетевой интерфейс между OMC и сетью, так называемый управляющий интерфейс между OMC и элементами сети, определен ETSI/GSM Рекомендациями 12.01 и является аналогом интерфейса Q.3, который определен в многоуровневой модели открытых сетей ISO OSI. Соединение сети с OMC могут обеспечиваться системой сигнализации МККТТ SS N7 или сетевым протоколом X.25. Сеть X.25 может соединяться с объединенными сетями или с PSDN в открытом или замкнутом режимах.
- GSM - протокол управления сетью и обслуживанием также должен удовлетворять требованиям Q.3 интерфейса, который определен в ETSI/GSM Рекомендациях 12.01.

Интерфейсы между сетью GSM и внешним оборудованием.

- Интерфейс между MSC и сервис – центром (SC) необходим для реализации службы коротких сообщений. Он определен в ETSI/GSM Рекомендациях 03.40.
- Интерфейс к другим OMC. Каждый центр управления и обслуживания сети должен соединяться с другими OMC, управляющими сетями в других регионах или другими сетями. Эти соединения обеспечиваются X – интерфейсами в соответствии с
- Рекомендациями МККТТ М.3О. Для взаимодействия OMC с сетями высших уровней используется О.3 – интерфейс.

Интерфейсы с внешними сетями

Соединение с PSTN

- Соединение с телефонной сетью общего пользования осуществляется MSC по линии связи 2 Мбит/с в соответствии с системой сигнализации SS N 7. Электрические характеристики 2 Мбит/с интерфейса соответствуют Рекомендациям МККТТ G.732.

Соединение с ISDN

- Для соединения с создаваемыми сетями ISDN предусматриваются четыре линии связи 2 Мбит/с, поддерживаемые системой сигнализации SS N 7 и отвечающие Рекомендациям Голубой книги МККТТ Q.701-Q.710, Q.711-Q.714, Q.716, Q.781, 0.782, 0.791, 0.795, 0.761-0.764, 0.766.

Соединение с существующей сетью NMT-450

- Центр коммутации подвижной связи соединяется с сетью NMT-450 через четыре стандартные линии связи 2 Мбит/с и системы сигнализации SS N7. При этом должны обеспечиваться требования Рекомендаций МККТТ по подсистеме пользователей телефонной сетью (TUP – Telephone User Part) и подсистеме передачи сообщений (MTP – Message Transfer Part) Желтой книги. Электрические характеристики линии 2 Мбит/с соответствуют Рекомендациям МККТТ G.732.

1.3. Технологии GPRS и EDGE

С момента появления сотовой связи идея мобильной передачи данных не давала покоя наиболее продвинутым пользователям мобильных телефонов. С началом бурного развития сети Интернет проблема передачи данных при помощи мобильного телефона стала еще более актуальной, но существовало два основных препятствия на пути ее решения. Первой проблемой является чрезвычайно строгое ограничение скорости передачи, накладываемое системой GSM, которая обеспечивает максимальную скорость передачи 9,6 кбит/с, а при замене отдельных модулей базовых станций - 14,4 кбит/с. Второй проблемой является высокая стоимость передачи данных, поскольку при передаче информации на столь низких скоростях абоненту требуется большое количество времени, которое он должен оплачивать по тарифам, близким к тарифам за услуги голосовой связи. Именно по этим причинам количество абонентов сотовой связи, пользующихся услугой передачи данных, оставалось небольшим. Появление системы пакетной передачи данных GPRS кардинально изменила сложившуюся ситуацию [5-8]. Схема организации GPRS приведена на рисунке 1.3.

Рис.1.3. Схема GPRS

Передача данных в GSM и GPRS. Передача данных по GSM каналам организована следующим образом: абоненту выделяется отдельный канал, используемый системой для передачи голоса, посредством модема, встроенного в мобильный терминал, происходит передача данных через этот канал, при этом в промежутках между передачей данных канал остается занятым. GPRS (General Packet Radio Service) - это система, которая реализует и поддерживает протокол пакетной передачи информации в рамках сети сотовой связи GSM. При использовании системы GPRS информация собирается в пакеты и передается в эфир, они заполняют те "пустоты" (не используемые в данный момент голосовые каналы), которые всегда есть в промежутках между разговорами абонентов, а использование сразу нескольких голосовых каналов обеспечивает высокие скорости передачи данных. При этом этап установления соединения занимает несколько секунд. В этом и заключается принципиальное отличие режима пакетной передачи данных. В результате у абонента появляется возможность передавать данные, не занимая каналы в промежутках между передачей данных, более эффективно используются ресурсы сети.

Возможности технологии GPRS. GPRS позволит ввести принципиально новые услуги, которые раньше не были доступны. Прежде всего это мобильный доступ к ресурсам Интернета с удовлетворяющей потребителя скоростью, мгновенным соединением и с очень выгодной системой тарификации. Например, при просмотре с помощью системы GPRS WEB-страницы в Интернете, можно изучать содержимое столько, сколько необходимо, поскольку оплата производится только за принятую информацию, а не за время нахождения в сети Интернет (не передавая данные, не занимаются каналы сети). При введении повременной оплаты на фиксированных телефонных линиях, тарифы на доступ в Интернет с мобильного GPRS-телефона будут еще более конкурентоспособны.

Технология GPRS позволит быстро передавать и получать большие объемы данных, видеоизображения, музыкальные файлы стандарта MP-3 и другую мультимедийную информацию.

Для тех абонентов, кто уже оценил удобство использования телефонов с WAP - броузером, внедрение технологии GPRS означает практически мгновенную загрузку WAP - страниц на экране телефона и более выгодную систему тарификации.

Для корпоративных пользователей система GPRS может послужить отличным инструментом для обеспечения безопасного и быстрого доступа сотрудников к корпоративным сетям предприятий, к почтовым, информационным серверам, удаленным базам данных. При этом, появляется возможность получать доступ к корпоративным сетям даже если абонент находится в сети другого GSM оператора, с которым организован GPRS-роуминг.

Технологии GPRS может применяться в системах телеметрии: устройство может быть все время подключено, не занимая при этом отдельный канал. Такая услуга может быть востребована службами охраны, банками для подключения банкоматов и в других областях, в том числе и промышленных.

Принципы построения системы GPRS. На структурном уровне систему GPRS можно разделить на 2 части: подсистему базовых станций и ядро сети GPRS (GPRS Core Network). В подсистему базовых станций входят все контроллеры и базовые станции системы GSM, которые поддерживают пакетную передачу данных на программном и аппаратном уровне. Ядро сети GPRS включает в себя совершенно новые сетевые элементы, предназначенные для обработки пакетов данных и обеспечения связи с сетью Интернет.

Основным сетевым элементом является пакетный коммутатор - SGSN (Serving GPRS Support Node). Данный сетевой элемент берет на себя все функции обработки пакетной информации и преобразования кадров GSM в

форматы, используемые протоколами TCP/IP глобальной компьютерной сети Internet. Пакетный коммутатор призван разгрузить GSM коммутатор, обеспечивая обработку пакетной информации, оставляя обычному коммутатору лишь голосовой трафик.

Вторым важным сетевым элементом является GPRS шлюз - GGSN (Gataway GPRS Support Node). Он обеспечивает связь системы GPRS с пакетными сетями передачи данных: Internet, Intranet, X.25 и др. GGSN содержит всю необходимую информацию о сетях, куда абоненты GPRS могут получать доступ, а также параметры соединения.

Кроме упомянутых элементов в GPRS Core входят другие элементы: DNS (Сервер доменных имен), Charging Gateway (Шлюз для связи с системой тарификации), Border Gateway (Пограничный шлюз) и другие вспомогательные элементы.

Следует отметить широкие возможности масштабирования системы GPRS. При быстром увеличении количества абонентов, пользующихся услугой пакетной передачи данных возможно увеличение емкости системы GPRS за счет расширения или установки дополнительных пакетных коммутаторов (SGSN). При увеличении суммарного объема данных, передаваемых абонентами (при несущественном увеличении числа абонентов), возможна установка дополнительных GPRS - шлюзов, которые обеспечат большую суммарную пропускную способность всей системы, а также расширение системы базовых станций. Таким образом, наращивая систему GPRS, оператор сможет обеспечивать высокое качество услуг, основанных на пакетной передаче данных.

Терминальное оборудование GPRS. Для того, чтобы использовать возможность передачи данных посредством системы GPRS, требуется специальные терминалы, поддерживающие работу в режиме GPRS.

Стандартами определены 3-класса GPRS терминалов:

- класс А - терминал позволяет осуществлять одновременно голосовое соединение и работу в режиме GPRS;

- класс B - терминал поддерживает и голосовое соединения и передачу данных в пакетном режиме (GPRS), но эти режимы используются не одновременно (во время передачи данных через GPRS абонент не может совершать и принимать голосовые звонки и наоборот);
- класс C - терминал обеспечивает только передачу данных в пакетном режиме. Наиболее вероятное исполнение - PCMCIA карта устанавливаемая в портативный компьютер - ноутбук.

Первыми доступными на рынке терминалы были класса B. Эти терминалы поддерживают различные скорости приема и передачи информации. Терминалы класса *B* с поддержкой GPRS используются в качестве модема для передачи данных и доступа в Интернет (при подключении телефона к компьютеру через порт RS-232 или инфракрасный порт), для приема и передачи SMS (при этом стандартное ограничение на длину короткого сообщения -160 символов будет снято), а также для скоростного доступа к WAP-серверам с экрана своего мобильного телефона.

*Скорости передачи в системе GPRS***.** В сетях, поддерживающих GPRS, предусмотрен поэтапный путь наращивания скорости передачи данных; максимальная реальная скорость приема и передачи, которую на первом этапе сможет поддерживать система GPRS, равна 107 Кбит/с.

Сегодня основные ограничения накладывают абонентские терминалы. Скорость приема и передачи информации, которую может обеспечить мобильный терминал, зависит от количества каналов, которые терминал поддерживает на прием и передачу. Один канал поддерживает передачу информации с максимальной скоростью 13.4 кбит/с. Таким образом, количество каналов, которые будет поддерживать конкретная модель терминала будет определять максимальные возможные скорости, на которых возможна передача и прием информации.

Существующие абонентские терминалы GPRS поддерживают от 2 до 4 каналов для приема информации и до 2 каналов для передачи, что позволяет получить максимальную скорость приема до 53,6 кбит/с и передачи до 26.8

кбит/с. В последующем ожидается появление моделей GPRS терминалов, поддерживающих большее количество каналов (до 7).

При использовании системы пакетной передачи абонент получает и отправляет данные с переменной скоростью, которая определяется условиями распространения сигнала и наличием свободных каналов в пределах заданной соты. При этом динамическое выделение каналов производится исходя из приоритета голосовых каналов, т. е. система автоматически выделяет под пакетную передачу все каналы, не занятые передачей голоса. Таким образом, реальная скорость приема и передачи будет во многом зависеть от загруженности голосовых каналов в пределах каждой конкретной соты.

Перспектива появления новых аппаратов с поддержкой большого количества каналов, а значит, работающих на максимально возможных скоростях передачи данных (до 115 Кбит/с), вызывает определенное беспокойство у некоторых специалистов. Дело в том, что потенциально устройства GPRS при работе на высоких частотах могут выходить за рамки максимально допустимого уровня радиационного излучения. Повторим еще раз, речь идет только о высоких скоростях обмена, поскольку, например, канал GPRS, работающий со скоростью 30-40 Кбит/с (а именно такая скорость нам светит в ближайшем будущем), излучает максимум 0.75 Вт. Это конечно больше, чем фактическое излучение терминала стандарта GSM, но в пределах нормы. Средний уровень мощности излучения еще ниже, поскольку передатчик работает только тогда, когда передаются данные, а в остальное время он выключен. При передаче файла из телефона в базовую станцию передатчик работает постоянно; при передаче текстовых сообщений или вовремя веб-браузинга он включается редко, что снижает мощность излучения до нескольких милливатт.

Перспективы развития услуг на базе GPRS и пакетной передачи. Появление технология GPRS должно значительно ускорило развитие мобильной передачи данных во всех областях человеческой деятельности. Во

многом это связано с появлением новых услуг, развитие которых было затруднено из-за низкой скорости и высокой стоимости передачи данных через голосовые каналы GSM. Технология GPRS позволяет абонентам получать доступ в глобальную сеть из любой точки, где существует покрытие сети, при этом цена такой передачи чрезвычайно привлекательна, а введении повременной оплаты на фиксированных телефонных линиях, тарифы на доступ в Интернет с мобильного GPRS-телефона стали еще более конкурентоспособны.

Для корпоративных пользователей появление услуг на основе технологии GPRS позволило реализацию давней мечты полностью мобильного офиса с доступом, как в глобальную, так и в корпоративную сеть своей фирмы, с гарантией безопасного соединения. Практически исчезла проблема доступа к корпоративной сети во время командировок, в том числе и зарубежных, поскольку организация GPRS-роуминга обеспечивает безопасный, дешевый и высокоскоростной доступ к любому ресурсу корпоративной сети. Существуют множество приложений промышленного применения данной технологии для различных задач подвижного мониторинга и контроля состояния объектов.

Следует отметить, что GPRS является идеальным транспортом для WAP-приложений, практически все телефоны с поддержкой GPRS имеют встроенный WAP-браузер, что позволит их владельцам не только передавать данные, но и получать оперативную информацию с различных WAP-серверов.

*Перспективы пакетной передачи данных***.** Система GPRS является первым шагом на пути развития сетей беспроводной пакетной передачи данных. Первоначально услуги на основе GPRS предоставлялись на ограниченной территории действия сотовой связи. В настоящее время зона, где представляются услуги на основе GPRS, расширена до всей территории действия сети сотовой связи. Также увеличены скоростей приема и передачи

информации за счет улучшения характеристик мобильных терминалов и инфраструктуры GPRS.

Следующим шагом на пути развития сетей пакетной передачи данных является внедрение технологии EDGE, которая позволяет достичь скорости передачи информации до 385 Кбит/с, при этом базой для развертывания технологии EDGE частично служит система GPRS. Таким образом, был осуществлен плавный переход от систем с коммутацией каналов к системам пакетной передачи данных, которые нашли свою конечную реализацию в системах передачи информации третьего и последующих поколений, позволяющих обеспечить абонентам скорости передачи свыше 2 Мбит/с.

Особенности технологии EDGE. Технология EDGE может внедряться двумя разными способами: как расширение GPRS, в этом случае ее следует называть EGPRS (enhanced GPRS) или как расширение CSD (ECSD). GPRS распространена намного шире, чем HSCSD, поэтому будем рассматривать EGPRS [8-10].

EDGE не является новым стандартом сотовой связи, однако, EDGE подразумевает дополнительный физический уровень, который может быть использован для увеличения пропускной способности сервисов GPRS или HSCSD. В этом случае сами сервисы предоставляются точно так же, как и раньше. Теоретически сервис GPRS способен обеспечивать пропускную способность до 160 Кбит/с (на физическом уровне, на практике же поддерживающие GPRS Class 10 или 4+1/3+2 аппараты обеспечивают лишь до 38-42 Кбит/с и то, если позволяет загруженность сети сотовой связи), а EGPRS — до 384-473,6 Кбит/с. Следует однако при этом использовать новую модуляционную схему, новые методы кодирования каналов и коррекции ошибок.

EDGE, по сути, является «надстройкой» (вернее, подстройкой, если считать, что физический уровень находится ниже остальных) к GPRS и не может существовать отдельно от GPRS. EDGE, как уже было сказано выше,

подразумевает использование иных модуляционных и кодовых схем, сохраняя совместимость с CSD-сервисом голосовой связи.

Таким образом, с точки зрения клиентского терминала, внедрение EDGE ничего не изменяет. Однако, инфраструктура базовой станции претерпит некоторые изменения (рисунке 1.4), хотя и не такие уж серьезные.

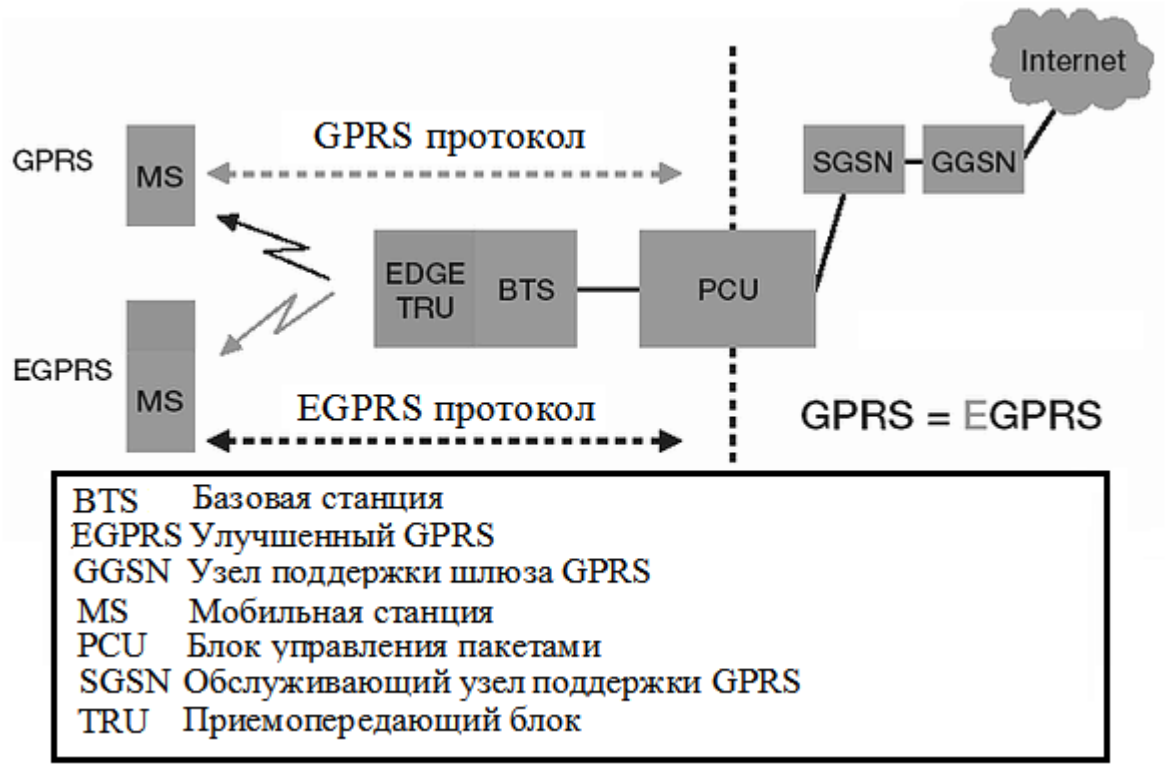


Рис. 1.4. Отличия между EDGE и GPRS

Помимо увеличения пропускной способности для передачи данных, внедрение EDGE увеличивает емкость сети сотовой связи, так как в один и тот же тайм-слот можно теперь «упаковать» большее количество пользователей, соответственно, можно надеяться не получать сообщение «сеть занята» в самые неподходящие моменты.

Таблица 1.1. иллюстрирует разные технические характеристики EDGE и GPRS. Хотя и в EDGE, и в GPRS в единицу времени отправляется одинаковой число символов, благодаря использованию другой модуляционной схемы, число бит данных в EDGE втрое больше.

Таблица 1.1.

Сравнительные характеристики EDGE и GPRS

	GPRS	EDGE
Модуляционная схема	GMSK	8-PSK/GMSK
Скорость передачи символов	270 тыс. в секунду	270 тыс. в секунду
Пропускная способность	270 Кбит/с	810 Кбит/с
Пропускная способность на тайм-слот	22,8 Кбит/с	69,2 Кбит/с
Скорость передачи данных на тайм-слот	20 Кбит/с (CS4)	59,2 Кбит/с (MCS9)
Скорость передачи данных с использованием 8 тайм-слотов	160 (182,4) Кбит/с	473,6 (553,6) Кбит/с/s

Сразу оговоримся здесь, что приведенные в таблице значения пропускной способности и скорости передачи данных отличаются друг от друга из-за того, что в первой также учитываются заголовки пакетов, пользователю ненужные. Ну, а максимальная скорость передачи данных в 384 Кбит/с (требуемая для соответствия спецификациям IMT-2000) получается в том случае, если используется восемь тайм-слотов, то есть, на каждый тайм-слот приходится по 48 Кбит/с.

Модуляционная схема EDGE. В стандарте GSM применяется модуляционная схема GMSK (Gaussian minimum shift keying, кодирование по сдвигу Гауссового минимума), являющейся разновидностью фазовой модуляции сигнала. Для пояснения принципа схемы GMSK рассмотрим фазовую диаграмму на рисунке1.5, на которой изображена действительная (I) и мнимая (Q) часть комплексного сигнала. Фаза передаваемых логических «0» и «1» отличаются друг от друга фазой π. Каждый передаваемый в единицу времени символ соответствует одному биту.

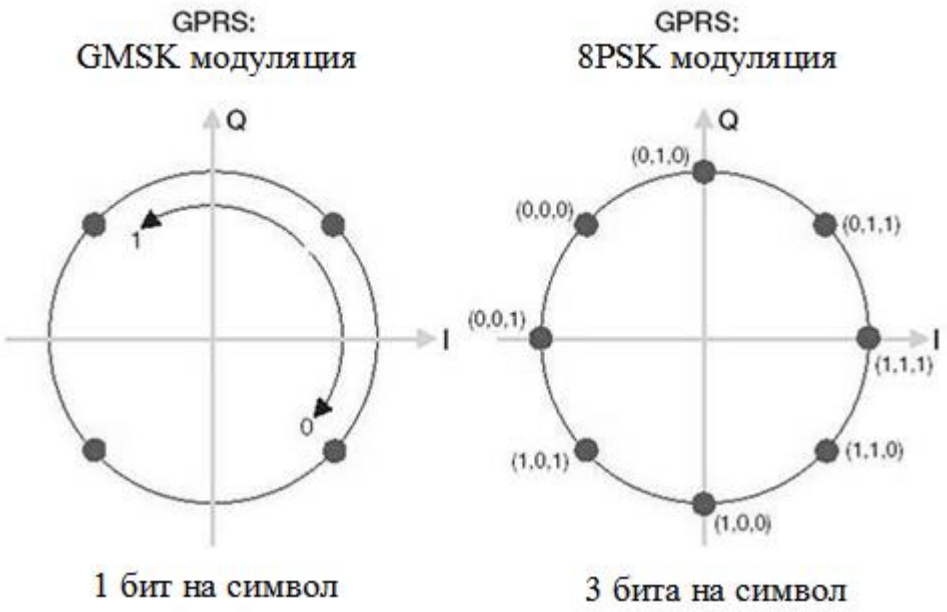


Рис. 1.5. Разные модуляционные схемы в GPRS и EDGE

В технологии EDGE применяется модуляционная схема 8PSK (8-phase shift keying, сдвиг фазы, как видно из рисунка, равен π/4), используя все те же спецификации структуры частотных каналов, кодирования и ширины полос, как в GSM/GPRS. Соответственно, соседние частотные каналы создают ровно те же взаимные помехи, как и в GSM/GPRS. Меньший сдвиг фазы между символами, в которые теперь кодируется не один бит, а три (символы соответствует комбинациям 000, 001, 010, 011, 100, 101, 110 и 111), делает задачу детектирования сложнее, особенно если уровень сигнала невысок. Впрочем, в условиях хорошего уровня сигнала и стабильного приема, дискриминировать каждый символ не составляет большого труда.

Кодирование. В GPRS возможно применение четырех разных схем кодирования: CS1, CS2, CS3 и CS4, в каждой из которых используется свой алгоритм коррекции ошибок. Для EGPRS разработано девять схем кодирования, MCS1..MCS9, соответственно, назначение которых также в обеспечении коррекции ошибок. Причем в «младших» MSC1..MSC4 используется модуляционная схема GMSK, в «старших» MSC5..MSC9 — модуляционная схема 8PSK.

Характеристики кодовых схем EGPRS приведены в таблице 1.2, а на рисунке 1.6. представлена зависимость скорости передачи данных от использования разных модуляционных схем вкупе с разными схемами кодирования (скорость передачи данных меняется в зависимости от того, как много требуемой для работы алгоритмов коррекции ошибок избыточной информации закладывается в каждый кодируемый пакет). Нетрудно догадаться, что чем хуже условия приема (отношение сигнал/шум), тем больше приходится закладывать избыточной информации в каждый пакет, а значит, тем меньше скорость передачи данных. Небольшое отличие в скорости передачи данных, наблюдаемое между CS1 и MCS1, CS2 и MCS2, и т. д., связано с разницей в величине заголовков пакетов.

Таблица 1.2.

Характеристики кодовых схем EGPRS

Схема кодирования (MCS)	**Скорость (кбит/с/слот)**	**Модуляция**
MCS-1	8.8	GMSK
MCS-2	11.2	GMSK
MCS-3	14.8	GMSK
MCS-4	17.6	GMSK
MCS-5	22.4	8-PSK
MCS-6	29.6	8-PSK
MCS-7	44.8	8-PSK
MCS-8	54.4	8-PSK
MCS-9	59.2	8-PSK

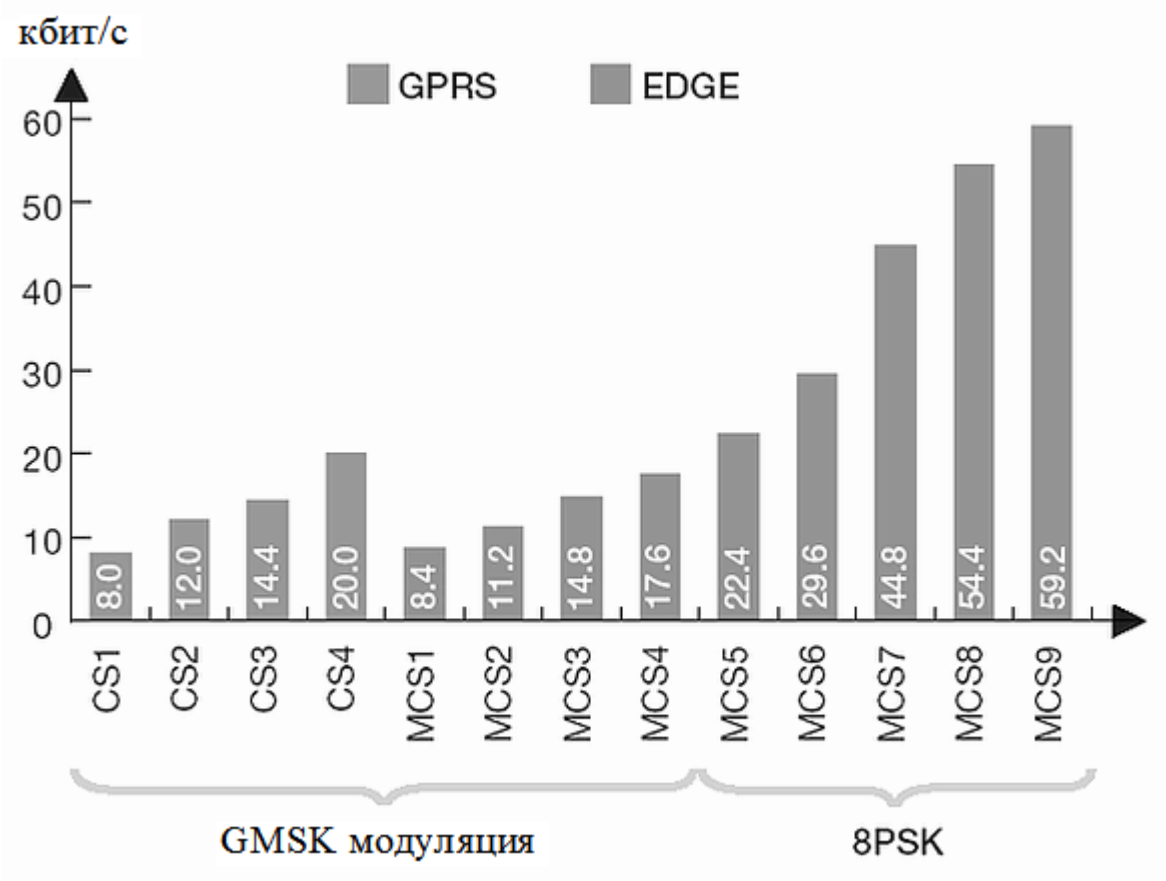


Рис. 1.6. Разные кодовые схемы в GPRS и EDGE

Впрочем, если соотношение сигнал/шум невелико, не все потеряно: в старших модуляционно-кодовых схемах EGPRS MCS7, MCS8, MCS9 предусмотрена процедура «наложения»: так как стандарт способен отправлять группы пакетов на разных несущих (внутри частотного диапазона), для каждой из которых условия (и прежде всего — «зашумленность») могут быть разными, в этом случае повторной передачи всего блока можно избежать, если знать, в какой группе произошел сбой и повторно транслировать именно эту группу. В отличие от старшей кодовой схемы GPRS CS4, где не используется аналогичный алгоритм коррекции ошибок, в EGPRS MCS7, MCS8, MCS9 разные блоки данных «накладываются» друг на друга, поэтому при сбое в одной из групп (как показано на рисунке), повторной пересылке подлежит лишь половина пакетов (рис. 1.7).

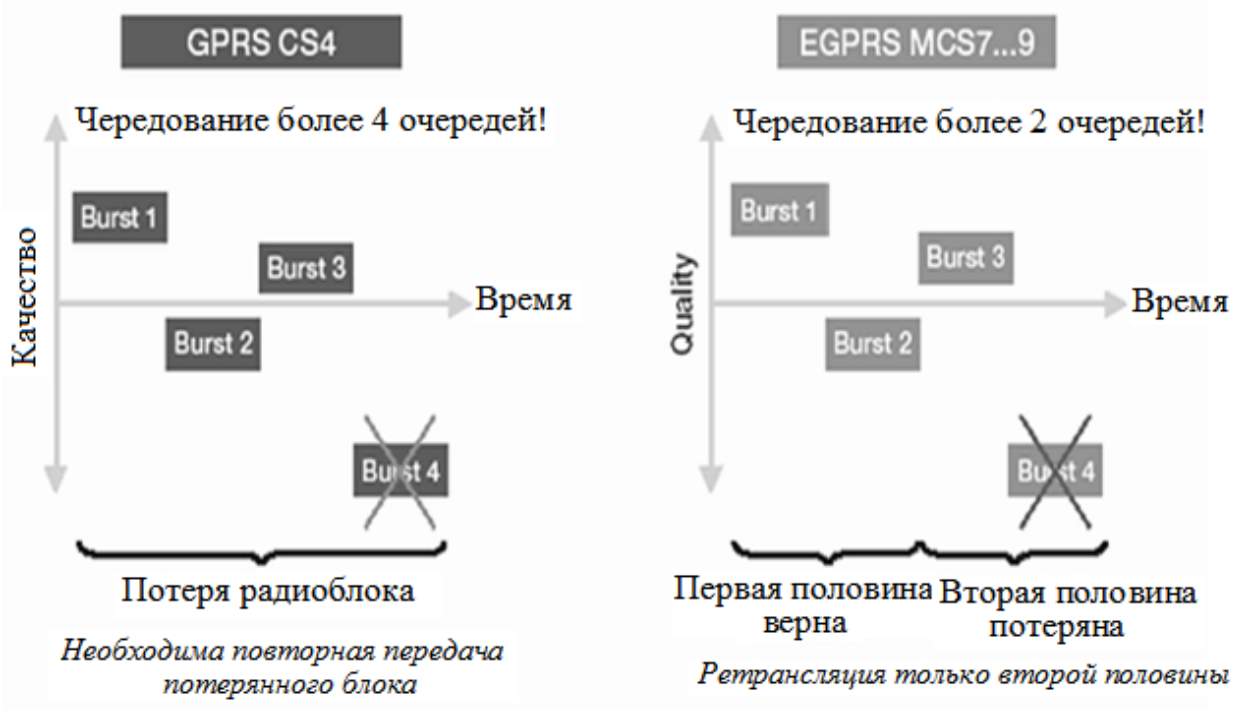


Рис. 1.7. Использование наложения групп пакетов в EDGE

Обработка пакетов. Если по каким-то причинам пакет, отправленный с использованием «старших» схем кодирования, не был корректно принят, EGPRS позволяет его ретранслировать заново с использованием «пониженной» кодировочной схемы. В GPRS такой возможности, названной «ресегментацией» (resegmentation), предусмотрено не было: некорректно принятый пакет отправляется вновь по той же модуляционно-кодировочной схеме, что и в предыдущий раз.

Окно адресации (addressing window).Прежде чем последовательность кодированных (то есть, в которые закодированы «слова», состоящие из нескольких бит) пакетов (фрейм) может быть передана по радиочастотному интерфейсу, передатчик присваивает пакетам идентификационный номер, включенный в заголовок каждого пакета. Номера пакетов в GPRS составляют от 1 до 128. После того, как последовательность пакетов (например, 10 штук) отправлена адресату, передатчик ждет от приемника подтверждения того, что они были приняты. В отчете, который приемник отправляет обратно передатчику, содержатся номера пакетов, которые были успешно

декодированы, и которые получатель декодировать не смог. Важный нюанс: номера пакетов принимают значения от 1 до 128, а ширина адресного окна — всего 64, вследствие чего вновь передаваемый пакет может получить такой же номер, как в предыдущем фрейме. В этом случае протокол вынужден повторно отправлять весь текущий фрейм, что отрицательно сказывается на скорости передачи данных в целом. Для снижения риска возникновения такой ситуации в EGPRS номер пакета может принимать значения от 1 до 2048, а адресное окно увеличено до 1024.

*Точность измерения***.** Для обеспечения корректного функционирования технологии GPRS в среде GSM приходится постоянно измерять радиоусловия: уровень сигнал/шум в канале, частоту появления ошибок и т. п. Эти измерения никак не сказываются на качестве голосовой связи, где достаточно постоянно использовать одну и ту же кодировочную схему. При передаче данных в GPRS измерение радиоусловий возможно лишь в «паузах» — дважды за период 240 мс. Для того, чтобы не ждать каждые 120 мс, EGPRS определяет такой параметр, как вероятность возникновения ошибки на бит (BEP, bit error probability), в каждом фрейме. На величину BEP влияет как отношение сигнал/шум, так и временная дисперсия сигнала и скорость перемещения терминала. Изменение BEP от фрейма к фрейму позволяет оценить скорость терминала и «дрожание» частоты, но для более точной оценки используется среднее значение вероятности ошибки на бит на каждые четыре фрейма и его выборочное стандартное отклонение. Благодаря этому, EGPRS быстрее реагирует на изменения условий: увеличивает скорость передачи данных при снижении BEP и наоборот.

*Контроль за скоростью соединения в EGPRS***.** В EGPRS используется комбинация двух подходов: подстройки скорости соединения и инкрементной избыточности. Подстройка скорости соединения, измеряемой либо мобильным терминалом по количеству принимаемых в единицу времени данных, либо базовой станцией по количеству, соответственно, передаваемых данных, позволяет выбрать оптимальную модуляционно-

кодовую схему для последующих объемов данных. Обычно, использование новой модуляционно-кодовой схемы может быть назначено при передаче нового блока (по четыре группы) данных.

Инкрементная избыточность изначально применяется для самой старшей модуляционно-кодовой схемы, MCS9, с незначительным вниманием к коррекции ошибок и без учета условий радиосвязи. Если информация декодируется адресатом некорректно, по каналу связи передаются не сами данные, а некий контрольный код, который «добавляется» (используется для преобразования) к уже загруженным данным до тех пор, пока данные не будут декодированы успешно. Каждый такой «инкрементный кусочек» дополнительного кода увеличивает вероятность успешной расшифровки переданных данных — в этом и заключается избыточность. Главным преимуществом этого подхода является то, что здесь нет необходимости следить за качеством радиосвязи, поэтому инкрементная избыточность является обязательной в стандарте EGPRS для мобильных терминалов.

Интеграция EGPRS в существующие GSM/GPRS. Как уже было сказано выше, главное различие между GPRS и EGPRS — в использовании иной модуляционной схемы на физическом уровне. Поэтому для поддержки EGPRS достаточно установки на базовой станции поддерживающего новые модуляционные схемы трансивера и программного обеспечения для обработки пакетов. Для обеспечения совместимости с не поддерживающими EDGE мобильными телефонами, в стандарте прописано следующее:

- поддерживающие и не поддерживающие EDGE мобильные терминалы должны быть способны использовать один и тот же тайм-слот;
- поддерживающие и не поддерживающие EDGE трансиверы должны использовать один и тот же частотный диапазон;
- возможна частичная поддержка EDGE;
- для облегчения процесса внедрения на рынок новых мобильных телефонов подразделяют EDGE - совместимые терминалы на два класса: поддерживающие модуляционную схему 8PSK только в приемном

потоке данных (downlink) и поддерживающие 8PSK как в приемном, так и в передающем (uplink) потоке данных.

Внедрение EGPRS позволяет достичь пропускной способности, примерно втрое больше, чем в технологии GPRS. При этом используется в точности такие же профили QoS (quality of service, качество сервиса), как в GPRS, но с учетом увеличившейся пропускной способности. Помимо необходимости установки трансивера на базовой станции, для поддержки EGPRS обновляется программное обеспечения, которое обрабатывает измененный протокол передачи пакетов.

Таким образом, технология EDGE обеспечивает качественное улучшение радиоинтерфейса без существенных изменений существующих стандартов сетей второго поколения, т.е. EDGE предоставляет те же услуги, что и GPRS, как, например, получить доступ к ресурсам Интернета, получать и отправлять сообщения электронной почты, скачивать картинки, мелодии, игры и видеофайлы с WAP-сайтов, обмениваться MMS-сообщениями в несколько раз быстрее, чем через GPRS, а также новые услуги реального времени, как IP-телефония, мобильное телевидение и он-лайн приложения (игры), и является следующим качественным шагом на пути построения и введения нового (третьего) поколения мобильных сетей.

1.4. Географические зоны сети GSM

Каждая телефонная сеть нуждается в определенной структуре для маршрутизации вызовов к требуемой станции и далее к абоненту. В сети мобильной связи эта структура особенно важна, так как абоненты перемещаются по сети, то есть меняют свое местоположение и это местоположение должно постоянно отслеживаться [5-8].

Сота является базовым элементом сотовой системы и определяется как область радиопокрытия, обеспечиваемого одной антенной одной базовой станции (рис.1.8). Каждой соте назначается свой уникальной номер,

называемый Глобальным идентификатором соты (CGI). В сети, охватывающей, например, целую страну, число сот может быть очень большим.

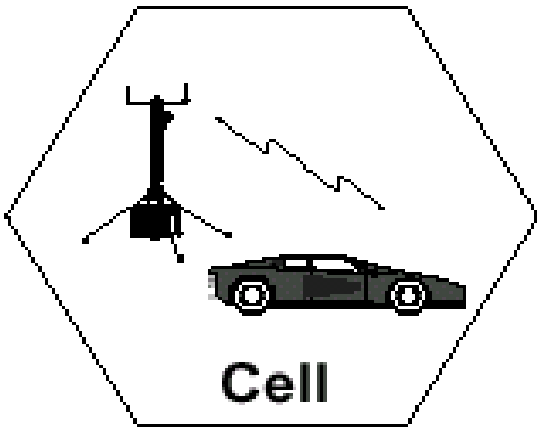


Рис. 1.8. Сотовая ячейка

Зона местоположения (LA) определяется как группа сот. Местоположение абонента в пределах сети связано с той LA, в которой в данный момент находится абонент. Идентификатор данной LA хранится в VLR.

Когда MS пересекает границу между двумя сотами, принадлежащими различным LA, она передает в сеть информацию о новой LA. Это происходит только в том случае, если MS находится в режиме «Свободно» (Idle). Информация о новом местоположении не передается в течение установленного соединения, этот процесс будет происходить после освобождения соединения. Если MS пересекает границу между сотами в пределах одной LA, она не сообщает сети о своем новом местоположении. При поступлении входящего вызова к MS пейджинговое сообщение распространяется в пределах всех сот, принадлежащих одной LA.

Зона обслуживания MSC (SA)состоит из некоторого числа LA и отображает географическую часть сети, находящуюся под управлением одного MSC (рис.1.9). Для того, чтобы направить вызов к MS информация о зоне обслуживания MSC также необходима, поэтому зона обслуживания

также отслеживается, и информация о ней записывается в базе данных (HLR).

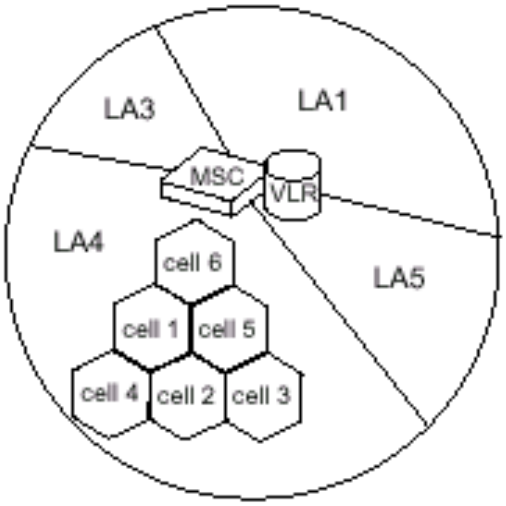


Рис. 1.9. Зона обслуживания MSC

Зона обслуживания PLMN. Представляет собой совокупность сот, обслуживаемых одним оператором и определяется как зона, в которой оператор обеспечивает абоненту радиопокрытие и доступ к своей сети. В любой стране может быть несколько зон обслуживания PLMN, по одной на каждого оператора. Определение роуминг употребляется в случае перемещения MS из одной области обслуживания PLMN в другую. На рисунке 1.10. представлены соотношения между различными областями обслуживания.

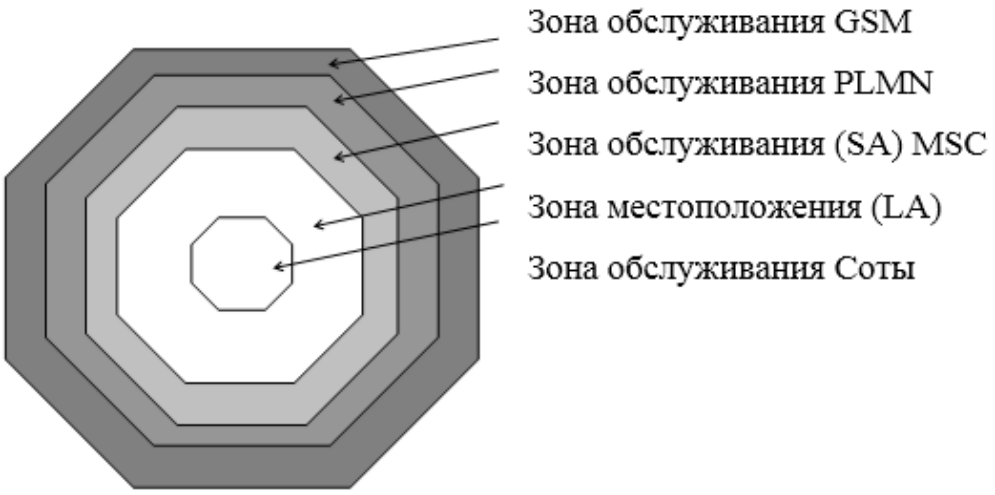


Рис. 1.10. Иерархическая взаимосвязь между зонами GSM

Зона обслуживания GSM. Представляет собой всю географическую область, в которой абонент может получить доступ к сети GSM. Зона обслуживания GSM увеличивается по мере того, как новые операторы подписывают контракты, предусматривающие совместную работу по обслуживанию абонентов. В настоящее время зона обслуживания GSM охватывает с некоторыми промежутками многие страны от Ирландии до Австралии и от Южной Африки до Америки. Международный роуминг – это термин, который применяется в том случае, когда MS перемещается от одной национальной PLMN в другую национальную PLMN.

На рисунках 1.11. и 1.12. представлены различные точки зрения на одну и туже сеть. Первый отражает расположения узлов сети и их взаимодействие на уровне аппаратного обеспечения, а второй отражает географическую структуру сети на уровне программного обеспечения.

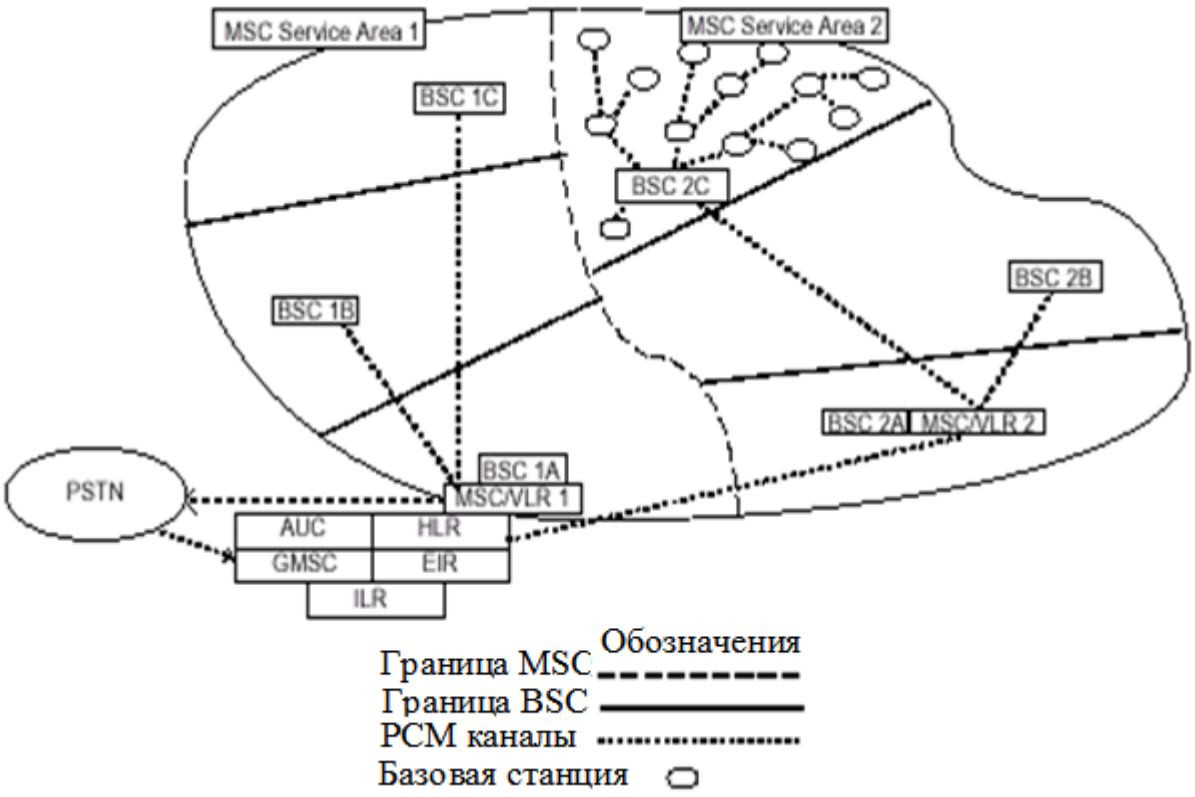


Рис. 1.11. Расположение узлов сети и их взаимодействие на уровне аппаратного обеспечения

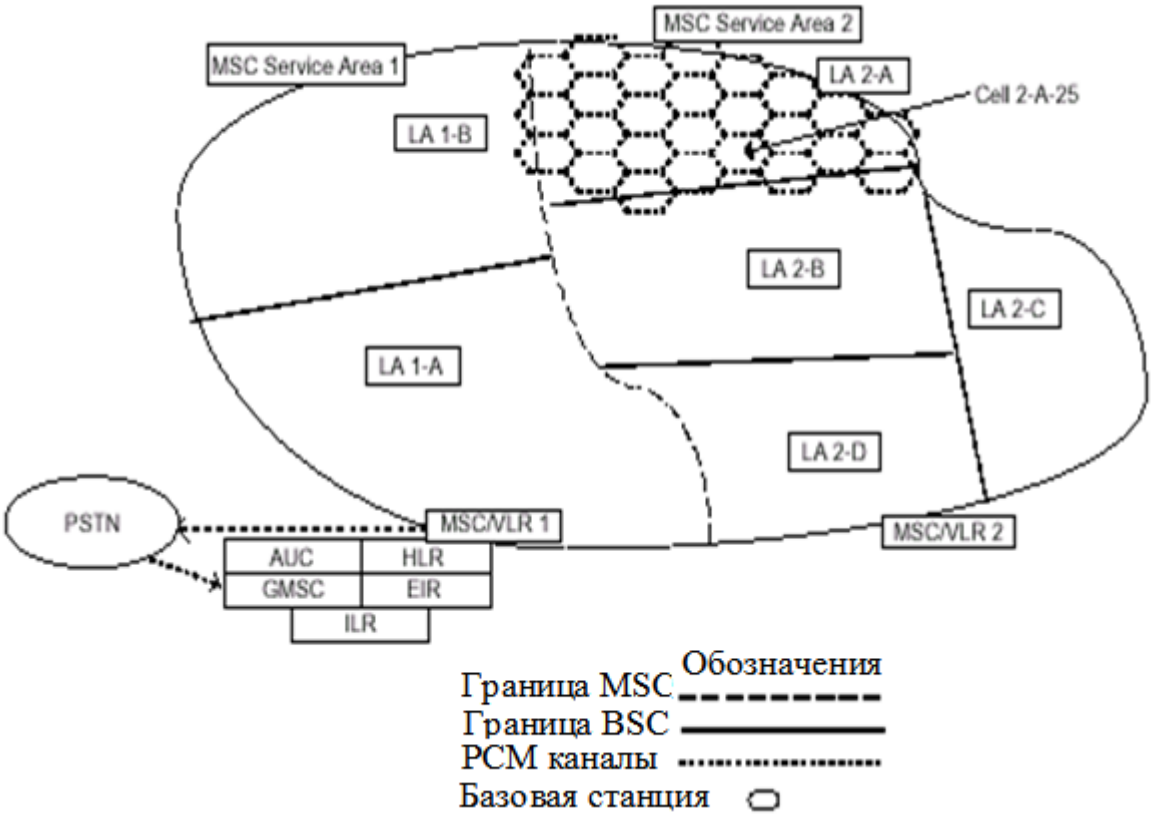


Рис. 1.12. Расположение узлов сети и их взаимодействие на уровне программного обеспечения

Частотный диапазон GSM включает в себя три диапазона частот: 900, 1800, 1900 МГц. (рис.1.13).

Диапазон 900 МГц

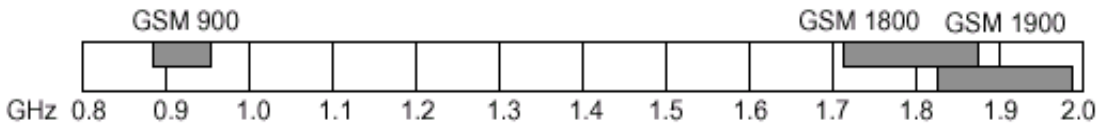


Рис.1.13. Частотные диапазоны GSM

Изначально под стандарт GSM был выделен диапазон 900 МГц. В настоящее время данный диапазон остаётся всемирным. В некоторых странах используются расширенные диапазоны частот, обеспечивающие большую ёмкость сети. Расширенные диапазоны частот называются E-GSM и R-GSM, в то время как обычный диапазон носит название P-GSM (primary).

- P-GSM900 890-915/915-960 MHz
- E-GSM900 880-915/925-960 MHz
- R-GSM900 890-920/915-970 MHz

Диапазон 1800 МГц. В 1990 г. для увеличения конкуренции между операторами, United Kingdom начали развивать новую версию GSM, которая адаптирована к диапазону частот 1800. Сразу после утверждения данного диапазона несколько стран сделали заявку на использование данного диапазона частот. Введение данного диапазона увеличило рост количества операторов, приводя к увеличению конкуренции и, соответственно, улучшению качества обслуживания. Применение данного диапазона позволяет увеличивать емкость сети за счёт увеличения полосы пропускания и, соответственно, увеличение несущих. Диапазон частот 1800 использует следующие пары дуплексных частот: GSM 1710-1805/1785-1880 MHz.

До 1997 года стандарт 1800 носил название Digital Cellular System (DCS) 1800 MHz, в настоящее время носит название GSM 1800.

Диапазон 1900 МГц. В 1995 году в США была специфицирована концепция PCS (Персональные услуги связи). Основной идеей этой концепции является возможность предоставления персональной связи, то есть связи между двумя абонентами, а не между двумя мобильными станциями. PCS не требует, чтобы эти услуги были реализованы на основе сотовой технологии, но в настоящее время эта технология признана наиболее эффективной для данной концепции. Частоты, доступные для реализации PCS, находятся в области 1900 МГц. Поскольку в Северной Америке стандарт GSM 900 не может быть использован из-за того, что эта полоса частот занята другим стандартом, стандарт GSM 1900 является возможностью заполнения этого пробела. Основным различием между американским стандартом GSM 1900 и GSM 900 является то, что GSM 1900 поддерживает сигнализацию ANSI.

Диапазон GSM 800. Традиционно полоса 800 МГц была занята распространенным в США стандартом TDMA (AMPS и D-AMPS). Как и в случае со стандартом GSM 1800 этот стандарт дает возможность получения дополнительных лицензий, то есть расширяет область работы стандарта на национальных сетях предоставляя операторам дополнительную емкость.

В таблице 1.3 снесены сравнительные данные различных частотных диапазонов.

Таблица 1.3.

Диапазоны частот

Передача	**Диапазоны частот**				
	P-GSM 900	**E-GSM 900**	**R-GSM 900**	**GSM 1800**	**GSM 1900**
Uplink	890 – 915 МГц	880 - 915 МГц	890 – 925 МГц	1710 – 1785 МГц	1850 – 1910 МГц
Downlink	935 – 960 МГц	925 - 960 МГц	935 – 970 МГц	1805 – 1880 МГц	1930 – 1990 МГц

Состояния мобильной станции. В процессе развития мобильных систем был разработан ряд понятий, описывающих различные состояния мобильной станции.

Мобильная станция может иметь несколько состояний.

- **Idle («Свободно»)**: MS включена, но разговор не установлен;
- **Active («Активный режим»)**: MS включена, режим установленного соединения;
- **Detached**: MS выключена
- **Implicit Detach**: MS не выходила на связь продолжительное время.

В таблице 1.4. приводятся ключевые понятия, которые помогают описать GSM режимы обслуживания трафика.

Регистрация МС и роуминг представлена на рисунке 1.14.

Таблица 1.4.

Состояния мобильной станции

Состояние	**Термин**	**Определение**
IDLE	Регистрация (Registration)	Процесс, когда MS сообщает системе о ее включении
	Роуминг (Roaming)	Режим, когда MS двигается по всей сети в свободном режиме
	Интернациональный роуминг (International Roaming)	Режим, когда MS уезжает в зону действия других операторов. MS будет в роуминге тогда, когда с другим оператором достигнуто роуминговское соглашение
	Location Updating	MS сообщает системе о том, что она вошла в новую LA
	Paging	Процесс, когда MS вызывается системой, т.е. когда MS получает вызывное сообщение с идентификационным номером MS
ACTIVE	Handover	Процесс эстафетной передачи, при движении MS через несколько сот

Когда MS выключается, в системе мобильная станция отмечается как Detach. Когда MS включается, она начинает сканировать весь частотный GSM диапазон, используя при этом специальные каналы управления. После того как MS находит каналы, она начинает измерять уровни сигнала на этих каналах, после чего эти данные запоминаются в MS. После того, как каналы были измерены, МС выбирает наилучший канал.

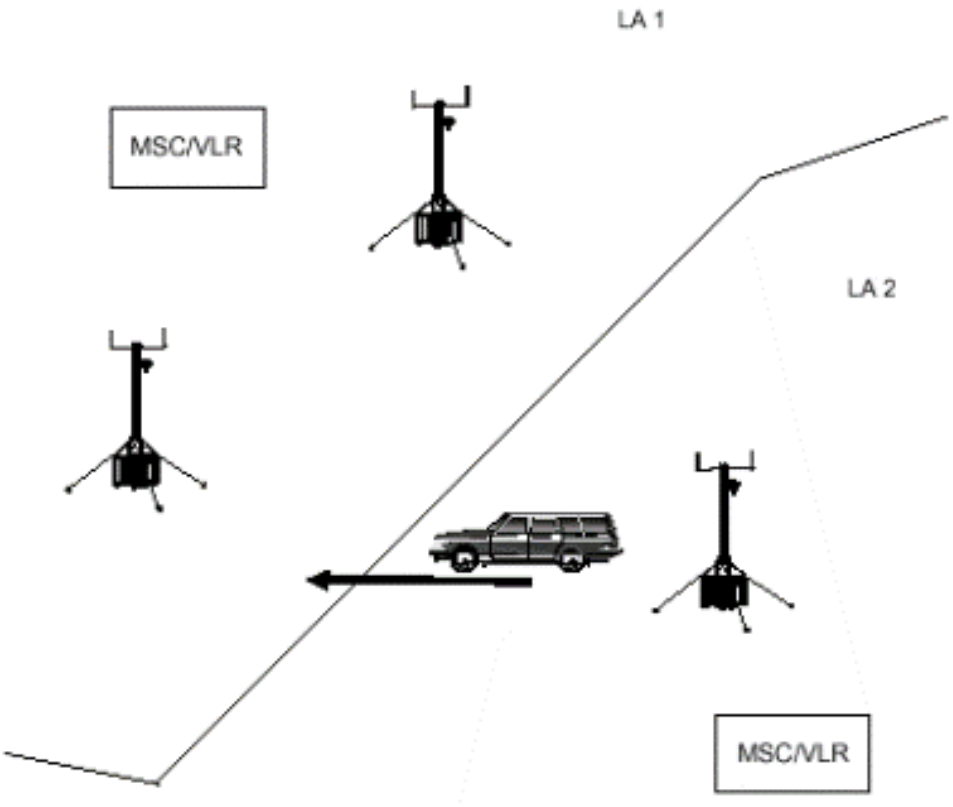


Рис. 1.14. Роуминг

После того как MS включилась, она должна зарегистрироваться в системе, после чего система помечает её как мобильную станцию в состоянии IDLE. Если оказывается, что MS находится в другой LA, то MS осуществляет процедуру обновления своего местоположения.

В процессе движения по сети MS постоянно сканирует каналы для определения канала с наибольшим уровнем сигнала. Если MS находит лучшую частоту, она перестраивается на неё. Если новая частота принадлежит новой LA, то система также оповещает об этом MS.

Принцип иерархии федеральной сети общего пользования GSM. Федеральная сеть GSM представляет иерархическую структуру, принцип построения которой приведен на рисунке 1.15.

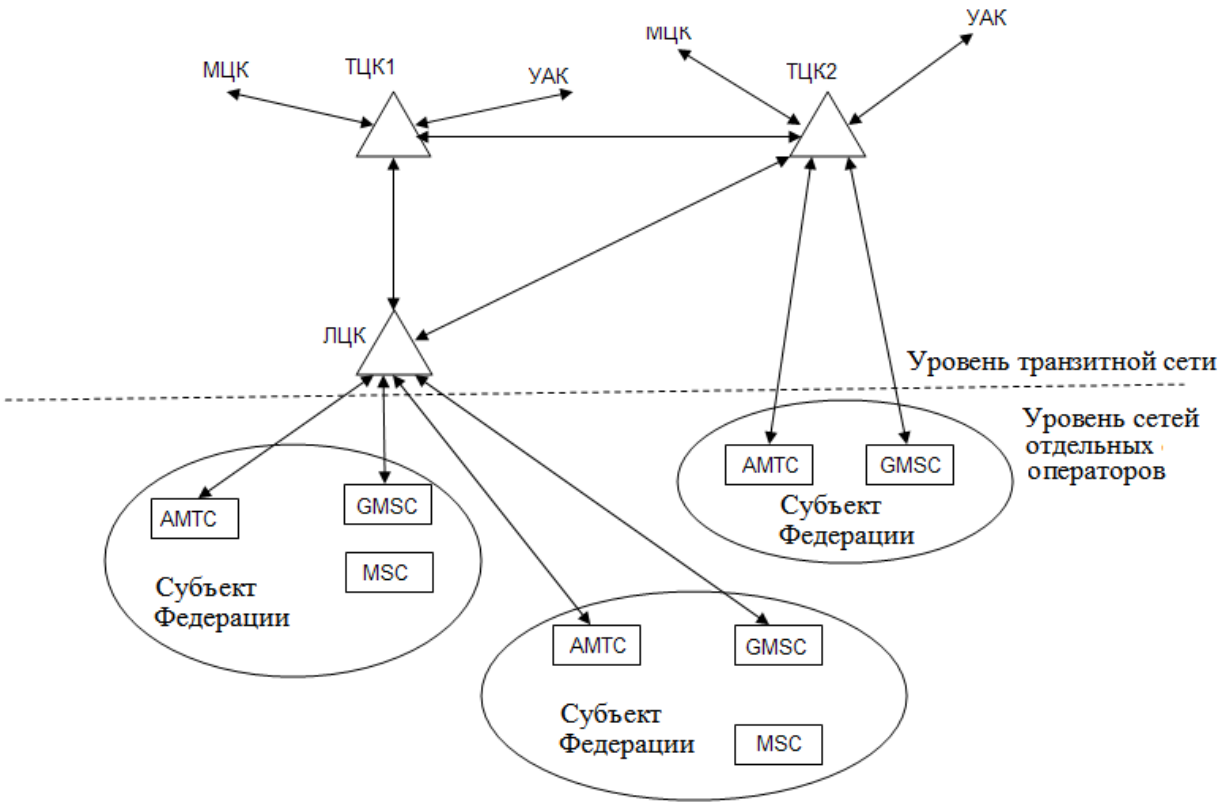


Рис. 1.15. Принцип иерархии федеральной сети общего пользования GSM

Первый уровень включает мобильные центры коммутации MSC, шлюз мобильного центра коммутации. Взаимодействие сети GSM со стационарной сетью ТфОП осуществляется через шлюз мобильного центра коммутации GMSC подключением к АМТС (основной вариант) и к АТС при значительном тяготении нагрузки абонентов на местном уровне. Второй уровень иерархии GSM- транзитная сеть, представляющая собой транзитные центры коммутации (ТЦК), выполняющие для мобильных абонентов те же функции, что и УАК для ТфОП. Все ТЦК соединены между собой по полносвязной схеме. При взаимодействии федеральной сети GSM с фиксированной сетью ТфОП на международном уровне возможны соединения мобильной станции MS с телефонным аппаратом (ТА) стационарной сети ТфОП:

MS – MSC – GMSC - ТЦК – УАК – АМТС – АТС – ТА

Кроме ТЦК уровень транзитной сети может включать также локальные центры коммутации (ЛЦК). ЛЦК является промежуточным уровнем

иерархии федеральной сети GSM. ЛЦК является узлом доступа к транзитной сети и соединяется не менее чем с двумя ТЦК. В этом случае взаимодействие мобильной станции и стационарного телефонного абонента при междугородней связи осуществляется по схеме:

MS – MSC – GMSC - ЛЦК – ТЦК - УАК – АМТС – АТС – ТА

Контрольные вопросы

1. Как классифицируются мобильные системы радиосвязи?
2. Поясните, в чем состоит принцип частотно-упаковывающей модели.
3. Поясните необходимость перехода к ССПС 2G.
4. Что означает аббревиатура GSM, когда и кем она была введена?
5. Какой способ передачи радиосигнала используется в стандарте GSM и поясните его?
6. Какими преимуществами обладает стандарт GSM, по сравнению с другими цифровыми стандартами?
7. Какие услуги предоставляются в стандарте GSM?
8. Какие диапазоны частот выделены для работы в стандарте GSM?
9. Приведите и поясните архитектуру сети GSM.
10. Приведите и поясните блок-схему приемо-передатчика мобильной станции.
11. Поясните, что понимается под подсистемой базовых станций.
12. Поясните коммутационную подсистему сети.
13. Назначение домашнего регистра местоположения (HLR).
14. Назначение визитного регистра местоположения (VLR).
15. Какие существуют внутренние интерфейсы GSM и их назначения.
16. Какие существуют интерфейсы с внешними сетями в GSM и их назначения.
17. Почему возникла необходимость модернизации стандарта GSM?
18. Как осуществляется передача данных в GSM и GPRS?

19. Поясните принципы построения системы GPRS.
20. Какое терминальное оборудование используется в GPRS?
21. Какие скорости передачи предусмотрены в системе GPRS**?**
22. Какие перспективы развития услуг ожидается на базе GPRS?
23. Какие перспективы у пакетной передачи данных?
24. В чем состоят особенности технологии EDGE?
25. Какие модуляционные схемы используются в EDGE?
26. Как осуществляется интеграция EGPRS в существующие GSM/GPRS?
27. Что понимается под «Сота» в сотовой системе связи?
28. Что понимается под «Зона местоположения (LA)»?
29. Что понимается под «Зона обслуживания MSC (SA)»?
30. Что понимается под «Зона обслуживания PLMN»?
31. Что понимается под «Зона обслуживания GSM»?
32. Какие частотные диапазоны используются в GSM?
33. В каких состояниях может быть мобильная станция в GSM?
34. Как осуществляется регистрация МС и роуминг в сети GSM?
35. Поясните иерархию федеральной сети общего пользования GSM.

ГЛАВА 2. УПРАВЛЕНИЕ МОБИЛЬНОСТЬЮ

2.1. Процедуры управления мобильностью

Управление мобильностью (*Mobility Management*) — одна из основных функций сети GSM, позволяющая работать мобильным телефонам (MS). Задача управления мобильностью заключается в отслеживание местонахождения абонентов, для направления к ним звонков, SMS и других услуг мобильной связи [5-7].

В функции управления мобильностью входят ряд процедур, основными из которых являются:

- Location update;
- Location area;
- Роуминг,

Location update (LU) — процедура обновления информации о местоположении. Как известно, сети GSM, как и все сотовые сети, представляют собой радио сети (BSS - Base station subsystem) состоящие из отдельных базовых станций (BTS) или сот. Каждая базовая станция покрывает небольшой участок территории, который является частью определенной Зоны Местоположения (LA - location area). Благодаря совместной работе базовых станций, сотовая сеть обеспечивает единую зону покрытия на значительных территориях. Группа базовых станций, работающая совместно, называется зоной местоположения, или зоной маршрутизации.

Радиосеть мобильного оператора BSS должна хотя бы примерно представлять, где в настоящий момент находится каждый мобильный телефон (MS-mobile station), чтобы в случае необходимости не искать его по всей территории радиопокрытия. Информация о текущем местоположении предоставляется самим MS с помощью процедуры, называемой LU.

В сети GSM все LA пронумерованы, у каждой есть определенный числовой код - location area code (LAC). Текущий "адрес" телефона в сети - это пара (LAC, Cell ID), где Cell ID - это числовой идентификатор "соты". Пара (LAC, Cell ID) - уникальна в пределах всей сети.

Какая же из сот является "адресом" телефона. В любой момент времени телефон "слушает в эфире" до 16 широковещательных каналов (broadcast channel, BCH) от 16 сот. На основании услышанного он выбирает 6 "лучших" сот, с которыми (по мнению телефона) у него будет максимально устойчивая связь с минимальными затратами энергии. Из этих шести сот телефон выбирает одну "самую лучшую" на основании так называем "критериев C1 и C2" (не будем вдаваться в технические детали о том, что это такое). Именно эту соту телефон постарается использовать для получения или совершения звонка.

Рассмотрим, какую информацию передает при включении телефон и куда она попадает (рис.2.1).

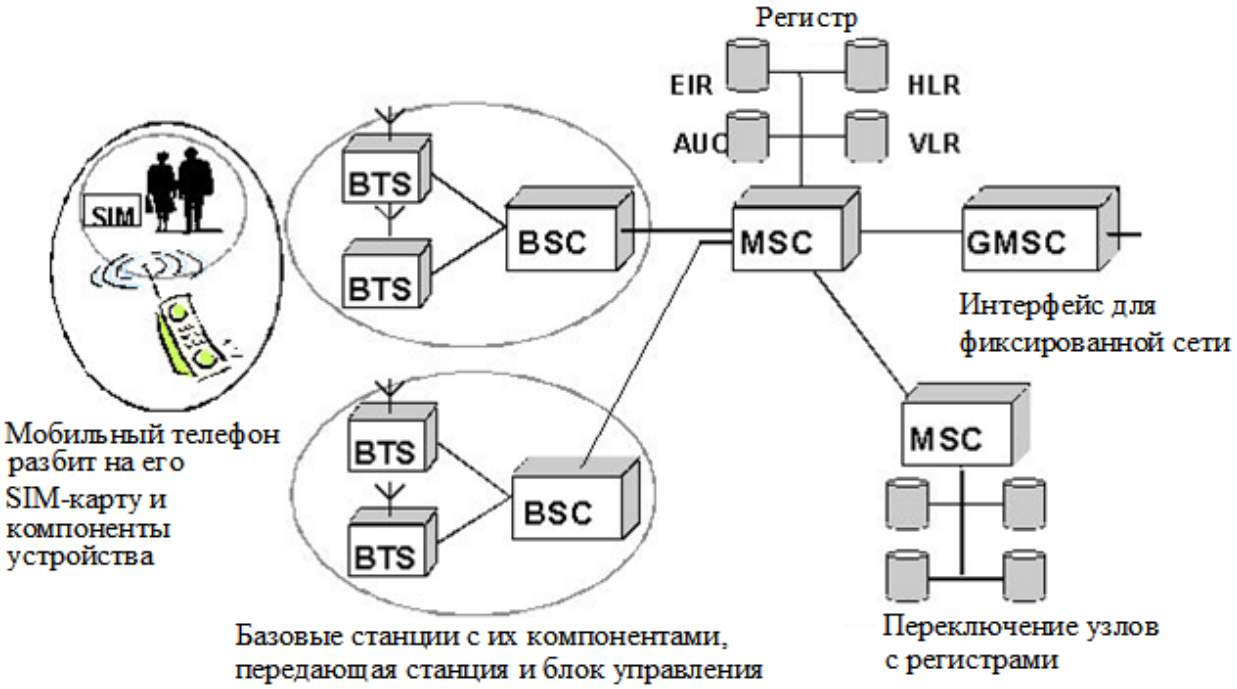


Рис. 2.1. Упрощенная структура сети GSM

После включения телефон пытается зарегистрироваться в сети. В процессе телефон формирует список 6 соседних сот, выбирает из них

лучшую, и использует "общий канал доступа" (RACH) этой соты, чтобы сообщить о том, что его текущее местоположение - тут, в это самой соте. Эта информация (пара (LAC, Cell ID)) попадает в контроллер базовых станций (BSC), а от него - передается коммутатору (MSC), который обслуживает эту часть сети. Коммутатор сохраняет информацию о текущем местоположении телефона в специальном "кэше", называемом VLR (visitor location register). В дальнейшем телефон периодически (обычно раз в час, но зависит от настроек сети) будет выполнять "location update". Либо же, если вы куда-то идете/едете, то телефон будет выполнять "location update" при переходе в зону покрытия соты из другого LA.

Рассмотрим теперь, как используется информация LU. Допустим, нам кто-то звонит. Сеть должна передать вызов на наш телефон, т.е. на ту соту в которой телефон зарегистрировался, или же какую-то из других ближайших.

Чтобы найти эту соту, надо использовать результат последнего LU нашего телефона. Происходит это следующим образом. По номеру телефона определяется, в каком из HLR-ов находится информация о нашей SIM-карте. Далее из этого HLR-а извлекается адрес MSC/VLR-а, в зоне ответственности которого последний раз делали LU и сигнал вызова перенаправляется на этот MSC. Он извлекает из своего VLR информацию о местоположении телефона (LA и Cell ID), и поручает контроллеру базовых станций, который обслуживает эту LA, организовать получение звонка. Контроллер базовых станций опрашивает соты, входящие в LA, а они на частоте своего paging channel (PCCH) сообщают "мобильный такой-то, вам звонок". Дальше телефон и базовая станция договариваются о том, как именно будет принят звонок. Если же вызываемый телефон не отозвался, звонящий получает "ваш абонент находится за пределами зоны покрытия".

Кроме того, информацию, предоставляемую сети в ходе LU, можно использовать также для определения вашего географического местоположения.

При организации процедуры LU мощность, излучаемая передатчиком телефона максимальная, но затем достаточно быстро понижается в ходе power control negotiation (телефон и базовая станция "договариваются" о минимальном уровне мощности, обеспечивающая устойчивую связь). Возникает вопрос, а если мощность большая, то не страдает ли головной мозг и прочие внутренние органы от LU? Официальная позиция: "еще неизвестно". Понятно, что мозг (если держать телефон у уха) нагревается СВЧ-излучением, но вот к чему приводит этот перегрев - тут мнения расходятся. Можно найти множество статей о том, что в этом ничего страшного нет и такое же количество статей с опровержением данного утверждения. Поэтому не рекомендуется прижимать телефон к уху и тогда однозначно вреда не будет: максимальная мощность передатчика GSM-телефона - всего 2 Вт.

Обобщая изложенное можно констатировать, что процедура обновления местоположения (LU) позволяет мобильному устройству уведомить сотовую сеть, что оно переходит из одной зоны местоположения в другую. Мобильные телефоны сами отвечают за определение кода зоны местоположения. Когда мобильное устройство считает, что код зоны местоположения изменился, оно отправляет в сеть запрос обновления зоны местоположения, содержащий информацию о предыдущем местоположении, и Временный Идентификатор Мобильной Станции (TMSI).

Есть несколько случаев, когда мобильное устройство передает в сеть запрос об обновлении зоны местоположения. Каждый раз, когда мобильный аппарат включается или отключается, в сеть передается его местоположения для регистрации или разрегистрации IMSI (международный индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи стандарта GSM.

Кроме того, каждое мобильное устройство регулярно уведомляет сеть о своем местонахождении через определенные интервалы времени. Как только мобильный аппарат перемещается из одной зоны в другую, также

производится обновление информации о местоположении. Мобильное устройство принимает решение о смене зоны местоположения, основываясь на уровне сигнала от базовых станций, выбирая наилучший. Таким образом, мобильный аппарат сохраняет гарантированный доступ к сети и может принимать вызовы, свободно перемещаясь в пределах всей зоны покрытия.

Location Area (LA) - область местоположения определяется как группа объединенных сот по географическому признаку (рис. 2.2). LA может управляться одним или несколькими BSC. Главная цель введения LA в структуру сети является то, что при входящем звонке абоненту сотовой связи его поиск и вызов должен осуществляться именно в одной конкретной LA, а не в соте. Эта процедура называется пейджинг (paging). Таким образом, когда оборудование абонента включено и зарегистрировано в сети, но нет активного соединения, то сеть знает, где находится абонент с точностью до конкретной LA. В том случае, когда абонент перемещается через границу текущей LA и попадает в другую, то он должен оповестить сеть о смене своего местоположения. Эта процедура, как известно, называется Location update. Исходя из этого, можно сделать вывод, что слишком большое число сот в LA приведет к высокой сигнальной нагрузке внутри LA из-за частого пейджинга, а слишком малое число к частым Location update.

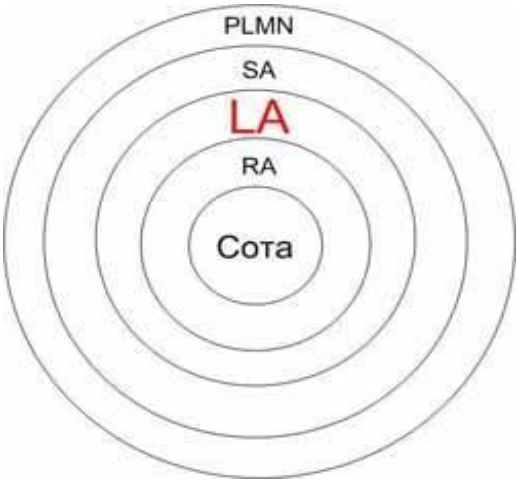


Рис. 2.2. LA по отношению к другим областям местоположения в сети сотовой связи

У каждой LA есть уникальный код, по которому данная область местоположения может быть уникально идентифицирована во всем мире. Это код называется LAC (Location area code).

Роуминг в сетях GSM. Подавляющему большинству мобильных абонентов связь нужна только в их родном городе, но есть и те, кому необходимо быть на связи, уезжая в другой город, а то и в другую страну. Для таких людей и существует роуминг - возможность со своим средством мобильной связи подключиться к сети, родственной по стандарту домашней сети [5,10].

В общем случае понятие "роуминг" ("странствование") неразрывно связано с GSM. В D-AMPS и NMT, в двух наиболее распространенных стандартах персональной сотовой связи на момент начала распространения GSM, роуминг также имелся и имеется, причем не менее автоматический. Однако эти два стандарта имели (и имеют) узко региональную специализацию. NMT - это Скандинавия, Восточная Европа и государства бывшего СССР, особенно - Россия. D-AMPS наиболее распространен в Америке, и, опять-таки, в России и государствах СНГ, т.е. европейцу нечего было и мечтать, чтобы приехать, скажем, в США со своим телефоном.

Вместе с тем GSM, не успев появиться, начал стремительно распространяться по планете. К настоящему моменту сетями этого стандарта опутаны все континенты (за исключением Антарктиды), правда, в разной степени. Наибольшая плотность покрытия, как и следовало ожидать, на родине GSM - в Европе и странах СНГ. Пока слабо развиты сети в Америке, особенно - Южной, и полностью отсутствуют в Японии и Корее - там ставка сделана совсем на другие стандарты. Есть GSM даже на самом большом острове в мире Гренландии. Таким образом, подведя итог можно считать, что GSM оправдал свое название - "Global System for Mobile communications".

Для организации роуминга системы сотовой мобильной связи должны быть одного стандарта, а центры коммутации MSC мобильной связи должны

быть соединены специальными каналами связи для обмена данными о местонахождении абонента (роумера).

Для обеспечения роуминга необходимо выполнение трех условий:

- наличие в требуемых регионах систем сотовой мобильной связи CMCS (Cellular Mobile Communication System), совместимой со стандартом компании-оператора, у которой была приобретена MS;
- наличие соответствующих организационных и экономических соглашений о роуминговом обслуживании абонентов;
- наличие каналов связи между системами $CMCS_д$ и $CMCS_г$;
- обеспечивающими передачу звуковой и других видов информации для роуминговых абонентов.

Различают три вида роуминга:

- ручной, то есть обмен одной $MS_д$ на другую $MS_г$; (или смену SIM-карты);
- полуавтоматический, когда абонент $MS_д$ ставит в известность своего оператора $CMCS_д$,;
- автоматический.

Упрощенную схему организации автоматического роуминга можно представить следующим образом:

- абонент $MS_д$ сотовой системы связи CMCSд, оказавшись на территории «чужой» системы $CMCS_г$, допускающей реализацию роуминга, инициирует вызов обычным образом, как если бы он находился на территории «своей» системы CMCS;

- центр коммутации MSC; убедившись, что в его домашнем регистре HLR этот абонент не значится, воспринимает его как роумера $MS_д$ (roamer — абонент, использующий услуги роуминга) и заносит его в гостевой регистр VLR. Одновременно (или с некоторой задержкой) MSC запрашивает в домашнем регистре «родной» системы роумера, то есть в $HLR_д$, относящиеся к нему сведения, необходимые для организации обслуживания (оговоренные подпиской виды услуг, пароли, шифры), и

сообщает, в какой системе роумер $MS_д$ находится в настоящее время. Последняя информация фиксируется в домашнем регистре $HLR_д$ «родной» системы роумера. После этого роумер MS, пользуется сотовой связью как «домашней» системой;

- исходящие от него вызовы обслуживаются обычным образом, с той только разницей, что относящиеся к нему сведения фиксируются не в домашнем регистре $HLR_д$ (HLR;), а в гостевом VLR;
- поступающие на его номер вызовы переадресуются «домашней» системой $CMCS_д$ в систему $CMCS_г$, где роумер $MS_д$ гостит.

По возвращении роумера $MS_д$ домой в домашнем регистре $HLR_д$ стирается адрес той системы $CMCS_г$, где роумер находился, а в гостевом регистре VLR той системы CMCS стираются сведения о $MS_д$.

Оплата услуг роуминга абонентом $MS_д$ производится через домашнюю систему $CMCS_д$, а оператор $CMCS_д$ возмещает расходы компании-оператору $CMCS_г$, оказавшему услуги роуминга, в соответствии с роуминговым соглашением.

В стандарте GSM процедура роуминга заложена как обязательный элемент. Кроме того, в стандарте GSM имеется возможность роуминга с SIM-картами с перестановкой SIM-карт между мобильными станциями различных вариантов стандарта GSM (GSM 900/1800/1900), поскольку во всех трех вариантах стандарта GSM используются унифицированные SIM-карты.

Процедура роуминга в стандарте GSM наиболее удобна для двух- и трехрежимных абонентских терминалов.

Роуминг в стандарте GSM. Для реализации роуминга мобильному абоненту сети GSM присваиваются следующие основные номера и идентификаторы [5,8,10]:

1. Международный идентификатор мобильного абонента — IMSI (International Mobile Subscriber Identity), который записывается в постоянное запоминающее устройство SIM-карты. IMSI включает: код

страны мобильной связи MCC (Mobile Country Code) — 3 знака, код сети оператора MNC (Mobile Network Code) —2 знака, номер абонента в сети оператора MSIN (Mobile Subscriber Identity Network) — 10 знаков.

2. Номер сети общего пользования — соответствует телефонной нумерации каждой сети оператора мобильной связи.
3. Временный роуминговый номер —MSRN (Mobile Station Roaming Number).

Он выделяется при установлении входящего соединения к абоненту-роумеру на время установления соединения, но не более 30 с. Блок номеров MSRN выделяется из общей телефонной нумерации сети.

Информация о местоположении абонента $MS_д$ должна обновляться в регистре HLR, каждые несколько минут. Для этой цели информация периодически передается в базу данных HLR из базы данных VLR, MSC, узла коммутации, в котором временно находится $MS_д$. Когда к вызываемому абоненту $MS_д$ поступает входящий вызов, регистр HLR, определяет, каким образом можно соединиться с абонентом $MS_д$ в зависимости от его текущего местоположения. По мере перемещения MS, из одной соты в другую содержимое HLR, постоянно обновляется. Такой механизм обеспечивает мобильному абоненту $MS_д$ абсолютно свободное передвижение в пределах всей сотовой сети $CMCS_г$ без риска потерять входящие вызовы.

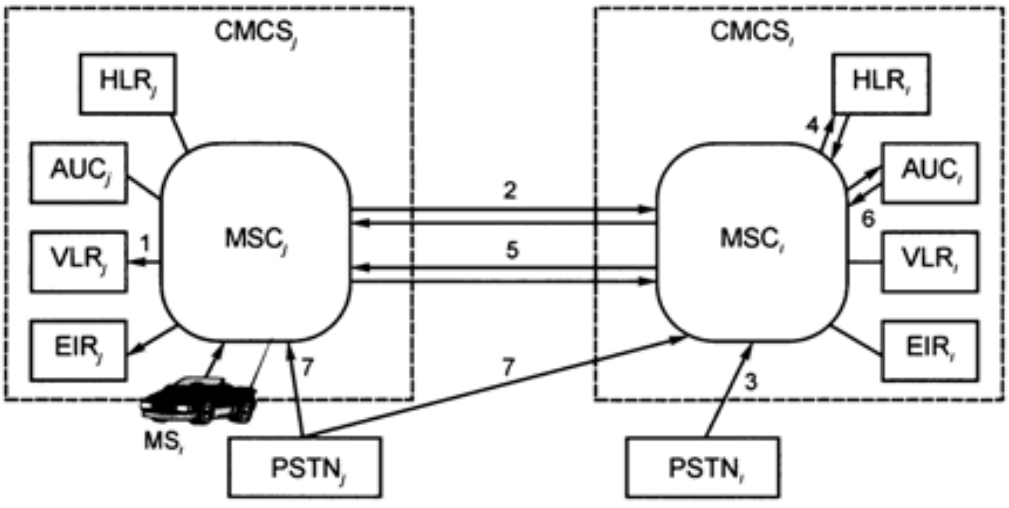


Рис. 2.3. Основные процедуры взаимодействия сетей GSM при роуминге

В соответствии с рисунком 2.3, процедуры взаимодействия сетей GSM при роуминге происходят следующим образом:

1. Пусть роумер-абонент $MS_д$ попал в визитную сеть CMCS. При этом $MS_д$ фиксируется ближайшей $BTS_г$, идентификатор IMSI по радиоинтерфейсу через $BTS_г$ передается в MSC, и далее в регистр VLR.
2. Далее осуществляется процедура обновления данных местоположения MS*полученный $IMSI_д$ роумера-абонента $MS_д$ из VLR, через MSC, и по каналу связи (луч 2 — от MSC; -> MSQ) поступает в MSQ и далее в $HLR_д$ (по лучу 4).
3. $HLR_д$ проверяет право абонента $MS_д$ на роуминг и передает подтверждение на обновление данных ($HLR_д$ -> луч 4 -> $MSC_д$ -> луч 2 -> MSC, -> луч 1 — VLR;).
4. Далее следует процедура запроса/передачи абонентских данных MS/(данных об услугах, параметры аутентификации $MS_д$)MSC; луч 2 —>$MSC_д$ —> луч 4—> $HLR_д$ или MSC; луч 2 ** MS $C_д$ луч 6 -* AUQ.
5. Дополнительно осуществляются процедуры запроса/передачи временного роумингового номера MSRN: MSC, —> луч 5 —> MSQ —> луч 4 —> HLR, или MSC, —> луч 5 —> MSQ —> луч 6 —> AUQ для установления соединения.
6. При входящем вызове от PSTN прохождение сигнала вызова: PSTN, ^ луч 3 ^ MSQ -> луч 2 -> MSC, -> BTS, -> $MS_д$, а далее реализуется формирование канала связи стационарного телефонного аппарата в PSTN, и MS, либо через международную сеть (луч 7), либо через национальную или международную роуминговую сеть по номеру MSRN.

Тарификация вызовов при роуминге. Организация роуминга связана не только с техническими возможностями. Прежде всего должна быть договоренность между компаниями-операторами по оплате звонков [10].

При роуминге ваш сотовый номер сохраняется, то есть тот, кто хочет позвонить вам, просто набирает номер как обычно. Для звонящего роумера

тарификация не меняется, т.е. если абонентский номер - Ташкентский, то звонок так и останется "звонком в Ташкент". А вот для абонента сотовой сети все будет по-другому. Так как имеет место перевод звонка в другую страну (другой город), то возникает международное (междугороднее) соединение, которое и оплачивается абонентом (естественно, что внутрисетевые скидки, бесплатные входящие с сотовых телефонов здесь уже не действуют). Кроме того, оператор "гостевой" сети тоже выставляет счет за свои услуги. Таким образом, стоимость роумингового звонка (неважно, входящего или исходящего) вычисляется по сложной формуле, которая в самом общем случае выглядит так:

Цена = услуги "гостевой" сети + налоги страны "гостевой" сети + операторский сбор "домашней" сети + перемаршрутизация + [налоги России]

Первые два слагаемых - это те суммы, которые выплачиваются оператору "гостевой" сети. Операторский сбор "домашней" сети - это комиссия вашего оператора за проведение расчетов, как правило, она составляет 10-15% от запрашиваемых сумм. Перемаршрутизация имеет смысл только при входящих звонках, это взимаемая "домашним" оператором плата за перенаправление звонка в "гостевую" сеть, равная стоимости международного звонка в эту страну/город.

При *входящих* вызовах, как правило, удерживается только стоимость перемаршрутизации, причем, как вытекает из смысла этой операции, учет ведет именно "домашний" оператор. Стоимость разговора в этом случае сразу же попадает в ваш счет, или списывается с баланса (в зависимости от способа оплаты).

Подавляющее большинство операторов GSM в мире не берут никакой дополнительной платы за входящие роумерские звонки. Однако некоторые из них за каждый входящий звонок берут дополнительную оплату. В этом случае эта сумма войдет в стоимость звонка как "услуга "гостевой" сети", вместе с удержанными с нее местными налогами и операторским сбором.

Следует отметить, что размер оплаты варьируется, и иногда даже может превышать непосредственно междугороднюю составляющую - плату за перемаршрутизацию.

Исходящие вызовы, напротив, учитываются только оператором "гостевой" сети, и ваш оператор узнает о них постфактум. В настоящий момент системы обмена информацией о совершенных звонках в реальном времени не развиты, поэтому счета за роуминговые сессии поступают с некоторой периодичностью, например, раз в неделю. И возможны ситуации, когда вы уже вернулись домой, взяли детализацию (или счет), а совершенные звонки в ней пока не отражены.

Именно из-за задержки в выставлении счетов операторы принимают меры предосторожности, чтобы не допустить неприятных ситуаций. Одни применяют кредитную систему оплаты, для пользования международным роумингом (и международным доступом), т.е. нужно внести дополнительный залог. Другие, где услуги оказываются по предоплате, нужно лично явиться в офис компании с паспортом, и заполнить бланк соответствующего заявления.

В случае исходящих звонков стоимость состоит из оплаты оператору "гостевой" сети, налогов его страны и операторского сбора компании-оператора "домашней" сети. Некоторые зарубежные операторы предлагают, для экономии средств, совершать звонки через Интернет, при этом сама процедура крайне проста: вместо [+] - выход на межгород - нужно набрать короткий префикс, и затем номер как обычно. Однако общего подхода здесь пока нет, поэтому в каждом случае порядок набора, и возможность предоставления данной услуги придется выяснить индивидуально.

Короткие сообщения (SMS). Практически все существующие сети GSM поддерживают прием и передачу коротких текстовых сообщений (SMS). При этом, находясь в роуминге, никаких изменений в настройках телефона производить не нужно. Входящие сообщения бесплатны, а исходящие оплачиваются по тарифам "гостевой" сети, причем расчет идентичен исходящим звонкам. В крайне редких случаях бесплатны и исходящие СМС.

Стоимость каждого отправленного сообщения не изменится, если вы попробуете использовать другой SMS-центр, так как тарифицируется именно факт отправки.

Для того чтобы отправить SMS в другие сети, достаточно наличие роумингового соглашения вашего оператора с оператором этой сети. Причем такое соглашение не обязательно должно быть полноценным роумингом. Например, абоненты разных мобильных сетей в Германии, Великобритании, имеют возможность обмениваться SMS. Однако в отдельных странах никак об этом не договорятся, и абонентам приходиться искать обходные пути.

Перспективы развития. Роуминг, без сомнения, дает огромные перспективы для общения, где бы вы ни были. Лавинообразное развитие сетей GSM оставляет все меньше населенных мест, где нет какой-нибудь сети.

С другой стороны, есть места, где развиты сети других стандартов, а GSM нет вообще. Самый яркий пример - это Япония, Южная Америка. Для того чтобы охватить роумингом и эти страны, World GSM Association организовала GSM Global Roaming Forum, целью которого является разработка стандартов для осуществления роуминга между сетями стандарта GSM и другими сетевыми технологиями: CDMA, TDMA и iDEN. Уже есть результаты этой деятельности, недавно БиЛайн заключил роуминговое соглашение с оператором стандарта iDEN Nextel. Абоненты компании получили возможность пользоваться своим номером в Аргентине и Перу, где сетей GSM пока нет.

Другим важным вопросом является роуминг для абонентов препейд-систем (предоплата), таких как Би+ или ТАКСАфон. На самом деле, уже давно в этой сфере применяется технология "одностороннего" роуминга - возможно только принимать звонки и получать СМС (такие звонки учитываются оператором "домашней" сети). А чтобы произвести исходящий звонок, применяется не очень удобная процедура "обратного звонка": номер набирается со специальным префиксом, после подтверждающего сигнала

соединение разрывается, и ожидается входящий звонок (немного напоминает использование службы автодозвона в БиЛайн или МТС). Однако уже разработана и кое-где используется система обмена информацией между операторами в реальном времени - CAMEL (Customized Applications for Mobile Networks Enhanced Logic). Такая служба, внедренная операторами Paegas в Чехии и D1 в Германии, позволяет абонентам препейд-систем пользоваться всеми преимуществами роуминга и дополнительно совершать бесплатные звонки для пополнения баланса и контроля использования средств.

В заключении отметим, что сейчас полным ходом разворачиваются сети третьего и четвертого поколений мобильной связи, разрабатываются сети пятого поколения с представлением разнообразных услуг. Поэтому можно с уверенностью утверждать, что технология автоматического роуминга, так блестяще проявившая себя в сетях GSM, будет существовать и дальше, пока не появится какая-нибудь новая, доступная глобальная мобильная сеть.

2.2. Идентификаторы сети GSM

Идентификаторы сети – ряд номеров, которые сеть GSM использует для определения местоположения абонента при установлении соединения. Данные идентификаторы используются для маршрутизации вызовов к MS. Важно, чтобы каждый идентификационный номер был уникальным и был всегда корректно определён.

Идентификаторы абонентов

Номер мобильной станции (MSISDN) уникально определяет абонирование мобильного абонента в номерном плане сети PSTN. Данный номер набирается при установлении входящего соединения к абоненту сети мобильной связи и не содержится на SIM-карте, а сопоставлен с IM SISIM-карты в HLR, и предназначается для передачи номера телефона назначенному абоненту и для получения звонков на телефон [5,6]. Основной

MS ISDN номер используется для идентификации абонента при предоставлении большинства услуг и может быть изменен без замены SIM-карты. Возможно также сопоставить SIM-карте несколько дополнительных MS ISDN для работы с факсимильной связью и передачи данных. MS ISDN входит в состав долговременных данных, хранящихся в HLR и VLR [10]. Структура MSISDN приведена на рисунке 2.4.

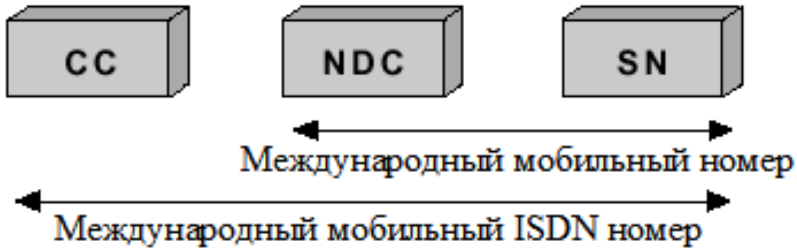


Рис.2.4. Идентификатор MSISDN

Где: CC (Country Code) – код страны;
NDC (National Destination Code) – национальный код пункта назначения;
SN (Subscriber Number) – номер абонента.

MS ISDN, как и IMSI, может достигать 15 цифр и, в соответствии с E.164, состоит из трех частей. При этом конкретные длины составляющих частей регулируются международным и локальным законодательствами, например:

- Россия: CC=1 цифра (7) (следует учитывать, что из данного диапазона выделен Казахстан, у которого CC=2 цифры (77)), NDC=3 цифры (например, 903), SN=7 цифр (1234567), итого — 11 цифр (итоговый пример: 7-903-1234567).
- Украина: CC=3 цифры (380), NDC=2 цифры (например, 50), SN=7 цифр (1234567), итого — 12 цифр (итоговый пример: 380-50-1234567).
- Белоруссия: CC=3 цифры (375), NDC=2 цифры (например, 29), SN=7 цифр (1234567), итого — 12 цифр (итоговый пример: 375-29-1234567).
- Узбекистан: CC=3 цифры (998), NDC=2 цифры (например, 90), SN=7 цифр (1234567), итого — 12 цифр (итоговый пример: 998-90-1234567).

Для каждой сети PLMN существует свой NDC. Например, в Ирландии NDC может быть 086 и 087, что указывает на наличие двух операторов PLMN. В России для каждой PLMN определены несколько NDC. Интернациональный номер MSISDN может быть переменной длины. В Узбекистане один NDC – 998.

Интернациональный идентификатор мобильного абонента (IMSI)– это индивидуальный номер каждого абонента, по которому система распознает пользователя мобильной связи, использующего стандарты GSM или UMTS. По данному номеру происходит идентификация абонента через радиоэфир и через всю сеть, а также используется для сигнализации PLMN. IMSI хранится в SIM, в HLR и в обслуживающем VLR.

В момент регистрации в сети аппаратом абонента передается идентификатор IMSI, с помощью которого и происходит идентификация. Для того, чтобы исключить возможность несанкционированного перехвата, отправка этого номера через сеть осуществляется так редко, как только это возможно. Во всех случаях, когда есть такая возможность, вместо него отправляется TMSI, код, который был случайно сгенерирован по определенному алгоритму. TMSI – это идентификатор конкретной мобильной станции, используемый как временный в процессе регистрации в сети, при установке звонка и тому подобное. Его назначение возможно только после успешного завершения аутентификации с помощью IMSI.

Идентификатор в системе GSM содержится в элементарном файле6F07 на SIM-карте. Формат, в котором на SIM-карте хранится IMSI, описан ETSI-стандартом, предусмотренным спецификацией GSM 11.11. Помимо этого, IMSI использует любая мобильная сеть, которая соединена с другими сетями, например, с CDMA или EVDO, идентично сетям GSM. Такой номер связан напрямую с телефоном, но может иметь связь с картой R-UIM, которая выполняет функции SIM-карты для систем CDMA.

Обычно IMSI имеет длину в 15 цифр, но иногда может быть несколько короче. Например, стандартный IMSI из 15 цифр: 250-07-XXXXXXXXX.

По первым трем цифрам (250) определяется страна (Россия). Дальше (07) закодирована мобильная сеть (СМАРТС). Для кода мобильной сети используются две или три цифры – для европейского стандарта две, а для североамериканского – три. Все оставшиеся цифры – это номер идентификации пользователя. E.212ITU – стандарт нумерации, которому соответствует IMSI.

Временный идентификатор мобильного абонента *(TMSI)*-временный номер IMSI, который дается MS при её регистрации. Он используется для того, чтобы защитить абонента от прослушивания и несанкционированного доступа в радиочастотном тракте.

TMSI используется только для локального абонирования (только в одной зоне MSC/VLR) и изменяется при изменении местоположения (Location Update). Структура TMSI может быть определена каждым оператором, но не может превышать 8 цифр. Поскольку TMSI имеет в два раза меньший размер, чем IMSI, пейджинг в одном кадре осуществляется для двух абонентов, что также сокращает нагрузку на процессор.

Идентификационный номер оборудования MS *(IMEI)* используется для уникальной идентификации мобильного оборудования в сети. Данный код используется в процедурах обеспечения безопасности связи для идентификации украденного оборудования и предотвращения неавторизованного доступа в сеть. Согласно спецификациям, GSM длина IMEI составляет 15 цифр (рис.2.5):

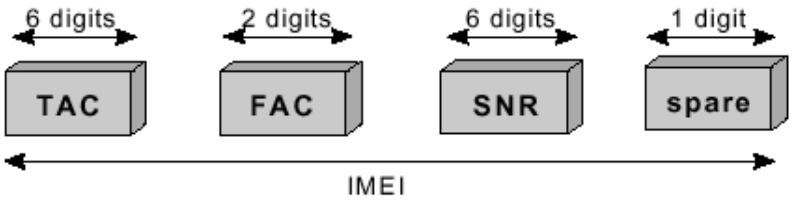


Рис. 2.5. Идентификатор IMEI

- TAC (Type Approval Code) - код утвержденного типового образца.

- FAC (Final Assembly Code) - код окончательно собранного изделия, присваивает производитель.
- SNR (Serial Number) - индивидуальный серийный номер. Идентифицирует полностью все оборудование с учетом кодов TAC и FAC.
- Spare - свободные цифры. Зарезервированы для будущего использования. Когда данный код передается в MS, значение данного кода должно быть всегда «0».

Интернациональный идентификатор оборудования MS и номер программного обеспечения (IMEISV) обеспечивает уникальную идентификацию каждой MS, а также обеспечивает соответствие версии программного обеспечения, инсталлированного в MS, разрешенному оператором. Версия программного обеспечения является важным параметром, так как от этого зависят услуги, доступные для MS, а также способность выполнять речевое кодирование. Так, например, PLMN необходимо знать для возможностей речевого кодирования MS при установлении соединения (например, halfrate/fullrate, и т д.). Данные возможности отображаются с помощью IMEISV.Идентификатор IMEISV состоит из (рис.2.6):

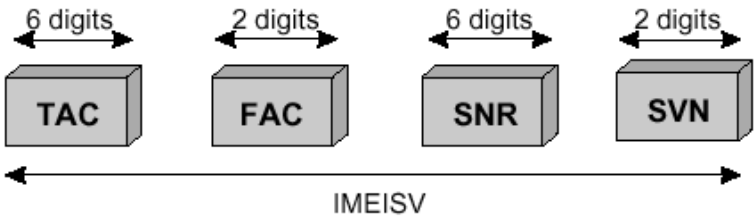


Рис.2.6. Идентификатор IMEISV

- SVN (Software Version Number) - номер программной версии, позволяет производителю MS идентифицировать различные версии программного обеспечения утверждённого типового образца MS. SVN со значением 99, зарезервирован для будущих целей.

Идентификаторы местоположения. *Номер MS в роуминге (MSRN)*- временный сетевой номер, назначаемый в течение установления соединения для MS, находящейся в роуминге. MSRN состоит из трёх частей (рис.2.7):

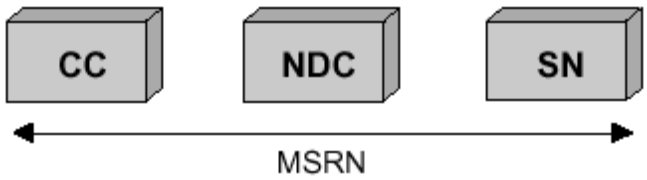


Рис. 2.7. Идентификатор MSRN

- В этом случае SN означает адрес обслуживающего MSC/VLR.

Идентификатор местоположения (LAI) – временный сетевой идентификатор, который тоже требуется для маршрутизации вызовов. Данный код введён для двух целей:

1. Пейджинг. В этом случае LAI используется для информирования MSC о LA, в которой находится MS.
2. Обновление местоположения абонента.

LAI состоит из следующих блоков (рис.2.8):

идентификатор абонент мобильный локальный

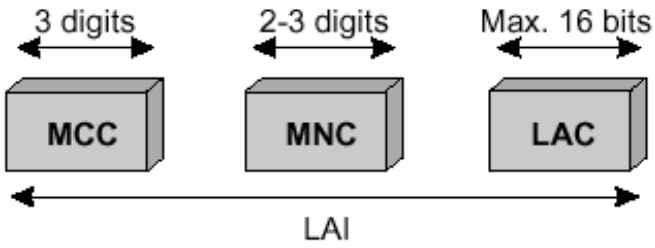


Рис. 2.8. Идентификатор LAI

- Location Area Code (LAC) - код местоположения, максимальная длина LAC составляет 16 бит, что позволяет определить 65536 различных LA внутри одной PLMN.

Cell Global Identity (CGI) используется для идентификации индивидуальной соты внутри LA. Идентификация соты осуществляется

посредством добавления параметра Cell Identity (CI) к компонентам LAI. CI имеет размер 16 бит. CGI состоит из (рис.2.9):

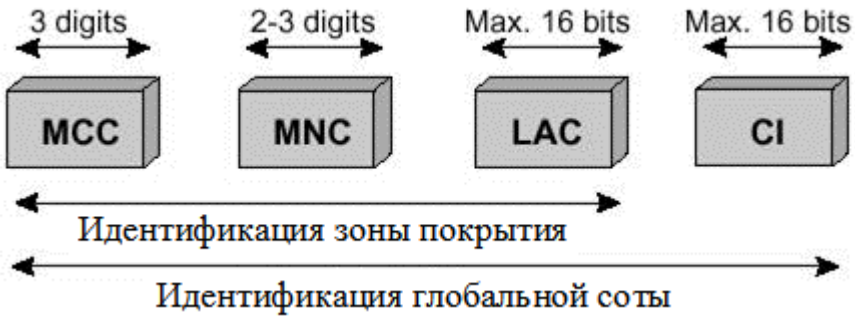


Рис. 2.9. Идентификатор CGI

Глобальный идентификатор соты CGI (Cell Global Identity) используется для идентификации индивидуальной соты внутри LA. Идентификация соты осуществляется посредством добавления параметра Cell Identity (CI) к компонентам LAI. CI имеет размер 16 бит. CGI состоит из (рис.2.10):

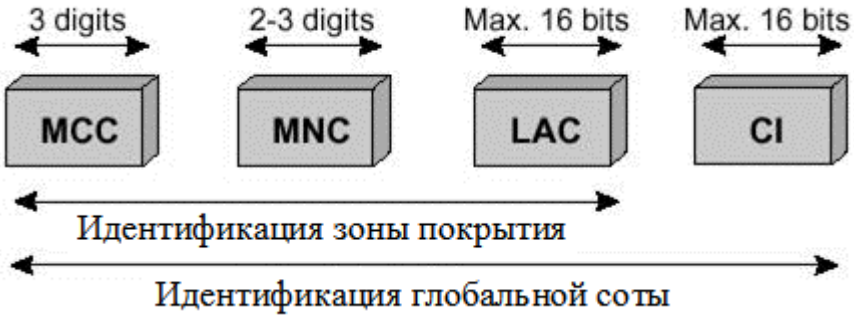


Рис.2.10. Идентификатор CGI

- *Идентификационный код БС (BSIC)*дает возможность MS различать соты.
- BSIC состоит из (рис.2.11):

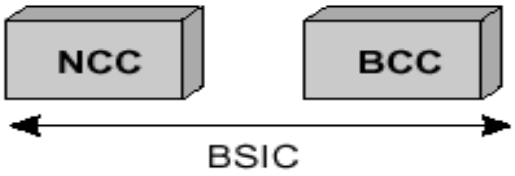


Рис. 2.11. Идентификатор BSIC

- NCC – National Color Code (национальный цветовой код). Используется для того, чтобы разграничивать зоны действия операторов в тех местах, где сети операторов перекрывают друг друга.
- BCC – Base station Color Code (цветовой код базовой станции). Используется для того, чтобы различать между собой базовые станции, использующие одинаковые частоты.

Номер местоположения LN, номер определённой географической зоны LA, зона обслуживания MSC/VLR. Данный номер используется для регионального/локального абонирования услуг сети мобильной связи и для тарификации на основе географического местоположения абонента.

LN состоит из идентификатор ДТ (рис.2.12):

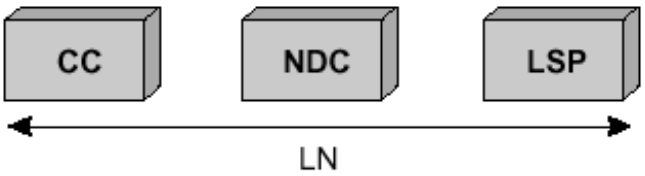


Рис. 2.12. Идентификатор ДТ

- LSP Locally Significant Part. Локально важная часть

Идентификатор локальной зоны абонирования (RSZI). Для каждого регионального абонирования необходимо определить зоны/области. Последнее достигается путем использования идентификатора Regional Subscription Zone Identity (RSZI).

Идентификатор RSZI представлена на рисунке 2.13.

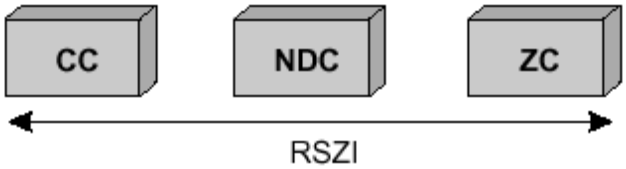


Рис. 2.13. Идентификатор RSZI

- ZC - Зональный код. Длина кода - 2 октета.

Конфиденциальная процедура идентификации абонента. Каждый раз, когда MS делает запрос на системные процедуры (LU, попытка вызова или активация сервиса) MSC/VLR ставит новый TMSI. В соответствие с IMSIMSC/VLR передаёт TMSI в MS, которая хранит его в SIM-карте. Сигнализация между MSC/VLR и MS использует только на основе TMSI. Таким образом, реальный номер абонента IMSI не передается через радиоэфир. TMSI в два раза короче IMSI, следовательно, в одном сообщении можно передать пейджинг для двух абонентов. IMSI используется тогда, когда процедура Location Updating выполнена неудачно или не назначен TMSI.

2.3. Варианты сценариев обслуживания вызовов

MS в состоянии IDLE. Последовательность обслуживание осуществляется в следующем порядке (рис.2.14) [10-11]:

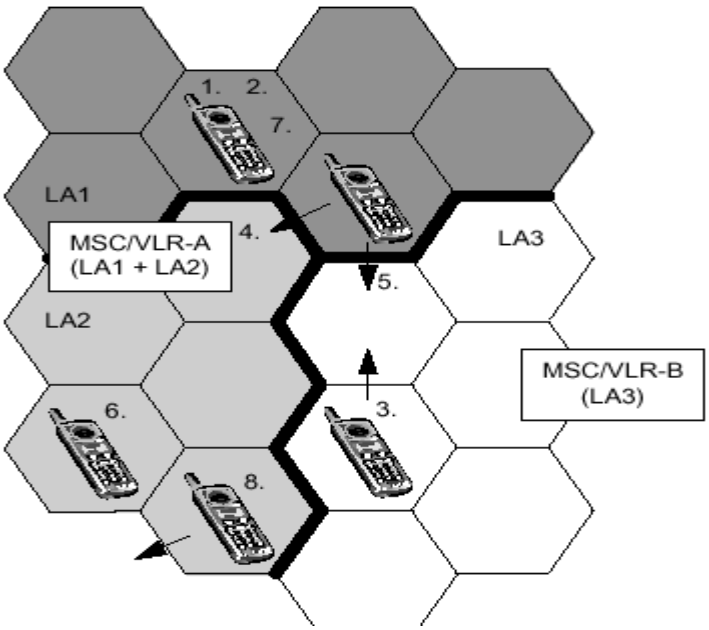


Рис. 2.14. MS в режиме IDLE

1. Регистрация в сети, регистрация IMSI (IMSI attach)
2. Обновление местоположения (Location updating)
3. Смена соты внутри LA
4. Обновление местоположения внутри одного MSC/VLR
5. Обновление местоположения при входе в зону действия нового MSC/VLR
6. Обновление местоположения, тип - периодическая регистрация.
7. Отключение от сети (IMSI detach)
8. Полное отключение от сети (отсутствует информации о местонахождении MS) (Implicit detach).

Включение MS в сеть. *IMSI Attached.*Когда абонент включает MS (включает питание на MS), выполняется процедура IMSI attach, которая содержит в себе следующие шаги (рис. 2.15):

1. MS передаёт в сеть сообщение «IMSI attach» указывая на то, что она изменила своё состояние из неактивного в IDLE.
2. VLR определяет, существует ли запись об этом MS. Если нет, то VLRсвязывается с HLR, к которому приписана данная MS, и копирует в себя данные абонирования этого абонента.

3. После этого VLR осуществляет обновление состояния MS и переводит это состояние в IDLE.
4. На MS передается уведомление.

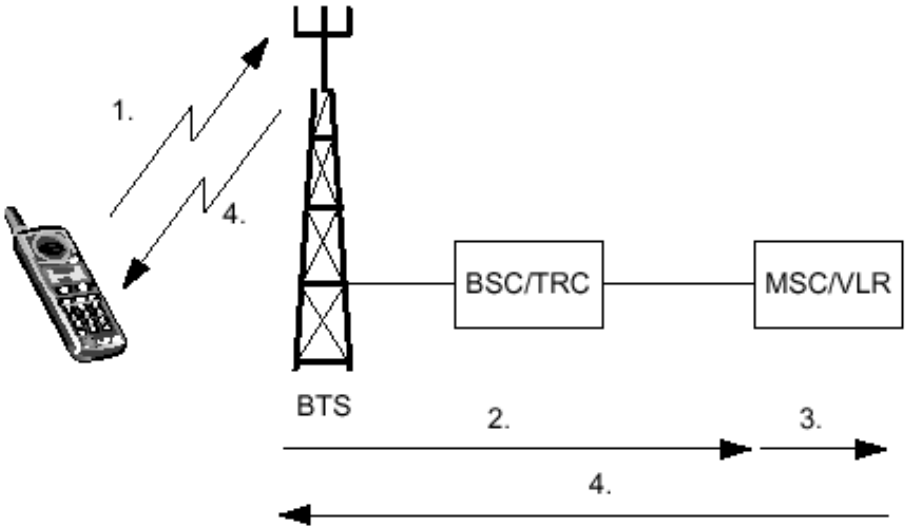


Рис. 2.15. Процедура IMSI attach

Обновление местоположение (LU), тип – IMSI attach. Если MS изменила LA будучи в состоянии OFF, то процедура IMSI attach может привести к обновлению местоположения MS. VLR в течение выполнения процедуры IMSI attach может определить, что текущий идентификатор LAI мобильной станции отличается от LAI, хранящегося в SIM-карте MS. Если это так, то VLR обновляет информацию о LAI мобильной станции.

Сетевой роуминг. *Смена соты внутри LA.* MS постоянно находится в процессе перемещения по всей сети. Информация о местоположении MS отображается с помощью параметра зоны местоположения Location Area (LA) и хранится в VLR. Если MS меняет соты внутри одной LA, процедура обновления местоположения в сети не выполняется. Информацию о том, что новая сота принадлежит той же LA, мобильная станция получает из канала BCCH соседних сот. По каналу BCCH передается LAI сот. MS сравнивает принятое значение LAI с новым LAI. Если LAI совпадают, то это означает, что обновление местоположения выполняться не будет и нет необходимости оповещать об этом сеть.

Обновление местоположения внутри одного MSC/VLR. Если MS обнаруживает изменения в LAI на основе анализа информации, передаваемой по каналу BCCH, она информирует об этом сеть. Когда MS передает сообщение об обновлении местоположения, MSC/VLR определяет, зарегистрирован ли данный абонент в этом VLR, или он переместился в зону обслуживания данного MSC/VLR из зоны обслуживания другого MSC/VLR (рис.2.16).

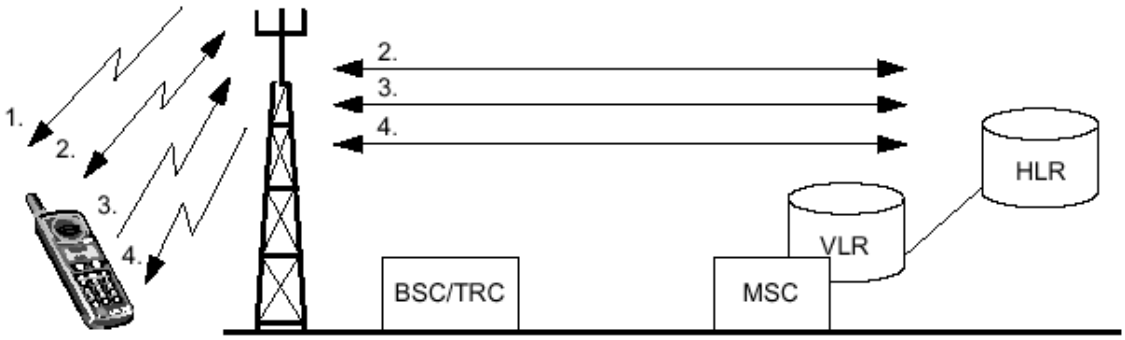


Рис. 2.16. Обновление местоположения внутри одного MSC/VLR

1. MS прослушивает BCCH в новой соте, чтобы определить LAI. Новый LAIсравнивается со старым. Если существует различие, то необходимо провести обновление местоположения.
2. MS устанавливает соединение с сетью через SDCCH. Выполняется аутентификация.
3. Если аутентификация прошла успешна, MS делает запрос в систему об обновлении местоположения.
4. Система подтверждает LU и дает команду базовой и мобильной станциям на освобождение канала.

Обновление местоположения при входе в зону обслуживания нового MSC/VLR. Обновление местоположения (LU) осуществляется тогда, когда MS перемещается в новую LA. Однако мобильной станции неизвестно, принадлежит ли LA новому MSC/VLR. Когда новый VLR принимает запрос об LU, то выполняется следующее (рис.2.17):

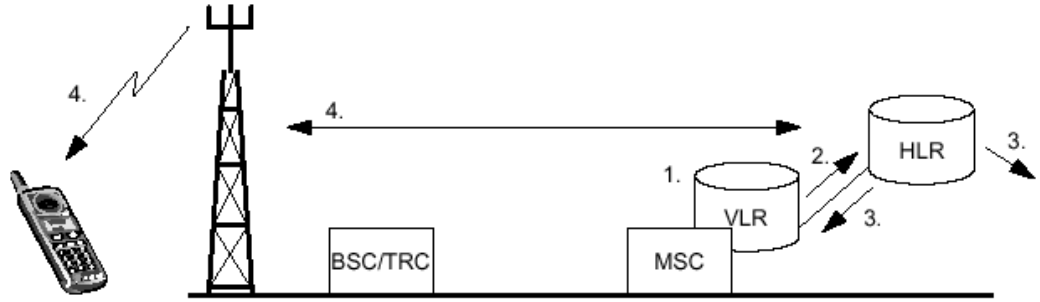


Рис. 2.17. Обновление местоположения, при входе в зону действия обслуживания MSC/VLR

1. Выполняется аутентификация. Если аутентификация прошла успешно, VLR проверяет свою БД, чтобы определить, есть ли там информация о данном абоненте.
2. Когда VLR не находит информации о MS, он передаёт запрос в HLR абонента для осуществления копирования данных об этом абоненте в свой VLR.
3. HLR передаёт информацию в VLR и обновляет у себя информацию о местоположении MS.
4. VLR записывает информацию об MS, включающую в себя данные о последнем местоположении и состоянии IDLE. VLR передает оповещение в MS.

Обновление местоположения, тип - периодическая регистрация. Периодическая регистрация – это услуга, которая позволяет MS посылать регистрационные сообщения через определённые интервалы времени. В случае, если MS не регистрируется через определённый интервал времени, то система помечает MS как выключенную (detached). Последнее случается тогда, когда MS оказывается вне зоны обслуживания сети или в этом случае, когда системе нет необходимости осуществлять пейджинг на мобильную станцию. В случае, если сеть использует процедуру периодической регистрации, информация о периоде регистрации мобильной станции передается по каналу BCCH. Периодическая регистрация использует

системное сообщение *acknowledgment message*. MS пытается зарегистрироваться в сети до тех пор, пока она не получит данное сообщение.

Отключение от сети. *Отключение IMSI (IMSI Detach).* Отключение IMSI указывает сети, что MS перешла в неактивное состояние. MS при отключении от сети направляет в сеть сообщение о своем отключении. VLR, получив такое сообщение, отмечает соответствующий IMSI как отключенный. HLR при этом не уведомляется. На MS не отправляется никакого подтверждающего сообщения.

Полное отключение от сети (Implicit Detach). Если MS направляет в сеть сообщение об отключении в условиях плохого качества обслуживания, система может не расшифровать информацию о выключении MS. Так как на MS не отправляется никакого подтверждающего сообщения, дальнейшие попытки сообщить об отключении не делаются. С помощью метода периодической регистрации сеть по истечении периода регистрации определит, что MS отключена. После этого VLR выполнит скрытое отключение, отмечая MS как отключенную. (Implicit Detach).

В случае, если MS выходит из зоны обслуживания сети и не выходит на связь в течение периода регистрации, то система также отмечает состояние MS как Implicit Detach.

Удаление из VLR информации о MS (MS Purging). Эта процедура используется для того, чтобы информировать HLR о предстоящем удалении информации о конкретном MS из VLR. После удаления из VLR этой информации HLR устанавливает флажок, указывающий на то, что данные о MS удалены и воспринимает эту MS как недоступную. Это исключает лишние процессы в сети, а также сокращает затраты ресурсов на проверку базы данных абонента.

Рассмотрим пример, когда MS из Узбекистана перемещается в Германию и производит обновление данных о местоположении в MSC/VLR сети GSM в Германии. Далее абонент переезжает обратно в Узбекистан.

Переезд из Германии в Узбекистан занимает некоторое время. На протяжении этого времени MS абонента находится в неактивном режиме. Если не применять процедуру удаления данных об MS (MS Purging), то при поступлении вызова к данному абоненту HLR определяет MS как зарегистрированную в MSC/VLR Германии и направляет вызов в сеть GSM Германии. Затем MSC/VLR сети GSM Германии уведомляет HLR, что абонент недоступен.

При применении процедуры удаления данных об MS (MS Purging) запись узбекистанского абонента будет удалена из MSC/VLR Германии и при поступлении входящего вызова к этому абоненту HLR видит, что MS недоступна и, следовательно, не направляет вызов в MSC/VLR Германии.

Варианты сценариев обслуживания вызовов:

MS в активном режиме. MS находится в активном режиме тогда, когда она занята обслуживанием вызова, это состояние не зависит от вида трафика (речевого, факсимильного или передачи данных) и типа соединения (входящего или исходящего) (рис. 2.18).

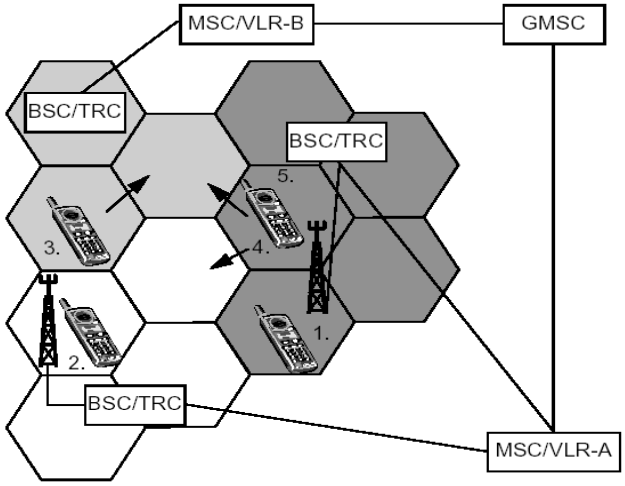


Рис. 2.18. Вариант, когда активируется MS и вариант когда MS находится в активном режиме

1. Исходящий вызов от MS (тип трафика: речевой, факсимильный, передача данных или сообщения SMS).

2. Входящий вызов к MS (тип трафика: речевой, факсимильный, передача данных, сообщений SMS или рассылка сообщений оператора (cell broadcast)).
3. Хэндовер внутри BSC.
4. Хэндовер между разными BSC внутри одного MSC.
5. Хэндовер между разными MSC.

Исходящий вызов (MS – PSTN). Здесь описывается процесс обслуживания исходящего вызова, направленного от MS в сеть общего пользования (рис.2.19). Передача информации и данных описываются отдельно.

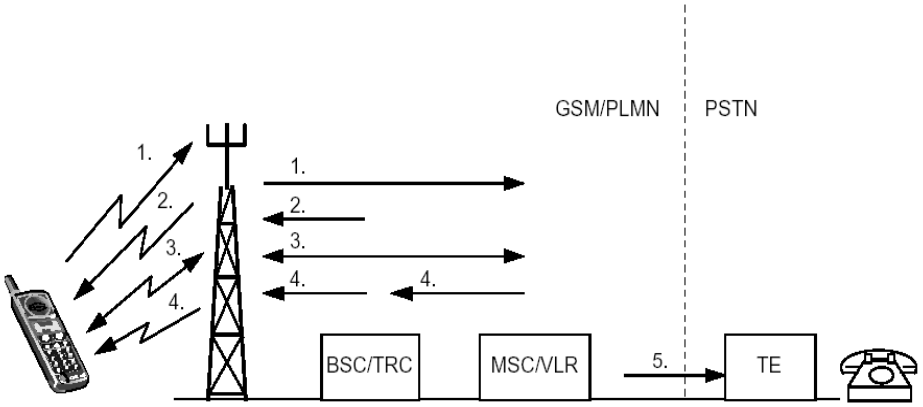


Рис. 2.19. Установление исходящей связи между MS и абонентом сети общего пользования

a. MS использует канал RACH для запроса сигнального канала.

b. BSC/TRC назначает канал AGCH.

c. MS через SDCCH направляет в MSC/VLR запрос на установление соединения. Все процессы сигнализации, предшествующие установлению соединения на канале трафика, проходят через канал SDCCH.

К процессам сигнализации относятся:

1. Отметка в VLR активного состояния MS (IMSI Attach).
2. Процедура аутентификации.
3. Идентификация оборудования.
4. Передача в сеть цифр B-номера абонента (набираемый номер).

5. Проверка статуса услуги «Запрет на исходящую связь» для данного абонента (инициирована/не инициирована).

a. MSC/VLR дает команду BSC/TRC назначить свободный TCH. BTS и MS получают команду настроиться на заданный TCH.

b. MSC/VLR направляет B-номер абонента на PSTN для установления соединения.

c. При ответе абонента связь считается установленной.

Входящий вызов (PSTN - MS). Главным отличием процедуры обслуживания входящего вызова от исходящего вызова является то, что при поступлении входящего вызова на MS неизвестно точное местоположение абонента. Следовательно, прежде чем установить связь с MS, необходимо передать вызывное сообщение для определения местоположения MS.

Ниже приведено описание процедуры установления соединения для входящего вызова от абонента PSTN к мобильному абоненту. Вызов с MS на MS происходит по той же схеме. Отличие только в том, что при входящей связи от MS установление соединения с MSC/VLR проходит через GMSC, а не через узел PSTN (рис.2.20).

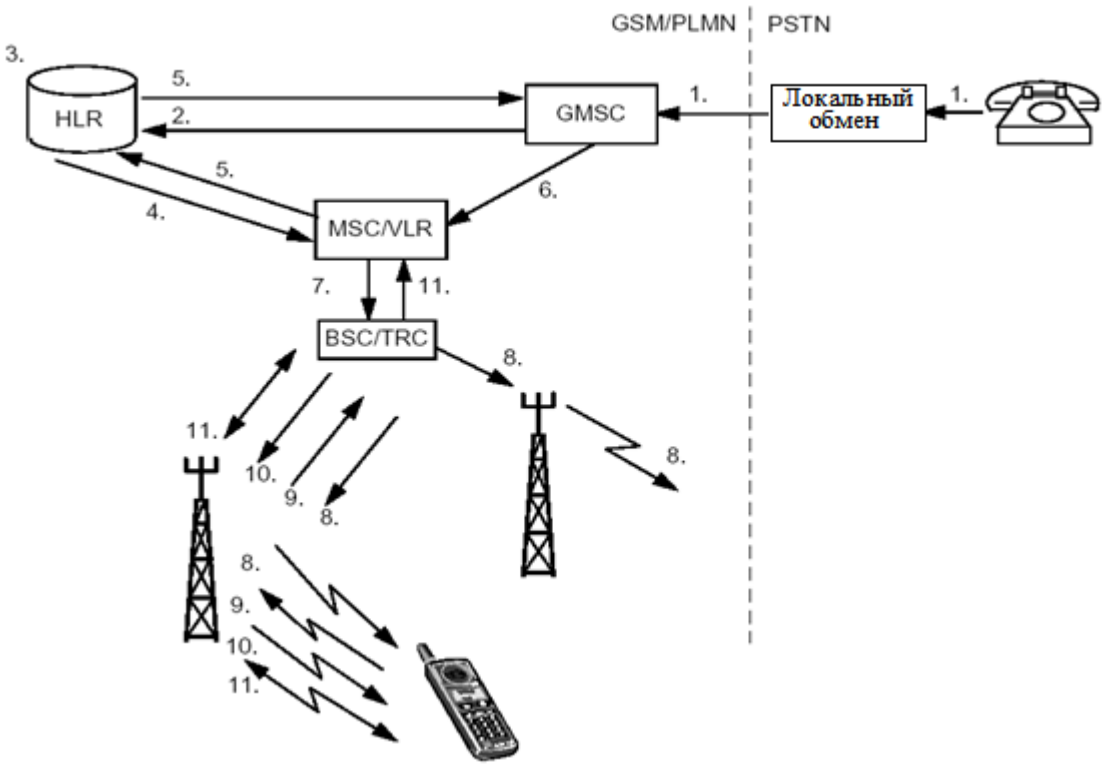


Рис. 2.20. Входящий вызов (PSTN- MS)

1. Абонент PSTN набирает номер MS (MS ISDN). MS ISDN анализируется в PSTN, которая определяет, что осуществляется вызов абонента мобильной сети. Устанавливается связь с GMSC, которому принадлежит MS.
2. GMSC анализирует MSISDN, чтобы выяснить, в каком HLRзарегистрирован MS. Затем GMSC запрашивает у HLR информацию о том, как маршрутизировать вызов на обслуживающий его MSC/VLR.
3. HLR устанавливает соответствие между MS ISDN и IMSI и определяет, какой MSC/VLR обслуживает MS в настоящее время. HLR также проверяет, активизирована ли услуга «Переадресация вызова». Если услуга в активном состоянии, GMSC переадресует вызов на заданный номер.
4. HLR запрашивает MSRN у обслуживающего MSC/VLR.
5. MSC/VLR возвращает MSRN через HLR на GMSC.
6. GMSC анализирует MSRN и маршрутизирует вызов на MSC/VLR.
7. MSC/VLR располагает информацией о том, в какой LA находится MS. Пейджинговое сообщение направляется на BSC, который контролирует эту LA.
8. BSC направляет пейджинговые сообщения на все BTS, которые распространяют ее в нужной LA. BTS передают это сообщение по радиоинтерфейсу, используя канал PCH. Для пейджинга сеть использует IMSI или TMSI, действительный только в зоне обслуживания текущего MSC/VLR.
9. Когда MS определяет, что пейджинговое сообщение предназначено именно ей, она отправляет запрос на выделение канала SDCCH.
10. BSC обеспечивает SDCCH, используя AGCH (передает по каналу AGCH номер канала SDCCH, назначенный данной MS).
11. SDCCH используется для процедуры установления соединения. По этому каналу передается информация о номере канала TCH, назначенного данному MS на время установления соединения.

12. Мобильный телефон начинает звонить. Когда абонент ответит, соединение считается установленным.

Хэндовер (Handover). В терминологии GSM процесс смены сот во время соединения называется хэндовером. Выбор лучшей соты и измерения ее параметров производятся с помощью MS и BTS. Так как MS в выборе хэндовер играет важную роль, такой тип хэндовера часто называется хендовером с участием мобильных систем (MAHO – Mobile Assisted Hand Over).

Процедура осуществления хэндовера (Locating). MS измеряет уровни и качество сигнала своей собственной соты и уровни сигналов несущей BCCH соседних сот. Передача запроса на выполнение измерения производится в направлении dawlink, когда MS находится в активном режиме. Результаты замеров отправляются на BTS по каналу SACCH через определенные интервалы времени (рис. 2.21). Обслуживающая BTS, получая от MS данные измерений, также осуществляет измерения.

Измерения от BTS и MS передаются в форме отчетов об измерениях (Measurement Reports). Основываясь на этих отчетах, BSC принимает решение о необходимости выполнения хэндовера. Если BSC принимает решение о выполнении хэндовера, он определяет, в какую соту будет передаваться управление. Этот процесс называется процедура осуществления хэндовера (locating).

Как только определяется, что какая-то из соседних сот лучше, чем обслуживающая сота, осуществляется хэндовер.

Другой причиной осуществления хэндовера является величина временной задержки (TA). Если она превышает установленное оператором пороговое значение, осуществляется хэндовер. Обычно это происходит во время перемещения MS от одной соты к другой.

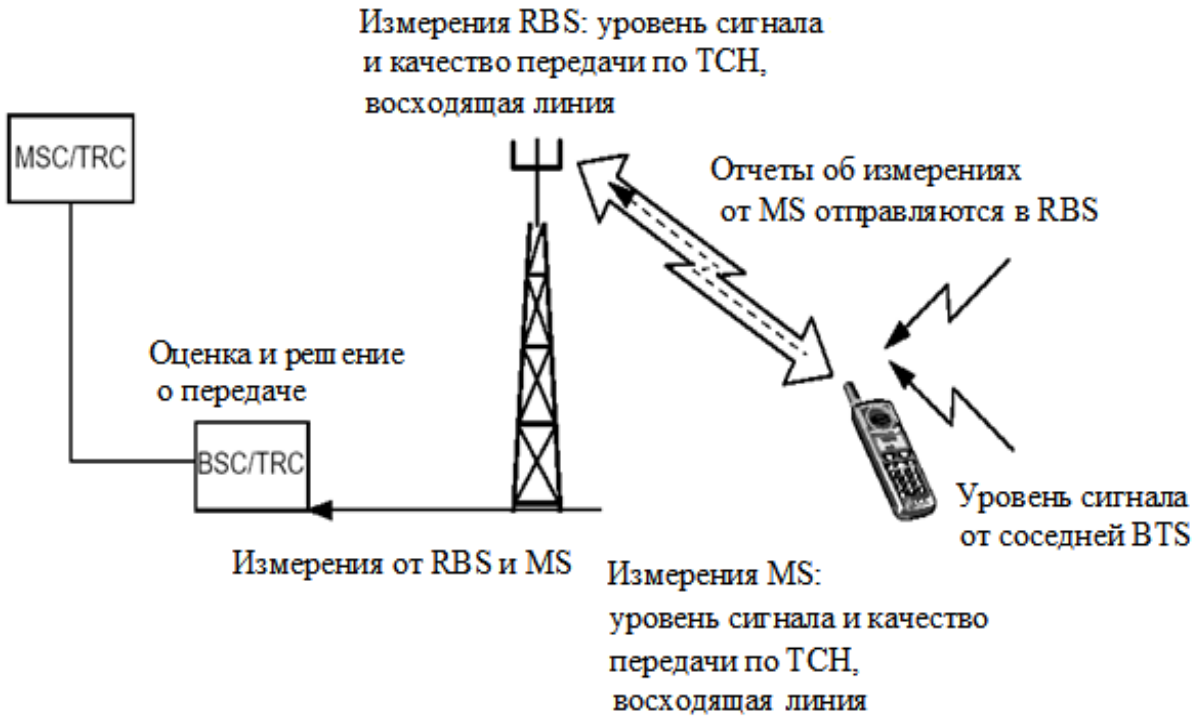


Рис. 2.21. Результаты измерений, передаваемые на BSC

Как только MS переместится в другую соту, новая BTS информирует MS о новых соседних несущих BCCH. Последнее делается для того, чтобы могли быть произведены новые измерения. Если MS также переключается на новую LA, то новые данные об изменении местоположения будут обновлены по окончании разговора.

Хэндовер может использоваться для распределения нагрузки между сотами. Во время попытки установления соединения в перегруженную соту MS может быть перенаправлена в соту с меньшим трафиком, где качество соединения приемлемое.

Различные типы хэндоверов:

- Хэндовер внутри соты;
- Хэндовер между сотами, контролируемыми одной и той же BSC;
- Хэндовер между сотами, контролируемыми разными BSC, но одной и той же MSC/VLR;
- • Хэндовер между сотами, контролируемыми разными MSC.

Каждый из этих случаев описывается более подробно ниже.

Хэндовер внутри соты. Этот тип хэндовера применяется в том случае, если BSC определяет, что качество соединения слишком низкое, но нет никаких данных об измерениях, указывающих на то, что есть сота с лучшими значениями параметров. В этом случае BSC определяет другой канал (частоту) в этой же самой соте, где качество может быть лучше, и MS перенастраивается на этот канал.

Примечание: BSC всегда пытается сначала использовать хэндовер на частотный канал другой соты. В случае, если такого канала нет, применяется внутрисотовый хэндовер.

Хэндовер между сотами, контролируемыми одним и тем же BSC. MSC/VLR не участвует в выполнении междусотового хэндовера между двумя сотами, контролируемыми одной и той же BSC. MSC/VLR будет информирован об осуществлении хэндовер. Если хэндовер охватывает разные LA, то обновление данных о местоположении будет выполнено сразу же, как только соединение завершиться (рис. 2.22).

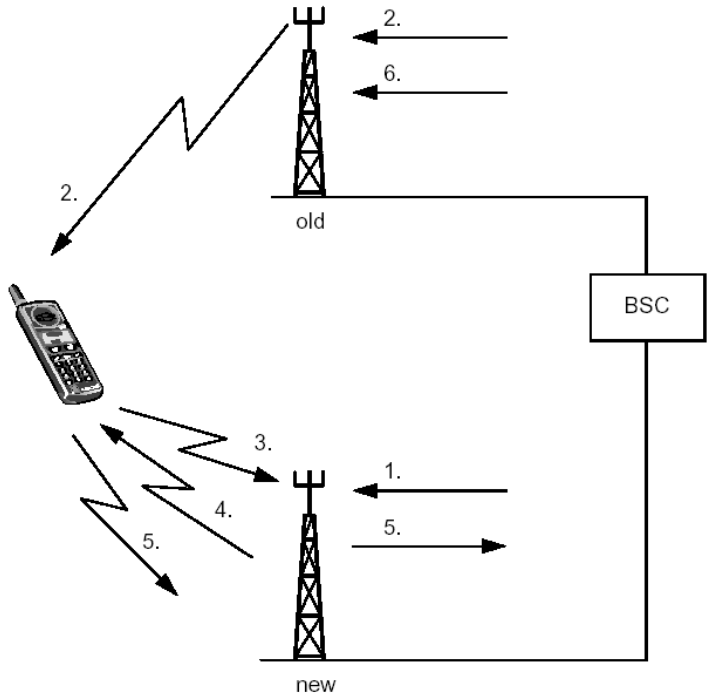


Рис. 2.22. Хэндовер между сотами, контролируемыми одним и тем же BSC

1. BCS посылает команду на новую BTS для занятия TCH.

2. BSC через предыдущую BTS отправляет на MS сообщение о том, на какую частоту и какой временной интервал (TS) необходимо произвести замену, а также какую выходную мощность нужно использовать. Эта информация отправляется на MS по каналу FACCH.
3. MS настраивается на новую частоту и передает пакет доступа для выполнения хэндовера в нужный временной интервал. Так как MS еще не имеет информации о TA, то пакеты для хэндовера очень короткие (только 8 бит информации).
4. Когда новая BTS определяет пакеты, содержащие информацию, необходимую для выполнения хэндовера, она отправляет информацию о TA по FACCH.
5. MS отправляет полное сообщение для хэндовера на новую BSC через новую BS.
6. BSC сообщает предыдущей BTS о необходимости освободить ранее использовавшийся TCH.

Хэндовер между сотами, контролируемыми разными BSC, но одним и тем же MSC/VLR. Если в хэндовере задействован другой BSC, то для установления соединения между этими BSC должен использоваться MSC/VLR (рис. 2.23).

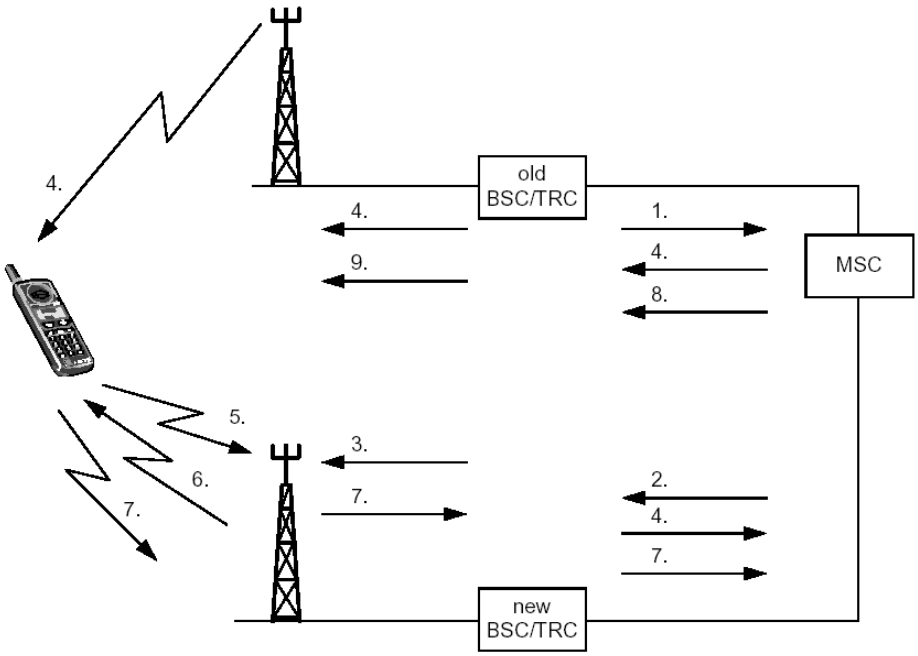


Рис. 2.23. Хэндовер между разными BSC, но внутри одного MSC/VLR

1. Обслуживающий (предыдущий BSC) отправляет в MSC сообщение, содержащее идентификатор нужной соты, с требованием на выполнение хэндовера.
2. MSC располагает информацией о том, какой из BSC контролирует эту соту и отправляет запрос на хэндовер на эту BSC.
3. Новый BSC дает команду нужной BTS для выделения канала TCH.
4. Новый BSC отправляет сообщение на MS через MSC и предыдущую BTS.
5. MS настраивается на новую частоту и передает пакет доступа для хэндовера, который будет выполняться в указанный временной интервал.
6. Новая BTS отправляет информацию о величине TA.
7. MS отправляет полное сообщение о хэндовере на MSC через новый BSC.
8. MSC отправляет предыдущему BSC команду на освобождение ранее использовавшегося канала TCH.

*Хэндовер между сотами, контролируемыми разными MSC*может применяться внутри одной PLMN. Соты, контролируемые разными MSC/VLR, соответственно, контролируются разными BSC (рис. 2.24).

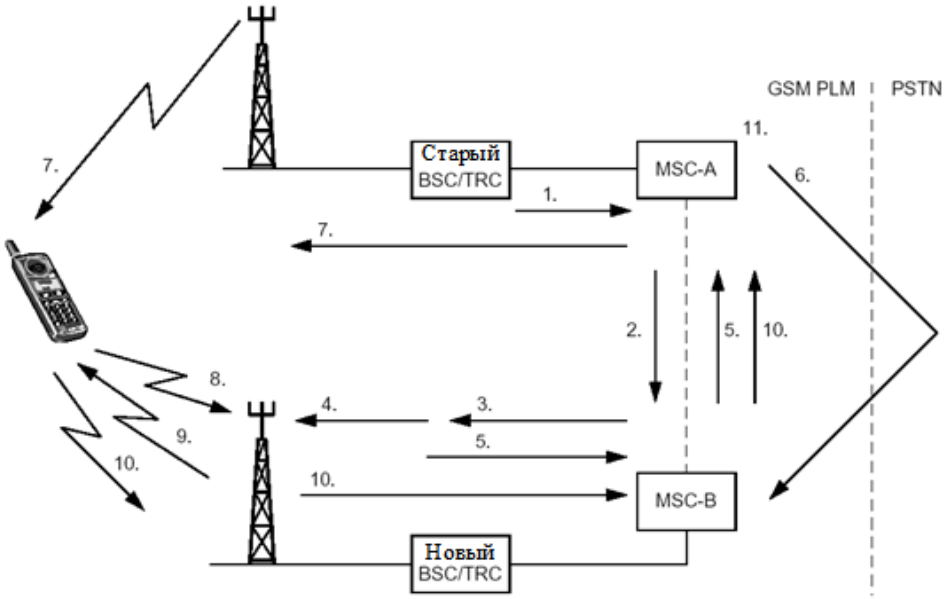


Рис. 2.24. Межсотовый хэндовер между разными MSC/VLR

1. Обслуживающий (предыдущий) BSC отправляет сообщение с требованием на хэндовер на обслуживающий MSC (MSC-A) с идентификацией нужной соты.
2. MSC-A определяет, что эта сота принадлежит другой MSC (MSC-B) и запрашивает ее.
3. MSC-B определяет номер хэндовера для перемаршрутизации. Далее запрос на хэндовер отправляется на новую BSC.
4. Новый BSC отправляет команду нужной BTS для занятия TCH.
5. MSC-B получает информацию и передает ее на MSC-A вместе с номером хэндовера.
6. Установление соединения с MSC-B возможно через PSTN.
7. MSC-A отправляет команду на хэндовер на MS через предыдущий BSC.
8. MS настраивается на новую частоту и передает пакеты доступа в нужный временной интервал.
9. Когда новая BTS определяет пакеты для хэндовера, она отправляет информацию о временной задержке (TA).
10. MS отправляет полное сообщение о хэндовере на предыдущий MSC через новый BSC и новый MSC.
11. После этого устанавливается новый путь в MSC-A и соединение устанавливается через него.
12. Предыдущий TCH освобождается тем BSC, который ранее управлял соединением (на рис.2.24 этого не показано).

Предыдущий MSC (MSC-A) контролирует соединение до тех пор, пока оно не будет прекращено. Связано это с тем, что в нем содержится информация об абоненте и подробностях соединения, которые необходимы для тарификации.

MS после прекращения соединения должна обновить данные о местоположении, так как LA не может принадлежать более чем одной зоне обслуживания MSC. HLR передает данные в VLR-B для обновления в нем

информации, а VLR-B, в свою очередь, передает в VLR-A команду на удаление всей информации о мобильном абоненте.

Международный вызов. Одной из основных характеристик GSM является возможность использования международного роуминга и осуществления международных соединений. Для того, чтобы абоненты могли воспользоваться услугой роуминга в сетях, принадлежащих операторам разных сетей сотовой связи, необходимо заключить между операторами роуминговое соглашение. Это же касается международного роуминга.

Процессы обслуживания международных вызовов при роуминге не отличаются от вариантов обслуживания вызовов абонентов, находящихся в пределах собственной сети. Но, тем не менее, рассмотрим два случая, характерных для случая роуминга.

Включение IMSI (IMSI Attach). Когда MS требует обслуживания в режиме международного роуминга, происходит следующее:

1. MS включается и начинает сканировать все частоты GSM внутри одного частотного диапазона (GSM –900). Производится поиск несущей BCCH. MS настраивается на ту несущую BCCH, которая имеет наибольший уровень сигнала и считывает ее системную информацию. Так происходит распознавание сетевого оператора.
2. MS сравнивает идентификатор сети со списком запрещенных PLMN, хранящимся в памяти SIM. Этот список содержит все сетевые идентификаторы, с которыми домашний оператор не имеет роуминговых соглашений. Если сеть, на которую настроилась MS, является запрещенной, то MS продолжает поиск разрешенной сети.
3. Если MS не находит разрешенной сети, но идентифицировала запрещенную сеть, то она выдает сообщение «Только экстренные вызовы». Если MS находит разрешенную сеть, то она настраивается на нее и отправляет сообщение о регистрации IMSI (IMSI Attach).

4. Этот случай идентичен случаю нормальной регистрации IMSI (в собственной сети). Отличие состоит только в том, что абонентский HLR находится в другой стране.

Вызов на MS. Когда MS находится в международном роуминге и на нее поступает вызов, процедура идентична той, когда MS находится в своей собственной сети. Разница лишь в том, что используемые GMSC и HLR находятся в собственной сети, а MSC/VLR находится в сети другой страны.

Процедура Drop back. Следующий случай показывает преимущество использования процедуры drop back (рис.2.25).

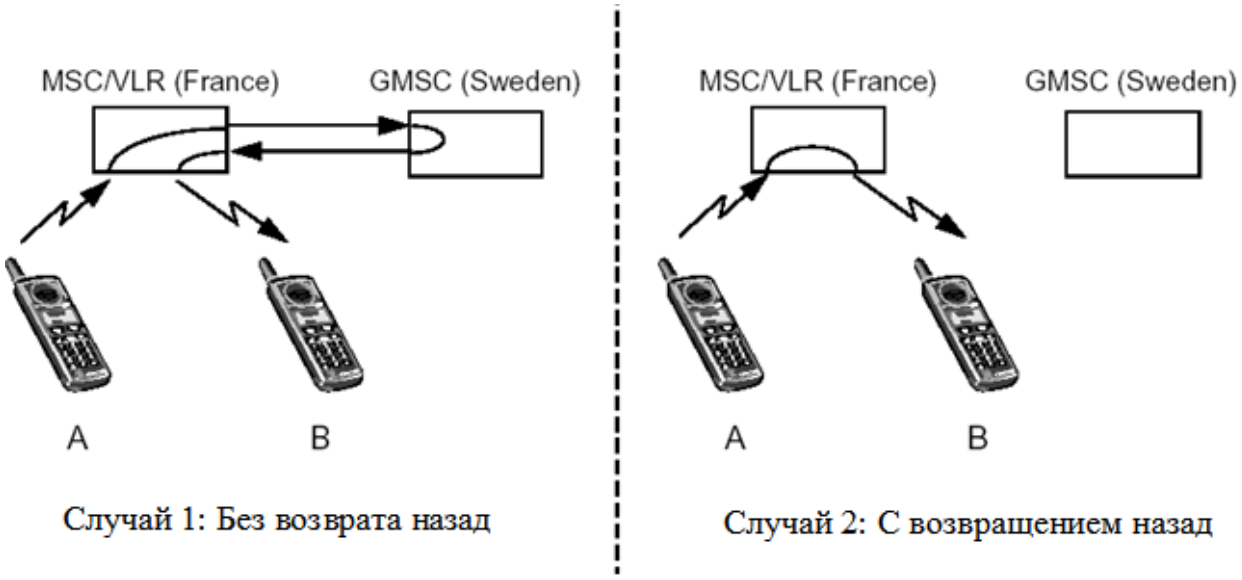


Рис. 2.25. Случай, показывающий преимущества при использовании drop back

В данную процедуру вовлекается два абонента. Рассмотрим пример, когда:

- Абонент ***A*** из Франции находится во Франции, его MS контролируется собственной MSC.
- Абонент ***B*** из Узбекистана находится в настоящий момент в Международном роуминге во Франции, его MS контролируется MSC/VLR-A.
- Абонент ***A*** звонит абоненту B. Вызов маршрутизируется из Франции в Узбекистан.

1. Сеть Узбекистана определяет, что абонент ***B*** находится в зоне действия MSC/VLR-A во Франции и перенаправит вызов обратно во Францию. Абоненты соединяются друг с другом в сети GSM Франции и ведут разговор.

- *Без использования процедуры drop back:* разговор при вызове идет через GMSC Узбекистана.
- *С использованием процедуры drop back***:** разговор при вызове переключается внутри MSC/VLR-A, что существенно влияет на стоимость разговора.

*Передача коротких сообщений***.** Служба коротких сообщений (SMS) предоставляет мобильным станциям средства для обмена текстовыми сообщениями, содержащими до 160 буквенно-цифровых символов. SMS-C (SMS Center) является хранилищем и центром, перенаправляющим короткие сообщения.

SMS поддерживает две основные услуги:

- Мобильный прием SMS: от SMS-C на MS
- Мобильная передача SMS: от MS на SMS-C

В обоих случаях MS находится в состоянии IDLE. Если MS находится в активном режиме, то короткие сообщения передаются по каналу SACCH. Пейджинг, установление соединения, аутентификация и т.д. в этом случае не требуется.

Передача SMS с MS. Мобильная передача SMS подразумевает передачу коротких сообщений от MS на SMS-C, который, в свою очередь, обеспечивает информацию о доставке сообщения, либо о его недоставке (рис.2.26).

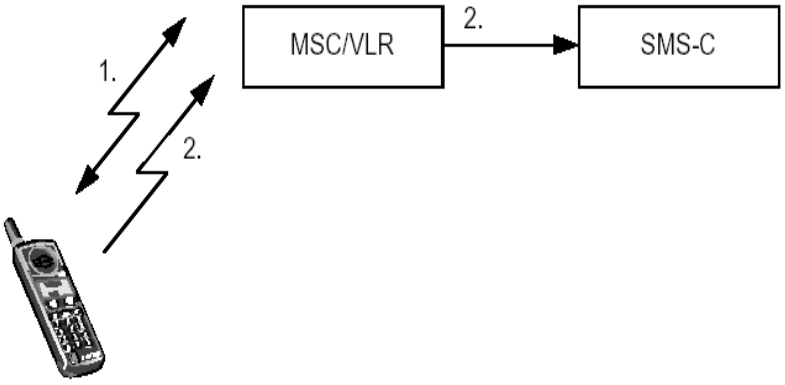


Рис. 2.26. Мобильная передача коротких сообщений

- MS устанавливает соединение с сетью, как в случае нормального установления соединения, используя сигнальные каналы RACH, AGCH, SDCCH.
- Если аутентификация прошла успешно, MS отправляет короткое сообщение по каналу SDCCH на SMS-C через MSC/VLR. SMS-C перенаправляет короткое сообщение в пункт назначения. Это может быть MS или терминал выделенной сети, например, PC.

Мобильный прием SMS- это возможность передачи коротких сообщений от SMS-C на MS (рис. 2.27).

1. Пользователь отправляет сообщение на SMS-C.
2. SMS-C отправляет сообщение на SMS-GMSC.
3. SMS-GMSC запрашивает HLR для маршрутизации вызова.
4. HLR возвращает информацию о маршруте на SMS-GMSC
5. SMS-GMSC перенаправляет сообщение на MSC/VLR.
6. На MS поступает вызывной сигнал, устанавливается соединение с сетью, так же как, для случая установления речевого соединения.
7. Если аутентификация успешна, то MSC/VLR передает короткое сообщение на MS, используя сигнальный канал SDCCH.
8. Если передача была успешной, то MSC/VLR отправляет отчет на SMS-C.Если нет, то MSC/VLR информирует HLR, и отчет о недоставке отправляется на SMS-C.

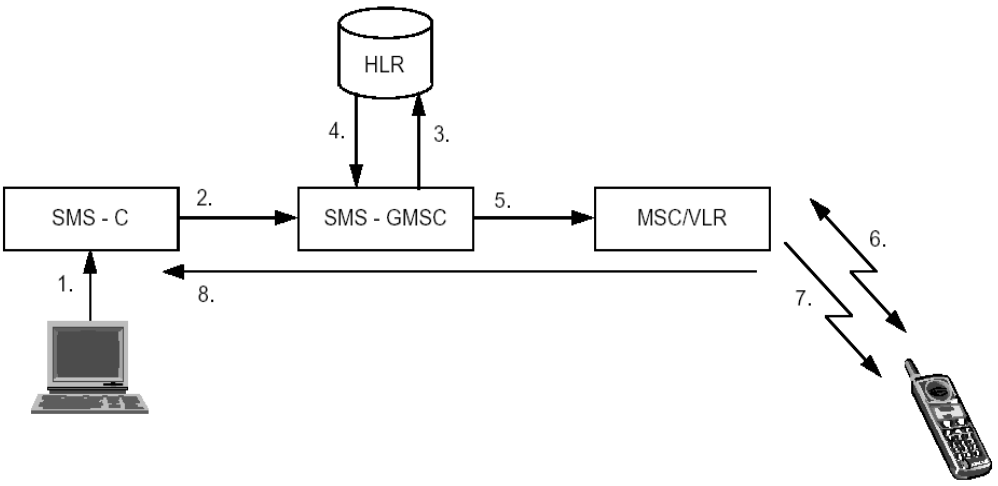


Рис. 2.27. Прием коротких сообщений

В случае неуспешной доставки, SMS-C информирует HLR и VLR о том, что сообщение ожидает отправки на MS. HLR затем проинформирует SMS-C о том, когда MS станет доступной. Прием сообщений SMS-C может идти от различных источников, например, телекса, факсимильного аппарата, из сети Интернет.

Контрольные вопросы

1. Что понимается под управлением мобильностью?
2. Что понимается под Location update (LU) и как она осуществляется?
3. Какую информацию передает при включении телефон и куда она попадает?
4. Как используется информация LU?
5. Как часто происходит обновление зоны местоположения абонента?
6. Что понимается под Location Area (LA) и его назначение?
7. Что такое роуминг в сотовой сети связи?
8. Какие требования существуют для организации роуминга и какие условия существуют для его обеспечения?
9. Какие существуют три вида роуминга?
10. Поясните основные процедуры взаимодействия сетей GSM при роуминге.

11. Как осуществляется тарификация вызовов при роуминге в сетях GSM?
12. Какие перспективы развития у роуминга?
13. Что понимается под идентификатором сети GSM?
14. Что понимается под номером мобильной станции (MSISDN) и к какому идентификатору он относится?
15. Что понимается под интернациональным идентификатором мобильного абонента (IMSI) и к какому идентификатору он относится?
16. Что понимается под временным идентификатором мобильного абонента (TMSI) и к какому идентификатору он относится?
17. Что понимается под идентификационным номером оборудования MS (IMEI) и к какому идентификатору он относится?
18. Что понимается под интернациональным идентификатором оборудования MS и номера программного обеспечения (IMEISV) и к какому идентификатору они относится?
19. Что понимается под идентификатором местоположения (LAI) и к какому идентификатору он относится?
20. Что понимается под Cell Global Identity (CGI) и к какому идентификатору он относится?
21. Что понимается под глобальным идентификатором соты CGI и к какому идентификатору он относится?
22. Что понимается под идентификационным кодом БС (BSIC) и к какому идентификатору он относится?
23. Что понимается под номером местоположения LN и к какому идентификатору он относится?
24. Что понимается под идентификатором локальной зоны абонирования (RSZI) и к какому идентификатору он относится?
25. Что понимается под конфиденциальной процедурой идентификации абонента?
26. Какая последовательность обслуживание MS в состоянии IDLE?
27. Как осуществляется включение MS в сеть?

28. Как организуется сетевой роуминг.
29. На что указывает отключение IMSI от сети?
30. Какие существуют варианты сценариев обслуживания вызовов
31. Что понимается и как организуется Хэндовер?
32. Как организуется международный вызов?

ГЛАВА 3. АСПЕКТЫ БЕЗОПАСНОСТИ В СТАНДАРТЕ GSM

3.1. SIM карта и обеспечение безопасности в стандарте GSM

SIM-карта. Каждый абонент мобильной связи стандарта GSM на время пользования системой сотовой связи получает стандартный модуль подлинности абонента, так называемую SIM-карту (SIM –Subscriber Identity Module, SIM –card). В аппаратах (мобильных телефонах) стандарта GSM используется унифицированная съемная SIM-карта, одинаковая для всех стандартов GSM: GSM 900, GSM 1800 и GSM 1900 и выполненная в двух вариантах:

- стандартная (стандарт ISO) – размером 55x85 мм, типа банковой кредитной карты;
- чаще, миниатюрная, «вставная» (plug-in) размером 15x25 мм.

Толщина SIM-карта в обоих случаях менее 1 мм.

MS без SIM-карты неработоспособна, хотя и в этом случае с него можно сделать экстренные вызовы по номеру 112 – международному номеру экстренной помощи.

Модуль SIM-карты вручается одновременно с мобильным телефоном и в принципе позволяет вести разговор с любого аппарата стандарта GSM, в том числе и с таксофонного. SIM-карта содержит следующую информацию:

- PIN (Personal Identification Number) – персональный идентификационный номер абонента, так называемый PIN-код;
- IMSI (International Mobile Subscriber Identity) – международный идентификатор абонента мобильной связи;
- Ki – индивидуальный ключ аутентификации абонента;
- A3– индивидуальный алгоритм аутентификации абонента;
- A8 – алгоритм вычисления ключа шифрования.

После включения MS с установленной SIM-картой абонент обязан, прежде всего, снять блокировку последней и ввести PIN-код, известный только абоненту, который должен служить защитой от несанкционированного использования SIM-карты, например, при утере. После трех неудачных попыток набора PIN-код SIM-карта блокируется, и блокировка может быть снята либо набором дополнительного кода – персонального кода разблокировки PUK (Personal Unbloc king Key), либо по команде с центра коммутации. PIN-код может быть изменен по усмотрению абонента и по соглашению с оператором сотовой сети.

Кроме того, на SIM-карте имеется некоторый объем доступной для абонента оперативной памяти, позволяющий записать до 100 номеров телефонов с комментариями (например, с именами абонентов) и до 10 текстов коротких сообщений.

Когда SIM-карта вынимается из MS, она сохраняет всю содержащею в ней информацию:

- персональные идентификаторы;
- ключи;
- шифры и пороли;
- записанные абонентом номера ТЛФ и сообщений, и может работать с другими MS стандарта GSM.

Таким образом, SIM-карта как бы «персонализует» абонентский аппарат MS, в которой она устанавливается.

Аспекты безопасности в стандарте GSM. Сотовые системы подвижной связи нового поколения в состоянии принять всех потенциальных пользователей, если будут гарантированы безопасность связи: секретность и аутентификация. Секретность должна исключить возможность извлечения информации из каналов связи кому-либо, кроме санкционированного получателя. Проблема аутентификации заключается в том, чтобы помешать кому-либо, кроме санкционированного пользователя (отправителя), изменить канал, то есть получатель должен быть уверен, что в настоящий момент он

принимает сообщение от санкционированного пользователя. Основным способом обеспечения секретности является шифрование. Относительно новая концепция - использование шифрования как способа аутентификации сообщений.

Аутентификация сообщений через шифрование осуществляется за счет включения в текст так называемого кода идентификации (то есть фиксированного или зависящего от передаваемых данных слова, которое знают отправитель и получатель или которое они могут выделить в процессе передачи). Получатель расшифровывает сообщение, путем сравнения получает удостоверение, что принимаемые данные являются именно данными санкционированного отправителя.

К системе шифрования предъявляются следующие основные требования:

- нелинейные связи между исходным текстом и зашифрованным текстом;
- изменение параметров шифрования во времени.

Если алгоритмы шифрования отвечают первому требованию, то, не зная ключа, исключается возможность изменить код идентификации, чтобы избежать обнаружения факта несанкционированного доступа. Второе требование исключает возможность нарушения работы системы за счет воспроизведения "обнаружителем" принятого ранее и записанного в память сообщения.

Один путь обеспечения этих требований - применение синхронных систем передачи, но при этом необходимы системы цикловой и тактовой синхронизации, что во многих случаях неприемлемо.

Второй путь - включение в информационную последовательность (каждое сообщение) временных меток так, чтобы зашифрованные данные были бы однозначно с ними связаны.

Алгоритмы шифрования делятся на два класса [1,5-7];

- классические алгоритмы;
- алгоритмы с открытым ключом.

Классические алгоритмы используют один ключ для шифрования-дешифрования. Алгоритмы с открытым ключом используют два ключа: первый - для перехода от нешифрованного текста к шифрованному; второй - для обратного перехода от шифрованного к нешифрованному. Причем знание одного ключа не должно обеспечить обнаружение второго ключа. В этих алгоритмах один из ключей, обычно используемый для шифрования, можно сделать общим, и только ключ, используемый для расшифровки, должен быть засекречен. Эта особенность очень полезна для снижения сложности протокола и интеграции структур шифрования в сетях связи.

Алгоритмы шифрования с открытым ключом построены на определении односторонней функции, то есть некоторой функции f, такой, что для любого x из ее области определения f (x) легко вычислима, однако практически для всех y из ее области значений нахождение x, для которого y=f(x) вычислительно, не осуществимо [10-11]. То есть, односторонняя функция является отдельной функцией, которая легко рассчитывается ЭВМ в приемлемом объеме времени, но время расчета обратной функции в существующих условиях недопустимо большое.

Первый алгоритм шифрования с общим ключом был назван RSA (первые буквы фамилий авторов Rivest, Shamir, Adieman). Алгоритм базируется на двух функциях E и D, связанных соотношением:

$$D (E (*) = E (D(*)).$$

Одна из этих функций используется для шифрования сообщений, другая - для дешифрования. Секретность алгоритма основана на том, что знание функции E (или D) не открывает легкого способа вычисления D (или E). Каждый пользователь делает общей функцию E и хранит в секрете функцию D, то есть для пользователя X есть открытый ключ Ex и секретный Dx.

Два пользователя А и В могут использовать алгоритм RSA, чтобы передать любое зашифрованное сообщение. Если абонент А хочет отправить сообщение М абоненту В, то он может сделать это следующим образом:

- зашифровать сообщение М;
- подписать сообщение М;
- зашифровать и подписать М.

В первом случае: А обеспечивает преобразование М, используя открытый ключ С = Ев (М)и посылает его абоненту В. В принимает С и вычисляет db (c) = db (Ев (М)) = М.

Во втором случае: А подписывает М посредством вычисления F= Da (M) и посылает F абоненту В (эти операции может осуществлять только пользователь А, которому известен секретный ключ Da). В получает F и вычисляет Ea (F) =Ea (Da (M)) = M.В теперь известно, что сообщение М действительно послано пользователем А. В этом случае секретность сообщения М не гарантируется, так как все могут осуществить такую же операцию с использованием общего ключа Ea.

В третьем случае: А вычисляет F = Da (M) и C = Ев (F) = Ев (Da (M); А посылает С к В. В получает С и вычисляет db (c) = db (Ев (F)) = Da (M); В может теперь легко получить М, вычислив Ea (Da (M)) = M.

До операции шифрования каждое сообщение М должно разделяться на блоки фиксированной длины, затем каждый блок кодируется как совокупность фиксированного числа цифр. RSA кодер оперирует такими отдельными блоками в каждом цикле кодирования. Полное описание алгоритма RSA изложено, например, в [8].

Алгоритм шифрования с открытым ключом RSA обеспечивает высокую степень безопасности передачи речевых сообщений и рекомендован к использованию в цифровых системах подвижной радиосвязи нового поколения.

В стандарте GSM термин "безопасность" понимается как исключение несанкционированного использования системы и обеспечение секретности

переговоров подвижных абонентов. Определены следующие механизмы безопасности в стандарте GSM [8]:

- аутентификация;
- секретность передачи данных;
- секретность абонента;
- секретность направлений соединения абонентов.

Защита сигналов управления и данных пользователя осуществляется только по радиоканалу. Режимы секретности в стандарте GSM определяются Рекомендациями, приведенными в таблице 3.1.

Таблица 3.1.

Режимы секретности в стандарте GSM

Аспекты секретности	Определяет характеристики безопасности, применяемые в сетях GSM. Регламентируется их применение в подвижных станциях и сетях
Секретность, связанная с функциями сети	Определяет функции сети, необходимые для обеспечения характеристик безопасности, рассматриваемых в рекомендациях GSM 02.09
Алгоритмы секретности	Определяет криптографические алгоритмы в системе связи
Модули подлинности абонентов (SIM)	Определяет основные характеристики модуля SIM

Рассмотрим последовательно механизмы безопасности в стандарте GSM, общий состав секретной информации, а также ее распределение в аппаратных средствах GSM системы. При этом будем использовать термины и обозначения, принятые в рекомендациях GSM.

Механизмы аутентификации. Для исключения несанкционированного использования ресурсов системы связи вводятся и определяются механизмы

аутентификации - удостоверения подлинности абонента. Каждый подвижный абонент на время пользования системой связи получает стандартный модуль подлинности абонента (SIM-карту), который содержит:

- международный идентификационный номер подвижного абонента (IMSI);
- свой индивидуальный ключ аутентификации (Ki);
- алгоритм аутентификации (A3).

С помощью, заложенной в SIM информации в результате взаимного обмена данными между подвижной станцией и сетью осуществляется полный цикл аутентификации и разрешается доступ абонента к сети.

Процедура проверки сетью подлинности абонента реализуется следующим образом. Сеть передает случайный номер (RAND) на подвижную станцию. Подвижная станция определяет значение отклика (SRES), используя RAND, Ki и алгоритм A3:SRES = Ki [RAND].

Подвижная станция посылает вычисленное значение SRES в сеть, которая сверяет значение принятого SRES со значением SRES, вычисленным сетью. Если оба значения совпадают, подвижная станция может осуществлять передачу сообщений. В противном случае связь прерывается, и индикатор подвижной станции должен показать, что опознавание не состоялось.

По причине секретности вычисление SRES происходит в рамках SIM. Несекретная информация (такая как Ki) не подвергается обработке в модуле SIM. Процедура аутентификации иллюстрируется рисунке 3.1.

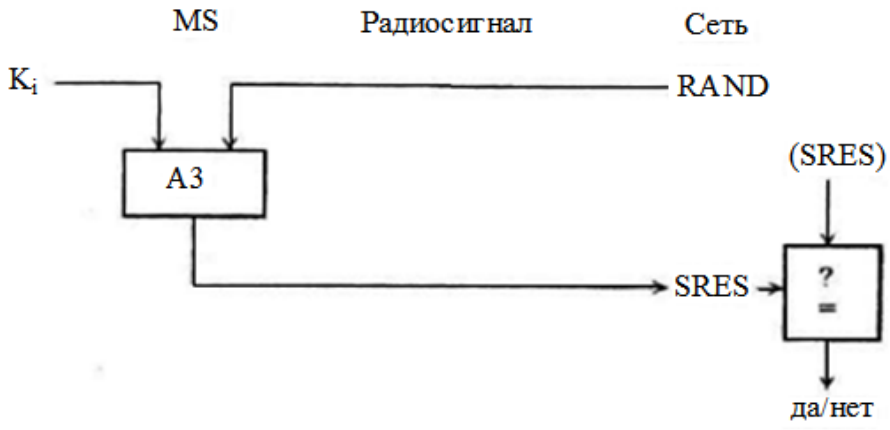


Рис. 3.1. Процедура аутентификации

Секретность передачи данных. Ключ шифрования. Для обеспечения секретности передаваемой по радиоканалу информации вводится следующий механизм защиты. Все конфиденциальные сообщения должны передаваться в режиме защиты информации. Алгоритм формирования ключей шифрования (A8) хранится в модуле SIM. После приема случайного номера RAND подвижная станция вычисляет, кроме отклика SRES, также и ключ шифрования (Кс), используя RAND, Ki и алгоритм A8 (рис.3.2):

$$Кс = Ki\ [RAND].$$

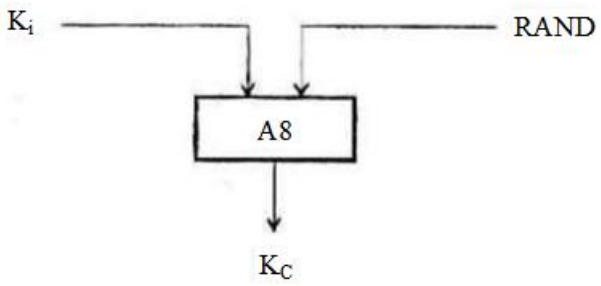


Рис. 3.2. Вычисление ключа шифрования (Кс)

Ключ шифрования Кс не передается по радиоканалу. Как подвижная станция, так и сеть вычисляют ключ шифрования, который используется другими подвижными абонентами. По причине секретности вычисление Кс происходит в SIM.

Числовая последовательность ключа шифрования. Кроме случайного числа RAND сеть посылает подвижной станции числовую последовательность ключа шифрования. Это число связано с действительным значением Кс и позволяет избежать формирование неправильного ключа. Число хранится подвижной станцией и содержится в каждом первом сообщении, передаваемом в сеть. Некоторые сети принимают решение о наличии числовой последовательности действующего ключа шифрования в случае, если необходимо приступить *к* опознаванию или, если выполняется предварительное опознавание, используя правильный ключ шифрования. В некоторых случаях это допущение реально не обеспечивается.

Установка режима шифрования. Для установки режима шифрования сеть передает подвижной станции команду CMC (Ciphering Mode Command) на переход в режим шифрования. После получения команды CMC подвижная станция, используя имеющийся у нее ключ, приступает к шифрованию и дешифрованию сообщений. Поток передаваемых данных шифруется бит за битом или поточным шифром, используя алгоритм шифрования A5 и ключ шифрования Кс.

Обеспечение секретности абонента. Для исключения определения (идентификации) абонента путем перехвата сообщений, передаваемых по радиоканалу, каждому абоненту системы связи присваивается "временное удостоверение личности" - временный международный идентификационный номер пользователя (TMSI), который действителен только в пределах зоны расположения (LA). В другой зоне расположения ему присваивается новый TMSI. Если абоненту еще не присвоен временный номер (например, при первом включении подвижной станции), идентификация проводится через международный идентификационный номер (IMSI). После окончания процедуры аутентификации и начала режима шифрования временный идентификационный номер TMSI передается на подвижную станцию только в зашифрованном виде. Этот TMSI будет использоваться при всех последующих доступах к системе. Если подвижная станция переходит в новую область расположения, то ее TMSI должен передаваться вместе с идентификационным номером зоны (LAI), в которой TMSI был присвоен абоненту.

Обеспечение секретности в процедуре корректировки местоположения. При выполнении процедуры корректировки местоположения по каналам управления осуществляется двухсторонний обмен между MS и BTS служебными сообщениями, содержащими временные номера абонентов TMSI. В этом случае в радиоканале необходимо обеспечить секретность переименования TMSI и их принадлежность конкретному абоненту.

Рассмотрим, как обеспечивается секретность в процедуре корректировки местоположения в случае, когда абонент проводит сеанс связи и при этом осуществляет перемещение из одной зоны расположения в другую. В этом случае подвижная станция уже зарегистрирована в регистре перемещения VLR с временным номером TMSI, соответствующим прежней зоне расположения. При входе в новую зону расположения осуществляется процедура опознавания, которая проводится по-старому, зашифрованному в радиоканале TMSI, передаваемому одновременно с наименованием зоны расположения LAI. LAI дает информацию центру коммутации и центру управления о направлении перемещения подвижной станции и позволяет запросить прежнюю зону расположения о статусе абонента и его данные, исключив обмен этими служебными сообщениями по радиоканалам управления.

Общий состав секретной информации и ее распределение в аппаратных средствах GSM. В соответствии с рассмотренными механизмами безопасности, действующими в стандарте GSM, секретной считается следующая информация:

- RAND - случайное число, используемое для аутентификации подвижного абонента;
- значение отклика - ответ подвижной станции на полученное случайное число;
- индивидуальный ключ аутентификации пользователя, используемый для вычисления значения отклика и ключа шифрования;
- ключ шифрования, используемый для шифрования/дешифрования сообщений, сигналов управления и данных пользователя в радиоканале;
- алгоритм аутентификации, используемый для вычисления значения отклика из случайного числа с использованием ключа Ki;
- алгоритм формирования ключа шифрования, используемый для вычисления ключа Кс из случайного числа с использованием ключа Ki;

- алгоритм шифрования/дешифрования сообщений, сигналов управления и данных пользователя с использованием ключа Кс;
- номер ключевой последовательности шифрования, указывает на действительное число Кс, чтобы избежать использования разных ключей на передающей и приемной сторонах;
- временный международный идентификационный номер пользователя.

В таблице 3.2. показано распределение секретной информации в аппаратных средствах системы связи GSM.

Таблица 3.2

Распределение секретной информации в аппаратных средствах системы связи GSM

NN п.п.	Аппаратные средства	Вид секретной информации
1	Подвижная станция (без SIM)	A5
2	Модуль подлинности абонента (SIM)	A3; A8; IMSI; Ki; TMSI/LAI; Kc/CKSN
3	Центр аутентификации (AUC)	A3; A8; IMSI/Ki
4	Регистр местоположения (HLR)	Группы IMSI/RAND/SRES/Kc
5	Регистр перемещения (VLR)	Группы IMSI/RAND/SRES/Kc, IMSI/TMSI/LAI/Kc/CKSN
6	Центр коммутации (MSC)	A5, TMSI/IMSI/Kc
7	Контроллер базовой станции (BSC)	A5, TMSI/IMSI/Kc***

Обеспечение секретности при обмене сообщениями между HLR, VLR и MSC. Основным объектом, отвечающим за все аспекты безопасности, является центр аутентификации (AUC). Этот центр может быть отдельным объектом или входить в состав какого-либо оборудования, например, в

регистр местоположения (HLR). Как управлять AUC будет решать тот, кому будет поручена эксплуатация сети. Интерфейс GSM с AUC не определен.

AUC может решать следующие задачи:

- формирование индивидуальных ключей аутентификации пользователей Ki и соответствующих им международных идентификационных номеров абонентов (IMSI);
- формирование набора RAND/SRES/Kc для каждого IMSI и раскрытие этих групп для HLR при необходимости.

Если подвижная станция переходит в новую зону расположения с новым VLR, новый VLR должен получить секретную информацию об этой подвижной станции. Это может быть обеспечено следующими двумя способами:

- подвижная станция проводит процедуру идентификации по своему международному номеру IMSI. При этом VLR запрашивает у регистра местоположения HLR группы данных " RAND/SRES/Kc, принадлежащих данному IMSI;
- подвижная станция проводит процедуру аутентификации, используя прежний временный номере TMSI с наименованием зоны расположения LAI. Новый VLR запрашивает прежний VLR для посылки международного номера IMSI и оставшихся групп из RAND/SRES/Kc, принадлежащих этим TMSI/LAI, если подвижный абонент остается на более длительный период в VLR, тогда после некоторого количества доступов с аутентификацией VLR из соображений секретности потребует новые группы RAND/SRES/Kc от HLR. Все эти процедуры определены в рекомендации GSM 09.02.

Проверка аутентификации выполняется в VLR. VLR посылает RAND на коммутационный центр (MSC) и принимает соответствующие отклики SRES. После положительной аутентификации TMSI размещается с IMSI. TMSI и используемый ключ шифрования Kc посылаются в центр коммутации (MSC). Эти же процедуры определяются в рекомендации GSM 09.02.

Передача секретной информации по радиоканалу уже описана в предыдущих разделах и определена в рекомендации GSM 04.08.

Модуль подлинности абонента. Введение режима шифрования в стандарте GSM выдвигает особые требования к подвижным станциям, В частности, индивидуальный ключ аутентификации пользователя Ki, связанный с международным идентификационным номером абонента IMSI, требует высокой степени защиты. Он также используется в процедуре аутентификации.

Модуль подлинности абонента SIM содержит полный объем информации о конкретном абоненте. SIM реализуется конструктивно в виде карточки с встроенной электронной схемой. Введение SIM делает подвижную станцию универсальной, так как любой абонент, используя свою личную SIM-карту, может обеспечить доступ к сети GSM через любую подвижную станцию.

Несанкционированное использование SIM исключается введением в SIM индивидуального идентификационного номера (PIN), который присваивается пользователю при получении разрешения на работу в системе связи и регистрации его индивидуального абонентского устройства.

Основные характеристики модуля SIM определены в Рекомендации GSM 02.17. Состав секретной информации, содержащейся в SIM, показан в таблице 3.2.

В заключение следует отметить, что выбранные в стандарте GSM механизмы секретности и методы их реализации определили основные элементы передаваемых информационных блоков и направления передачи, на которых должно осуществляться шифрование: (RAND/SRES/Kc от HLR к VLR; RAND и SRES - в радиоканале). Для обеспечения режима секретности в стандарте GSM решены вопросы минимизации времени соединения абонентов. При организации систем сотовой радиосвязи по стандарту GSM имеется некоторая свобода в применении аспектов безопасности. В частности, не стандартизованы вопросы использования центра

аутентификации AUC (интерфейс с сетью, структурное размещение AUC в аппаратных средствах). Нет строгих рекомендаций на формирование закрытых групп пользователей и системы приоритетов, принятых в GSM. В этой связи в каждой системе связи, использующей стандарт GSM, эти вопросы решаются самостоятельно.

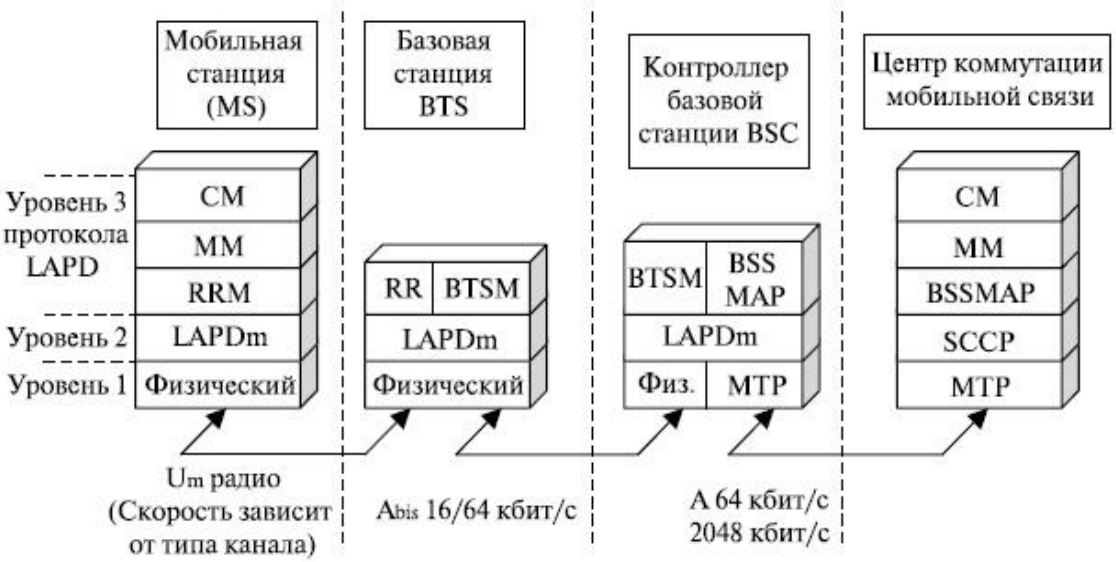
3.2. Протоколы сети GSM

Общая структура. Основное описание протоколов сети GSM дано в документах *ETSI*. Эти документы представляют некоторые группы, расположенные по версиям [12-16].

Рассмотренные ранее функции регистрации (registration), аутентификации (authentication), маршрутизации вызова (call routing) и обновление координат местоположения, механизм передачи соединения (handover) выполняются подсистемой сети главным образом с использованием протоколов системы мобильной связи, основанных на протоколах системы ОКС № 7 [17]. Структура этих протоколов показана на рисунке 3.3.

Сигнальный протокол в GSM разделен на три уровня [10,18] в зависимости от интерфейса, как показано на рисунке 3.3.

Участок "мобильная станция — базовая станция" работает со следующими уровнями. Уровень 1 — физический уровень, который использует структуры канала по воздушному интерфейсу. Уровень 2 — уровень звена передачи данных по U_m интерфейсу, уровень звена передачи данных — это модифицированная версия LAPD-протокола, используемого в ISDN; она называется LAPDm [15]. Уровень 3 — сигнальный протокол из GSM, использующий также модифицированную версию LAPD; самостоятельно разделен на 3 подслоя.



CM	Connection Management	Управление соединением
MM	Mobility Management	Управление передвижением
RRM	Radio Resources Management	Управление радио ресурсом
LAPD	Link Access Protocol D	Протокол доступа к звену передачи данных по каналу D
BTS M	Base Transceiver Station Message	Сообщение трансивера (приемопередатчика) базовой станции
BTSM	Base Transceiver Station Management	Управление Трансивером Базовой Станции
BSSMAP	BSS Application Part	Прикладная Система Управления Базовой Станцией
SCCP	Signaling Connection Control Part	Система управления соединением каналов сигнализации
MTP	Massage Transfer Part	Подсистема передачи сообщений

Рис. 3.3**.** Структура протоколов GSM

*Управление радиоресурсами (RRM — Radio Resources Management) у*правляет установкой, обслуживанием и конечным устройством, радио - и фиксированными каналами, включая хэндовер.

Управление передвижением (MM — Mobility Management) управляет обновлением местоположения и процедурами регистрации, так же как защитой и аутентификацией.

Управление соединением (Connection Management) обрабатывает общий процесс управления установлением соединения и сигнализацией и управляет дополнительными услугами, а также службой передачи коротких сообщений.

При взаимодействии базовой телефонной станцией (*BTS*) и контроллером базовой станции (*BSC*) используется интерфейсный протокол сообщение *трансивера* (приемопередатчика) базовой станции (BTSM — Base *Transceiver* Station Message). Он также называется интерфейс A_{bis}.

Передача сигналов между различными объектами в фиксированной части сети (интерфейс А) использует протоколы на уровне 1 MTP1 (Message Transfer Part — подсистема передачи сообщений) на уровне 1 и на уровне 2 — SCCP (Signaling Connection Control Part — система управления соединением каналов сигнализации) [13,16], принадлежащие системе сигнализации ОКС № 7. На уровне 3 применяют перечисленные выше протоколы GSM — MM и CM.

Подсистема 3 уровня BSSMAP прикладная система управления базовой станцией предназначена для связи контроллера базовой станции (*BSS*) с центром коммутации мобильной связи (MSC).

Подсистемы сигнальных протоколов. Для передачи сигнальных сообщений между центром коммутации мобильной связи (MSC) и системой базовой станции (*Base Station* System) [17,20] используются *MTP* (Message Transfer Part) и подсистемы управления соединением канала сигнализации SCCP (Signaling Connection Control Part), которые являются частями системы ОКС № 7. Рассмотрим кратко содержание этой подсистемы.

Основные сведения о подсистеме управления соединением канала сигнализации ОКС № 7 (SCCP-CSS№7). Система управления соединением канала сигнализации (SCCP — Signaling Connection Control Part) управляет *логическими соединениями* в сети ОКС для передачи блоков данных сигнализации. Она выполняет функции третьего уровня (сетевой уровень) модели взаимодействия протоколов ОКС [20]. SCCP предоставляет возможность осуществлять по сети ОКС передачу данных для управления соединением и при техническом обслуживании, непосредственно не связанную с конкретным каналом речи или передачи данных.

Подсистема SCCP предоставляет два класса услуг: ориентированных на соединение и не ориентированных на соединение.

В первом случае перед началом обмена данными устанавливается соединение. Доставка сообщений может быть гарантирована в порядке их передачи. Для ориентированных на соединение услуг различаются постоянные и кратковременные (*полупостоянные) соединения* для сигнализации. При этом для *полупостоянных соединений* предусмотрены три фазы: фаза установления соединения (примитив "N – соединение"), фаза обмена данными (примитив "N – данные") и фаза освобождение соединения (примитив "N – разъединение").

При реализации услуг, не ориентированных на соединение, SCCP обеспечивает передачу данных в двух режимах: с контролем последовательности доставки сообщений и без контроля. В последнем случае не гарантируется прием данных в порядке их передачи, так как они маршрутизируются в сети сигнализации по-разному и могут быть повторно запрошены при воздействии помех.

Структура сообщения SCCP детально рассмотрена в [13,16]. Ниже приведем только часть заголовков, посвященных подвижной системе.

Примеры типов сообщений для системы, ориентированной на соединение, следующие:

- запрос на соединение между двумя узлами (CR);
- подтверждение соединения (CC) в ответ на сообщение CR;
- запрос на разъединение (RLSD);
- подтверждение разъединения (RLC) со стороны любого из узлов;
- подтверждение разъединения (процесс освобождения завершен);
- данные для прозрачной передачи данных между двумя узлами (DT);
- разрешенная подсистема (*SSA*).

Последнее сообщение содержит следующие параметры (рис.3.4).

Номер задействованной подсистемы	1
Код задействованного пункта сигнализации	2
Код задействованного пункта сигнализации	3
Индикатор числа подсистем связанных с SCCP	4

Рис. 3.4**.** Сообщения "разрешенная подсистема"

Само сообщение "разрешенная подсистема" имеет код 0000 0001 Указанный на этом рисунке "номер задействованной подсистемы" может быть закодирован следующим образом.

В таблице 3.3. выделены "жирным" коды, относящиеся к передаче сигналов мобильных систем (не обязательно к системе GSM).

Таблица 3.3.

Таблица значения кодов "номер задействованной подсистемы в SCCP"

Код	**Задействованная подсистема**
0000	Подсистема неизвестна
0000	
0000	Техобслуживание SCCP
0001	
0000	Зарезервированная часть для ITU-T
0010	
0000	Подсистема пользователя ЦСИО (русская версия) ISUP-R
0011	
0000	Подсистема эксплуатации и технического обслуживания OMAP
0100	
0000	**Прикладная подсистема обслуживания мобильной связи MAP**
0101	
0000	**Домашний регистр местонахождения - HLR**
0110	
0000	**Визитный регистр местонахождения VLR**
0111	

0000 Центр коммутации подвижной связи MSC

1000

0000 Центр идентификации оборудования

1001

0000 Зарезервирован

1010

0000 Дополнительные услуги ISDN

1011

0000 Услуги коротких сообщений в мобильной связи

1100

0000 Услуги широкополосной B- ISDN

1101

0000 Тестирование возможностей транзакции (TCAP)

1110

0000 Коды зарезервированы для международного использования

1111

…….

0001

1111

0010 Коды зарезервированы для национальных сетей

0000

…….

1111

0111

1111 Центр коммутации подвижной связи NMT (подсистема пользователя

1000 мобильной связи)

1111 HLR-NMT (подсистема пользователя мобильной связи)

1001

1111 BSS (эксплуатация и техобслуживание базовых станций)

1001

1111 Прикладная часть системы базовой станции BSSAP

1110

1111 Код зарезервирован для расширения национального и международного

1111 номера подсистемы

Прикладная часть системы базовой станции BSSAP. Одна из пользовательских функций подсистемы управления соединением канала сигнализации SCCP (Signaling Connection Control Part) — прикладная часть системы базовой станции (BSSAP — *Base Station* System Part). Она предназначена для обслуживания взаимодействия *BSS* и MSC (рис.3.3). В случае соединения типа "точка — точка" BSSAP использует сигнальное соединение с активной мобильной станцией, имеющей один или более активизированных процессов для передачи сообщений уровня 3. В случае конференцсвязи или широковещательного вызова имеется всегда одно соединение в соте, связанное с данным вызовом, и одно дополнительное соединение в системе базовой станции (*BSS — Base Station* System) для передачи сообщений уровня 3. Есть дополнительное соединение для "главного абонента" при широковещательном вызове или конференц-связи. Дополнительные соединения могут также потребоваться для любых мобильных станций при конференцсвязи группы или широковещательном вызове, при которой сеть решает разместить выделенные или временно закрепленные каналы.

Пользовательские функции *BSS* (BSSAP — *Base Station* System Application Part) далее подразделены на две отдельных функции:

• прикладная часть для прямой передачи (DTAP — Direct Transfer Application Part), называемая также GSM L3, используется для передачи транзитных сообщений между MSC и MS. Информация уровня 3 в этих сообщениях не интерпретируется *BSS* (*Base Station* System);

• основная прикладная часть системы базовой станции (BSSMAP —*Base Station* System *Management Application* Part) поддерживает другие процедуры между MSC и *BSS* (*Base Station* System), связанные с MS управлением ресурсами, управлением передачей соединения (хэндовером), или в данной соте, или в пределах всей *BSS* (*Base Station* System). Описание протокола для обмена информацией BSSMAP (*Base Station Management Application* Part) на уровне 3 содержится в Рекомендации *ETSI* GSM 08.08 [13-16].

При применении BSSMAP (*Base Station Management Application* Part) используются процедуры без установления соединения и ориентированные на соединение. Rec. *ETSI* GSM 08.08 указывает для каждой процедуры уровня 3, должно ли использоваться соединение или нужно работать без установления соединения. Процедуры, ориентированные на соединение, задействуются, чтобы поддержать *DTP* (Direct Transfer Application Part). Функция распределения, размещенная в BSSAP, выполняет разделение между данными этих двух частей.

BSSAP сообщения включают следующие поля (рис. 3.5).

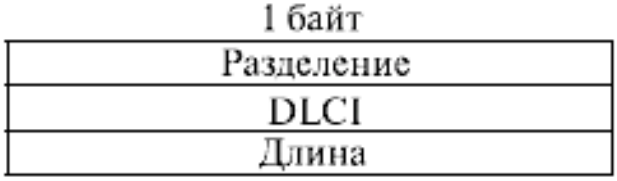


Рис. 3.5**.** Формат заголовка BSSAP

Длина - Параметр, указывающий последующую длину сообщения уровня 3.

Разделение (Discrimination). Разделяет сообщения, принадлежащие указанным выше двум протоколам: BSSMAP (*Base Station Management Application* Part) и DTAP (Direct Transfer Application Part).

Идентификатор управления звеном передачи данных (DLCI — Data Link Control Identifier). Применяется только для DTAP (Direct Transfer Application Part). Используется в MSC для передачи сообщений к *BSS* (*Base Station*

Subsystem), чтобы указать тип данных, исходящих первоначально от соединения по радиоинтерфейсу.

Прикладная система управления базовой станцией (BSS MAP) взаимодействует с обеими частями и SCCP (Signaling Connection Control Part), ориентированными на соединение и не ориентированными на соединение.

Прикладная система управления базовой станцией (BSSMAP) поддерживает все процедуры между MSC, и *BSS*, которые требуют интерпретации и обработки информации, связанной с обслуживанием отдельных вызовов, и управления ресурсами. Некоторые из процедур BSS MAP в конечном итоге вызываются сообщениями управления радиоресурсами (Radio Resource), определенными в *ETSI* [13-16].

Формат протокола BSS MAP (*Base Station Management Application* Part) следующий (рис. 3.6).

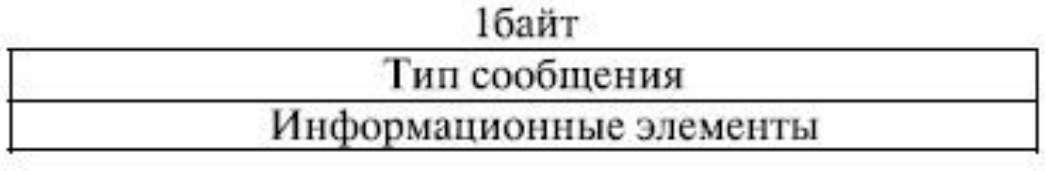


Рис. 3.6. Формат сообщений протокола BSSMAP

Тип сообщения. Поле из одного байта, определяющее тип сообщения. Это обязательное поле уникально определяет функцию и формат каждого сообщения BSMAP.

Информационный элемент. Каждый информационный элемент кодирован единственным кодом из восьми бит (идентификатором). Длина информационного элемента может быть фиксированная или переменная и может включать или не включать в себя индикатор длины.

Прикладная часть для прямой передачи (DTAP - Direct Transfer Application Part) применяется для передачи сообщений управления соединением и управления подвижностью между MS и MSC. Сообщения прямой передачи не обрабатываются в системе *BSS*, а только преобразуются

в соответствующие сигналы радиоинтерфейса и обратно. Для передачи сообщений DTAP используется следующий формат (рис. 3.7).

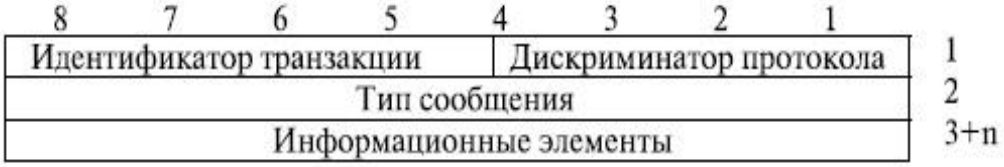


Рис. 3.7. Формат передачи сообщений DTAP

Формат идентификатора транзакции приведен на рис.3.8.

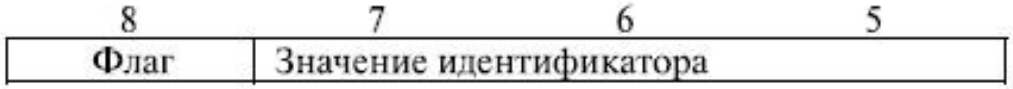


Рис. 3.8. Формат идентификатора транзакции

Флаг указывает, какой стороной назначена транзакция. Если MS, то флаг имеет значение 0, если MSC, то 1.

Значение *идентификатора транзакции* является целым числом и назначается инициатором. Оно уникально и на той стороне интерфейса, которая явилась инициатором этой связи, и не меняется в течение времени жизни транзакции, имеет смысл только в данном интерфейсе и остается в нем неизменной, после чего может использоваться вновь.

Поле *дискриминатор протокола* указывает тип подуровня (RR, CM, MM), к которому принадлежит сообщение.

Тип сообщения и *информационные элементы* приведены для каждого подуровня (RR, CM, MM) ниже.

Сигнальные протоколы третьего уровня. *Управление Радио-ресурсами.* Уровень управления радиоресурсами (RRM — Radio Resource Management) наблюдает за установлением соединения по радио и фиксированной сети между подвижной станцией и центром коммутации подвижной связи (MSC). Главные функциональные компоненты этого уровня

— подвижная станция и подсистема базовых станций, центр коммутации подвижной связи (MSC). Уровень RRM предназначен для управления радиосеансом [10]. Сеанс — это время, которое мобильная станция находится в режиме соединения и управляет конфигурацией радиоканалов, включая распределение специализированных каналов.

Радиосеанс всегда инициализируется подвижной станцией с помощью процедуры доступа, либо для исходящего вызова, либо в ответ на широковещательный вызов при входящем вызове. Уже рассмотренные выше процедуры исходящего вызова и широковещательного вызова, такие как назначение выделенного канала для сигнализации мобильной станции, и структура широковещательного подканала, устанавливаются на уровне RRM. Кроме того, уровень RRM осуществляет управление радиохарактеристиками, такими как управление мощностью, прерывистая передача и прием.

Управление мобильностью. Уровень управления мобильностью (MM — Mobility Management) относится к верхнему уровню управления радиоресурсами (RRM — Radio *Resources Management*) и выполняет функции, которые возникают при передвижении абонента, а также функции защиты и аутентификации. Управление местоположением включает процедуры, которые дают системе информацию о текущем местоположении включенных передвижных станций так, чтобы управлять маршрутизацией входящих вызовов.

Управление соединением. Уровень управления соединением (CM) отвечает за управление вызовом, управление дополнительными видами услуг и управление службой передачи коротких сообщений. Каждое из них можно рассматривать как отдельный подслой в пределах уровня управления соединением (CM). Процедура управления вызовом почти совпадает с процедурами цифровой сети ISDN, указанными в Q.931, хотя маршрутизация к (от) подвижному объекту, очевидно, является в GSM уникальной. Другие функции подслоя управления вызовом включают: установление соединения,

выбор типа обслуживания (включая чередование услуг в течение вызова) и отбой.

Виды сообщений и составы сигналов 3-го уровня. Как уже упоминалось выше, система протоколов взаимодействия 3-го уровня на участке MS — *BTS* (CM, MM, RR) является подмножеством протокола 3-го уровня *LAPD*. Ниже приведены некоторые форматы и команды, касающиеся протоколов участка MS — *BTS* [10]. Содержание каждого сигнала понятно из его названия; для более детального рассмотрения этих сигналов можно рекомендовать [18,20].

Обмен сигнальной информацией по протоколу *LAPD* производится в виде сообщений, каждое из которых имеет следующий вид (рис. 3.9).

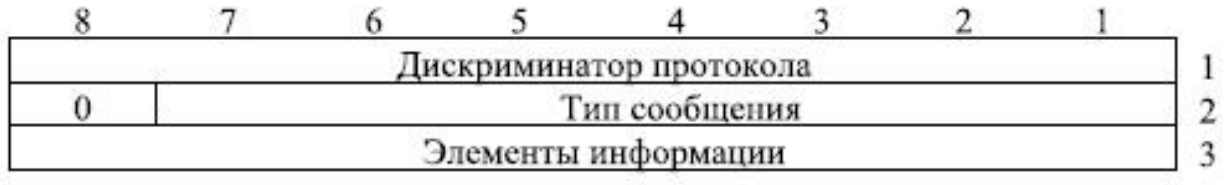


Рис. 3.9. Вид сообщения протоколов LAPD 3-его уровня

Сообщение содержит следующие области: дискриминатор протокола, метка соединения и тип сообщения.

Дискриминатор протокола служит для того, чтобы отделить процедуры управления вызовом от любых других сообщений, а также отделить сообщения, передаваемые в ЦСИО (ISDN), от сообщений других систем, в частности, GSM.

Дискриминатор протокола кодируется в соответствии со следующей таблице 3.4 [10].

Из других полей формата сообщений уровня 3 в протоколах GSM используется поле "Тип сообщения". В таблицах 3.5-3.7 приведены значения, которые применяются на уровнях CM, MM, RR. Заглавные буквы в английском значении терминов обозначают буквы, входящие в сокращенное обозначение сообщений.

Таблица 3.4.

Кодировка дискриминатора протокола

Коды и порядок следования бит	**Дискриминатор протокола**
8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	Сообщения по протоколу пользователь-пользователь
.....	
0 0 0 0 0 1 1 1	
0 0 0 0 1 0 0 0	Сообщения управления вызовом по Рекомендации I.451
.....	(включая сообщения CM, отмеченное жирным
0 0 1 1 0 0 0 0	шрифтом)
.....	
0 0 1 1 1 1 1 1	
0 1 0 1 0 0 0 0	Сообщения MM
.....	
0 1 1 0 0 0 0 0	Сообщения RRM
.....	
0 1 1 1 0 0 0 0	Сообщения CM
.....	
0 0 1 0 0 0 0 0	
.....	
0 0 1 1 1 1 1 1	
0 1 0 1 0 0 0 0	Для национального использования
.....	
0 1 0 0 1 1 1 1	
0 1 0 1 0 0 0 0	Резерв для других сетевых протоколов 3-го уровня
1 1 1 1 1 1 1 1	

Таблица 3.5.

Типы сообщений 3-го уровня протокола СМ на участке MS —*BTS*

(Дискриминатор протокола — значение 01110000)

x000	0x000	Переход к национальным типам сообщений
x000	xxxx	**Сообщения организации соединения**
	0001	Оповещение (ALERting)
	1000	Вызов завершен (CALL COMplete)
	0010	Вызов обслуживается (CALL PROCeeding)
	0111	Соединить (CONnect)
	1111	Подтверждение соединения (CONnect *ACKnowledge*)
	1110	Аварийный вызов (*EMERGence* SETUP)
	0011	Вызов (SETUP)
X001	xxxx	**Сообщения информационной фазы соединений**
	0111	Модификация (MODify)
	1111	Модификация закончена (MODify COMplete)
	0011	Отказ в модификации (MODify *REJect*)
	0000	Информация пользователя (USER INFormation)
	1000	Удержание (HOLD)
	1001	Подтверждение удержания (HOLD *ACKnowledge*)
	1010	Отказ от удержания (HOLD *REJect*)
	1100	Возобновление (*RETRieve*)
	1101	Подтверждение возобновления (*RETRieve ACKnowledge*)
	1110	Отказ от возобновления (*RETRieve REJect*)
X010	xxxx	**Сообщения разъединения**
	0101	Разъединение (DISConnect)
	1100	Освобождение (RELease)
	1101	Освобождение закончено (RELease COMplete)
X011	xxxx	**Прочие сообщения**
	1001	Управление перегрузкой (*CONGestion* Control)
	1100	Извещение (NOTIFY)

1101 Статус (STATUS)

0010 Запрос статуса (STATUS *ENQuiry*)

0101 Начало частотного набора (START *DTMF*)

0001 Остановка частотного набора (STOP *DTMF*)

0010 Подтверждение остановки частотного набора

0110 Подтверждение начала частотного набора (STOP *DTMF ACKnowledge*)

1110 Отмена начала частотного набора (START *DTMF ACKnowledge*)

1010 Обращение к дополнительным услугам (FACILITY)

Таблица 3.6.

Типы сообщений 3-го уровня протокола ММ на участке MS —*BTS*

(Дискриминатор протокола — значение 01010000)

x000 xxxx **Регистрационные сообщения**

0001 Выделен индикатор *IMSI* (*IMSI* DETuch INDicator)

0010 Изменение местоположения принято (LOCation UPDate ACcept)

0100 Изменение местоположения отклонено (LOCation UPDate *REJect*)

1000 Запрос на изменение местоположения (LOCation UPDate REQuest)

x000 xxxx **Сообщения аутентификации и определения подлинности оборудования**

0001 Аутентификация отклонена (AUTHentication *REJect*)

0010 Запрос на аутентификацию (AUTHentication REQuest)

0100 Ответ на аутентификацию (AUTHentication RESponse)

1000 Запрос на идентификацию (IDENtification REQuest)

1001 Ответ на идентификацию (IDENtification RESponse)

1010 Команда на изменение TSMI (TSMI *REALlOCation* CoMmanD)

1011 Изменение TSMI закончено (TSMI *REALlOCation* COMplete)

x010 xxxx **Сообщения управления соединением**

0001 Услуги СМ приняты (CM SERVice ACCept)

0010 Услуги СМ отклонены (CM SERVice REJ ect)

0011 Услуги СМ прерваны (CM SERVice ABORT)

0100 Запрос услуг СМ (СМ *SERVice REQuest*)

1000 Изменение услуг СМ (CM SERVice REESTABlishment)

1001 Прерывание (ABORT)

x011 xxxx **Различные сигналы**

0100 Состояние ММ (MM STATUS)

Таблица 3.7

Типы сообщений 3-го уровня протокола RRM на участке MS —*BTS*

(Дискриминатор протокола — значение 01100000)

x0111 xxx **Сообщения организации каналов**

011 Дополнительное распределение (ADDitional ASSignment)

111 Непосредственное распределение (IMMdiate ASSignment)

001 Непосредственное расширенное распределение (IMMdiate ASSignment EXTended)

010 Непосредственное распределение отклонено (IMMdiate ASSignment *REJect*)

x0110 xxxx **Сообщения о шифровании**

101 Команда режима шифрования (Ciphering MODE CoMmanD)

010 Режим шифрования закончен (Ciphering MODE COMplete)

x0101 xxxx **Сообщения передачи**

110 Команда распределения (ASSignment CoMmanD)

001 Распределение закончено (ASSignment COMplete)

111 Ошибка распределения (ASSignment FAILure)

011 Команда хэндовера (HANDover CoMmanD)

100 Хэндовер закончен (HANDover COMplete)

000 Ошибка хэндовера (HANDover FAILure)

101 Физическая информация (PHYSical INFormation)

x0001 xxx **Сообщения освобождения каналов**

101 Освобождение канала (CHANnel RELease)

010 Частичное освобождение (PARTial RELease)

111 Частичное освобождение закончено (PARTial RELease COMplete)

x0100 xxx **Широковещательные сообщения**

001 Запрос типа 1 (PAGING REQuest 1)

010 Запрос типа 2 (PAGING REQuest 2)

100 Запрос типа 3 (PAGING REQuest 3)

111 Ответ на сообщения (PAGing RESpons 1)

x0011 xxx **Системные сообщения**

x0000 xxx **Системные информационные сообщения**

x00010 xxx **Различные сообщения**

000 Модификация режима канала (CHANnel MODE MODify)

010 Статус RR (RR STATUS)

111 Подтверждение модификации режима канала (CHANnel MODE MODify *ACKnowledge*)

100 Перераспределение частот (FREQuency *REDEFinition*)

101 Отчет об измерении (MEASurement REPort)

110 Изменение набора услуг (CLASSMARK CHANGE)

011 Запрос набора услуг (CLASSMARK *ENQuiry*)

BTSM представляет протокол взаимодействия *BSC — BTS* (*Base Station* Controller — Base *Transceiver* Station) или интерфейс A_{bis}. Сообщения передаются в формате *LAPD*, поле "тип сообщения" состоит при этом из двух байт (используется бит расширения). В первом байте передается дискриминатор сообщения, во втором — тип сообщения.

Дискриминатор протокола. Используется один из кодов таблице 3.4 в разделе сообщения управления вызовом (0011xxxx).

Дискриминатор сообщений. Однобайтовое поле, указывающее на тип обработки поступающих сообщений.

- *Transparent — прозрачный режим*: в этом случае сообщение пропускается транзитом без обработки и добавления информации;
- *Non transparent* — режим, обратный указанному выше;
- *Radio Link Layer Management* — сигналы управления радиосвязью;
- *Dedicated Channel Management* — управление выделенным каналом;
- *Common Channel Management* — управление общим каналом;
- *TRX Management* — управление приемопередатчиком.

Первый бит применяется для указания прозрачности (transparent). Для указания типа обработки используются 7 последних битов октета.

Таблица 3.8.

Дискриминатор сообщений 3-го уровня протокола
ВТМ на участке *BSC — BTS*

00000 000	Зарезервировано
00000 001	сигналы управления радиоканалом
00000 100	управление выделенным каналом
00000 110	управление общим каналом
00000 100	управление приемопередатчиком

Тип сообщения. Представляет однобайтное сообщение, старший бит которого отведен для возможности расширения сообщения, а остальные предназначены для кодирования типа сообщений, *отображающего функции* этого сообщения. Коды типа сообщений приведены в таблице 3.9.

Применение, рассматриваемых команд, легко устанавливается из их названия, поэтому, не останавливаясь на описании, приведем пример их использования при установлении соединения от станции ISDN к мобильной станции.

Таблица 3.9

Коды типа сообщений BSTM

0001xxxx	**Управление радиоканалом**	
0001	DATE REQuest	Запрос данных
0010	DATE INDication	Индикация данных
0011	EROR INDication	Ошибка индикации
0100	ESTablish REQuest	Запрос на установление соединения
0101	ESTablish CONfirm	Установление соединения закончено
0110	ESTablish INDication	Индикация установления соединения
0111	RF CHANnel RELease REQuest	Запрос на освобождение *радиоканала*
1000	RF CHANnel RELease CONfirm	Освобождение *радиоканала* закончено
1001	RELease INDication	Индикация освобождения
1010	UNIT DATA REQuest	Запрос блока данных
1011	UNIT DATA INDication	Индикация блока данных
0110 xxxx	**Сообщение управления общими каналами и приемопередатчиком**	
0001	BSSCH INFOrmation	Информация BSSCH
0010	CCCH Load INDication	Загрузка индикации CCCH
0011	CHANNel ReQuireD	Запрошен канал
0100	DELETE INDication	Удаление индикации
0101	PAGGING CoManD	Широковещательная команда
0110	IMMidaite ASSignee CoMmanD	Команда срочного назначения
0111	SMS Broadcast REQuest	Команда широковещательного SMS
1000	Зарезервировано	
1001	RF ReSourse INDication	Индикация ресурса радио частот
1010	SACCH FILing	Заполнение SACCH
1011	*OVERLOAD*	Перезагрузка

1100	EROR REPORT	Отчет об ошибках
1101	SMS Broadcast CoManD	Команда широковещательного SMS
1110	*BCCH* LOAD INDication	Загрузка индикации BSCCH
1111	NOTification CoManD	Команда извещения

100xxxxx **Сообщения управления выделенным каналами**

00001	CHANnel ACTivation	Активизация канала
00010	CHANnel ACTivation *ACKnowledge*	Подтверждение активизации канала
00011	CHANnel ACTivation Negative *Acknowledge*	Отрицательное подтверждение активизации канала
01000	CONNection FAILure	Ошибка подключения
00101	DEACTivation SACCH	Деактивизация SACCH
00110	ENCRyption CoMmanD	Команда шифрования
00111	HANDover DETECTion	Определение хэндовера
01000	MEASurement RESult	Результат измерений
01001	MODE MODify REQuest	Запрос режима модификации
01010	MODE MODify *ACKnowledge*	Подтверждение режима модификации

Этот пример был предварительно рассмотрен для участка MS — *BTS* (рис. 3.11).

В данном случае приведены конкретные команды и сигналы на других участках. На рисунке 3.10. сообщения на участке MS — *BTS* полностью совпадают с указанными на рисунке 3.11, но в начале каждой команды указан уровень протокола, которому принадлежит сообщения (RR, MM, CM). По коду сигнала можно определить, к какому классу принадлежит сообщение (например, сообщения организации соединения, сообщения информационной фазы соединений, сообщения разъединения).

К этому рисунку дадим некоторые дополнительные комментарии. На рис.3.10. используются следующие команды системы ISDN:

- IAM (Initial address) — начальное сообщение;
- ACM (Addresscomplete) — абонент определен;
- *ANM* (Answer) — ответ абонента.

Команда SABM (Set Asynchronous Balanced Mode) — "установить сбалансированный асинхронный режим" — используется в протоколе *LAPD* для установления по сети режима, предшествующего входу в синхронизм, для передачи в этом режиме команд управления. При этом отсутствует механизм защиты от ошибок (сообщение не нумеровано). В диаграмме она используется, чтобы указать, что обмен идет в асинхронном режиме.

UA — Unnumbered *Acknowledge* — ненумерованное подтверждение, используется для подтверждения сигналов в асинхронном режиме.

На рисунке 3.10 отмечены символами:

* — фаза посылки вызова;

** — контроль посылки вызова;

*** — ответ абонента.

Следует также обратить внимание, что многие сигналы идут транзитом через *BTS* и *BSC*. Эти сигналы в дискриминаторе сообщений содержат тип обработки **Transparent — прозрачный режим.** На рисунке 3.11 показан обмен сигналами для случая "отбой от MS" и "без задержки повешена трубка".

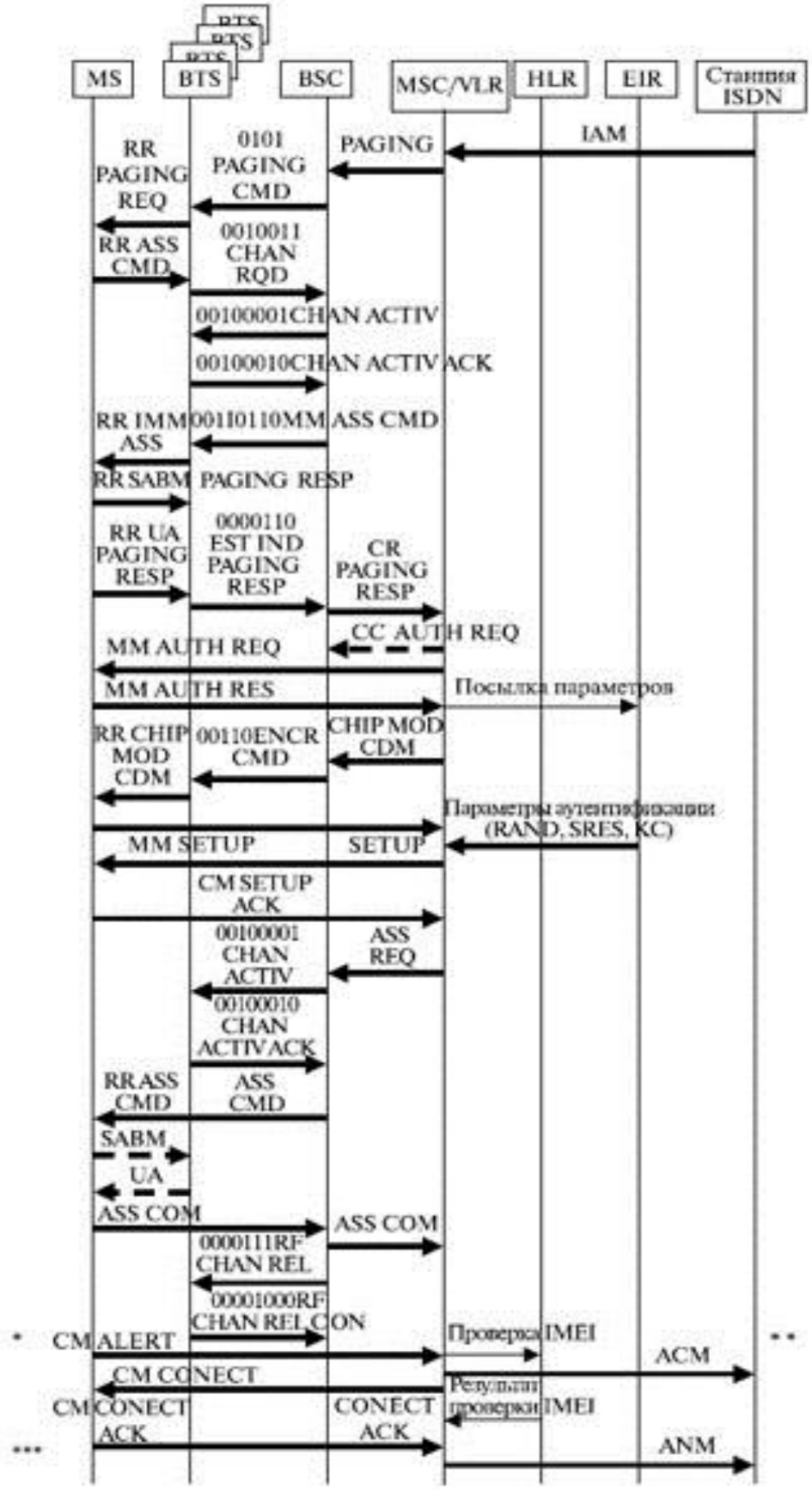


Рис. 3.10**.** Команды обмена при установлении связи. Станция ISDN-MS

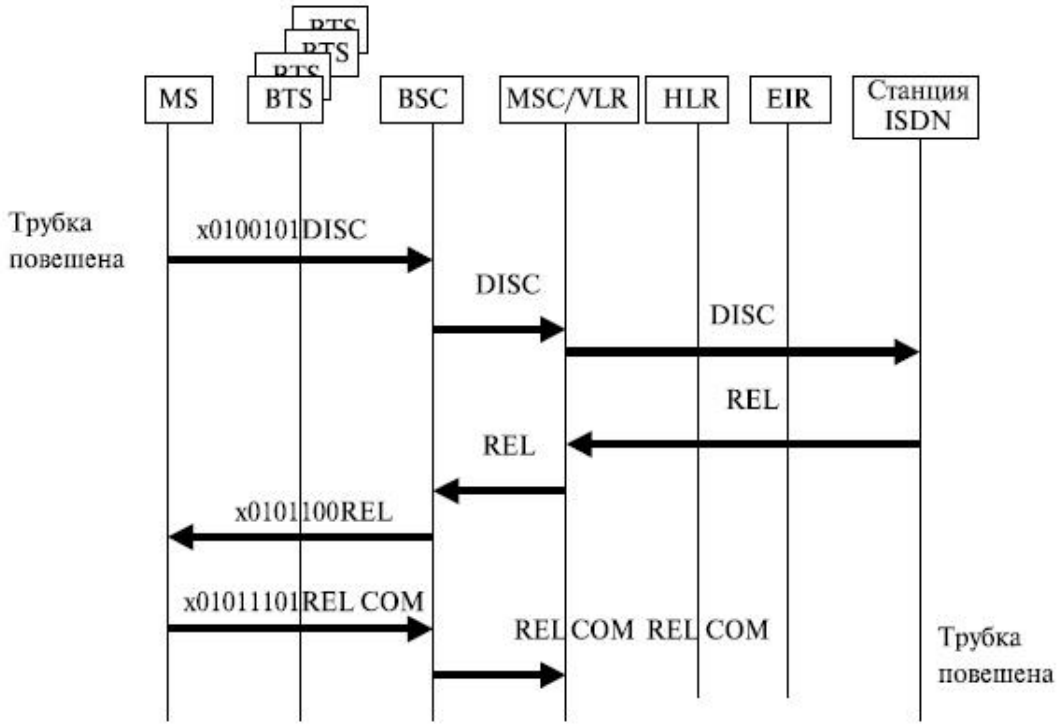


Рис. 3.11**.** Обмен сигналами при одном из вариантов отбоя

3.3. Частотный план и структура кадров в стандарте GSM

Частотный план в стандарте GSM. Принцип образования каналов в системе *GSM* [8,14], показан на рисунке 3.12.

Для радиодоступа *GSM* 900 выделены две полосы частот:

- 890–915 МГц для канала связи от абонента к станции (направление MS к BS);
- 935–960 МГц для исходящего канала от станции к абоненту (направления BS к MS).

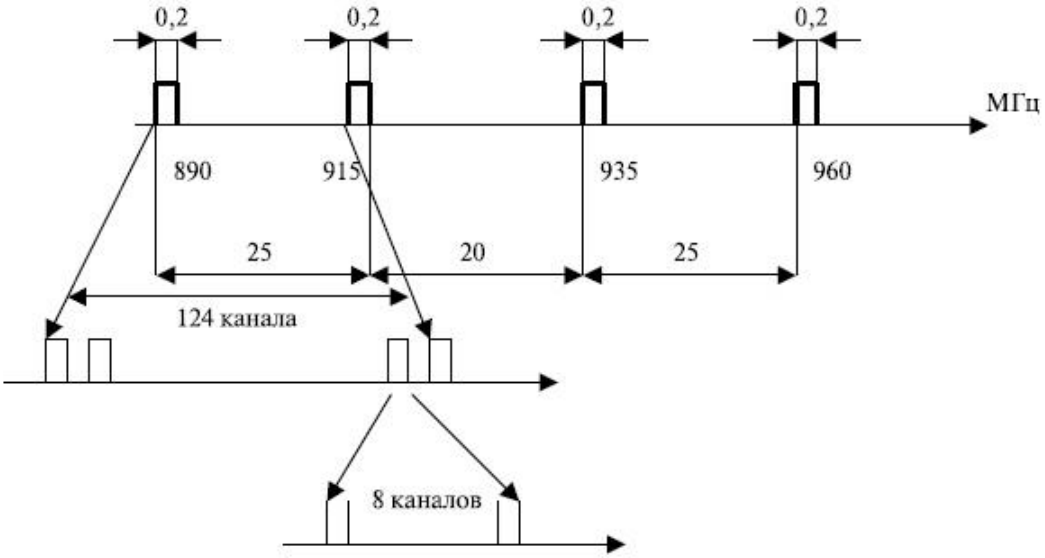


Рис. 3.12**.** Образование каналов в системе GSM

Полосы по 25 МГц разделены на 124 пары каналов, работающих в дуплексном режиме с интервалом несущей частоты по 200 кГц, используя многостанционный доступ с частотным разделением каналов (FDMA — Frequency Division Multiple Access). Каждый радиоканал с шириной полосы 200 кГц разделен на временные соты, которые создают 8 логических каналов. При этом используется методика, известная как многостанционный доступ с временным разделением (TDMA — Time Division Multiple ACCESS). Напомним: многостанционный доступ заключается в том, что группа пользователей имеет возможность использовать одну несущую частоту в разные моменты времени. Принцип доступа к этим каналам и разрешение ситуаций конкуренции за ресурс — различный.

Канал, переносящий информацию (канал трафика, или логический канал), определится номером несущей частоты и номером одного из 8 временных положений. Информация переносится в виде коротких пакетов (burst), объединенных в кадры.

Многостанционный доступ с временным разделением (TDMA), содержащий 8 слотов и 248 физических полудуплексных каналов, составляет группу из 1984 полудуплексных каналов. При размере кластера 7 число каналов в одной соте равно примерно 283 (1984 /7) полудуплексных каналов.

Как было показано ранее, разбиение, содержащее семь наборов частот, достаточно, чтобы охватить произвольно большую область, используя повторное применение частот с учетом допустимого расстояния между сотами.

Структура кадров и кадров управления в стандарте GSM. *Структура кадров трафика*. Каналы трафика (TCH) используются для доставки данных и речи. Структура образования кадров трафика (TCH) показана на рисунке 3.13 [5,11].

Мультикадр трафика содержит 26 кадров временного доступа (*TDMA*), каждый из которых состоит из 8 пакетов (burst) трафика. Длительность мультикадра трафика — 120 мс. Поэтому длительность кадров временного доступа 120 мс / 26 = 4,615 мс, а длительность временного положения (слота) трафика равна 120/(26 x 8)=15/26=0,577 мкс. Из 26 кадров 24 используются для трафика, один (12-й кадр) — как низкоскоростной выделенный канал управления (SACCH — *Slow* Associated Control Channel) и один (25-й) в настоящее время не используется.

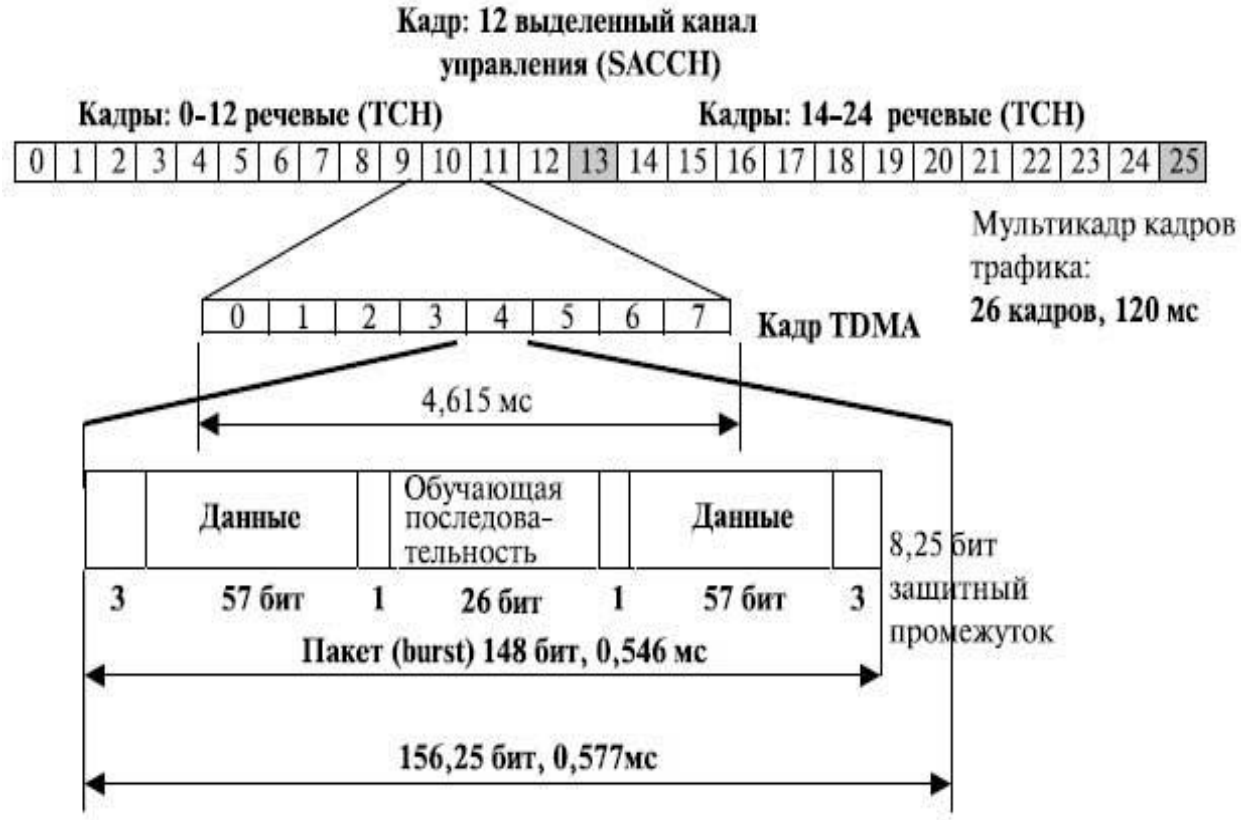


Рис. 3.13. Структура кадров трафика радио доступа системы GSM

Пакет содержит:

- два поля данных по 57 бит, т. е. в одном пакете содержится объем информации 114 бит;
- поле обучающей последовательности. Эта последовательность используется для оценки характеристик *радиоканала*. Она представляет собой набор заранее заданных знаков, по искажению которых определяют качество *радиоканала*;
- "хвостовые биты" (tail bits), располагающиеся по краям одного блока и указывающие его границы. Они защищают информацию при сдвиге слота;
- однобитовые поля — представляют собой флажки, которые указывают тип информации.

Пакет может использоваться как *для передачи трафика, так и для передачи кадров управления*. ТСН прямого и обратного направления разделены во времени на 3 периода передачи пакета. Поэтому мобильная станция не может одновременно получать и принимать один и тот же канал, что упрощает ее электронное устройство.

Данные передаются в пакетах, которые помещены в слоты. Общее число бит в мультикадре трафика равно 156,25 бит х 8 х 26 = 32500 бит. Эти биты передаются за 120 мсек. Поэтому скорость передачи информации в битах — 270,833 Кбит/с (32500/0,12=270,833 Кбит/с). Время передачи одного бита 3,69 мкс. Чтобы нейтрализовать влияние ошибок в настройке времени, дисперсию времени и т. д., пакет данных немного короче, чем временной интервал. Он составляет для одного пакета 148 бит из 156.25 битов, передаваемых в пределах слота.

В дополнение к каналам ТНС's с полной скоростью могут применяться каналы ТНС's с полускоростью. ТНС's с полускоростью фактически могут удвоить емкость системы, так как в них предусматривается кодирование речи в пределах 11,4 Кбит/с вместо 22,8 Кбит/с. Полускоростные ТНС's каналы также используются для передачи сигналов управления. В рекомендациях

они названы автономными специализированными каналами управления (SDCCH — *Stand*-alone *Dedicated* Control Channels) [9-12].

Если применяется полускоростное кодирование, то число слотов увеличивается до 16. При этом в четных кадрах мультикадра содержится информация 0–7-го слота, а в нечетных — 8–15-го.

Структура кадров управления. Структура кадров управления и мультикадров показана на рисунке 3.14. По сравнению с приведенными на рисунке 3.13 кадрами, мультикадр состоит из 51 кадра *TDMA*, каждый из которых содержит 8 слотов.

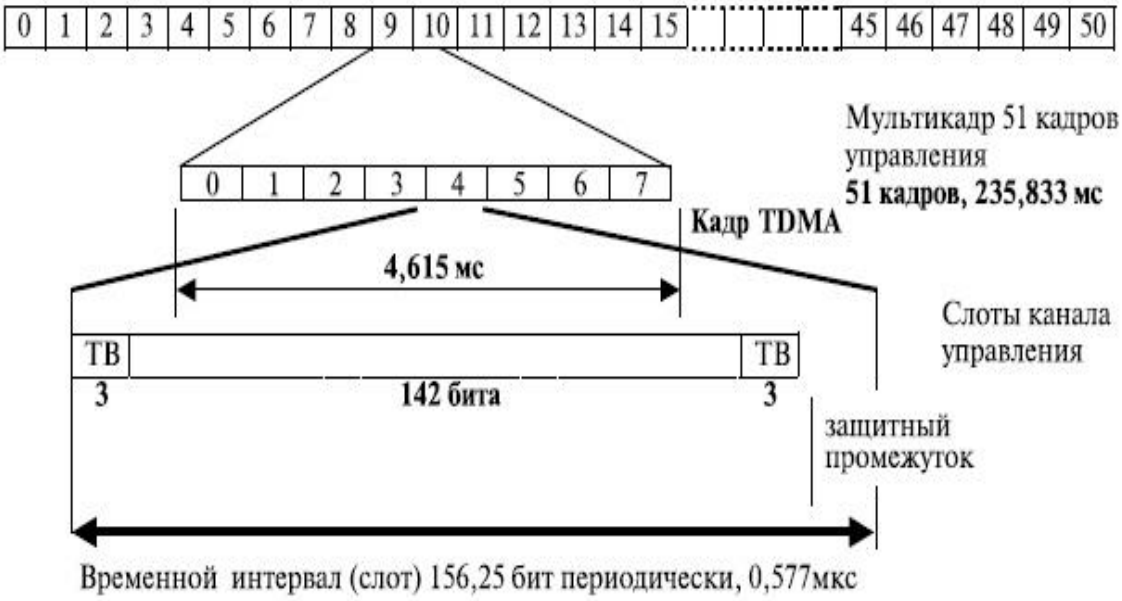


Рис. 3.14**.** Структура кадров управления

Содержания слотов управления и защитный интервал зависят от их назначения и указаны на рисунке 3.15.

Слот подстройки частоты (FB — Frequency correction Burst) предназначен для синхронизации частот мобильной станции. Для передачи этих слотов выделяется *канал подстройки частоты (FCCH — Frequency Correction Channel)*.

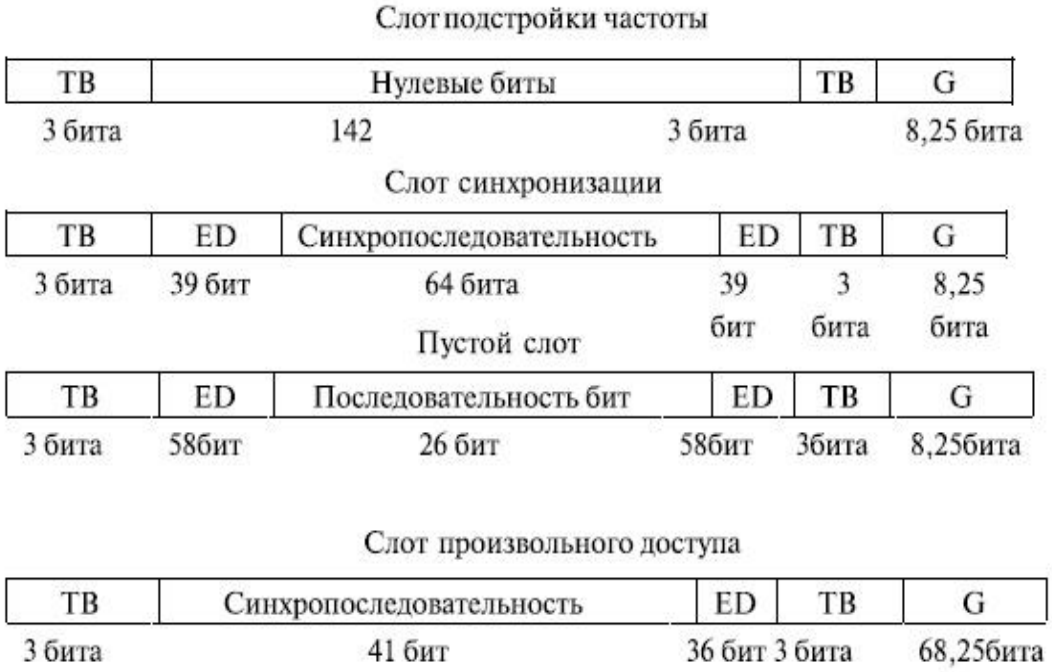


Рис. 3.15. Структуры слотов управления

Слот синхронизации (SB — Synchronization Burst) предназначен для синхронизации по времени базовой и мобильной станций. Слот содержит синхропоследовательность (64 бита), зашифрованную информацию о номере кадра *TDMA* и коде идентификации базовой станции два блока (по 39 бит каждый). Для передачи этих слотов выделяется отдельный *канал синхронизации (SCH — Synchronizing Channel).*

Пустой слот (DB — Dummy Burst) — этот вспомогательный пакет содержит два поля по 58 бит, не несущих информации. Такой пакет передается с целью оповещения о том, что станция находится в работоспособном состоянии.

Слот доступа (AB — Access Burst) предназначен для разрешения доступа MS к *BSS*, передается по *каналу права доступа (RACH — Random Access Channel)*. Этот слот передается в качестве первого запроса, когда станции еще не вошли в синхронный режим и неизвестно время прохождения сигнала. Он содержит концевую комбинацию (ТВ) — в данном случае она состоит из 3 бит; последовательность синхронизации для базовой станции — 41 бит, что позволяет базовой станции начать процесс

синхронизации и обеспечить правильный прием последующих 36 бит. Большой защитный интервал (68,25 бит длительностью 252 мкс) обеспечивает максимальное время для защиты кадров от эффекта межсимвольного искажения.

Все слоты имеют одинаковую длину 156,25 бит и длительность 235,833 мкс. Все слоты, кроме слота доступа, имеют концевые биты (TB — Tail Bit) по 3 бита каждый, и защитный интервал 8,25 бит.

На рисунке 3.16 показано объединение информации управления и трафика в единый поток.

Рис. 3.16. Объединение мультикадров трафика и управления в единый поток

Организация физических каналов. Для передачи быстродействующего объединенного канала управления (FACCH — Fast Associated Control Channel) и низкоскоростного выделенного канала управления (SACCH — *Slow* Associated Control Channel) применяются каналы трафика. Как уже было показано на 3.13, пакет трафика может использоваться и *для передачи трафика, и для передачи кадров управления*. Для этого применяются однобитовые флажки, которые указывают тип информации?

Из 26 кадров 24 используются для трафика, один (12-й кадр) — как низкоскоростной выделенный канал управления (SACCH — *Slow* Associated Control Channel). Один (25-й) в настоящее время не задействован, но при полускоростном режиме он может использоваться для организации второго канала SACCH. Для передачи в 12-м кадре может работать 8 слотов.

Поскольку один канал SACCH при полноскоростном режиме занимает один слот с информационным полем 114 бит (см.3.13), а время передачи 0,12 с, то скорость передачи по этому каналу 114/0,12=950 бит/с.

Слоты канала FACCH передаются со скоростью слота трафика. Остальные каналы управления передаются в мультикадре управления (рис. 3.14), содержащем 51 кадр. Организация каналов [21] управления в таком мультикадре показана на рисунке 3.17.

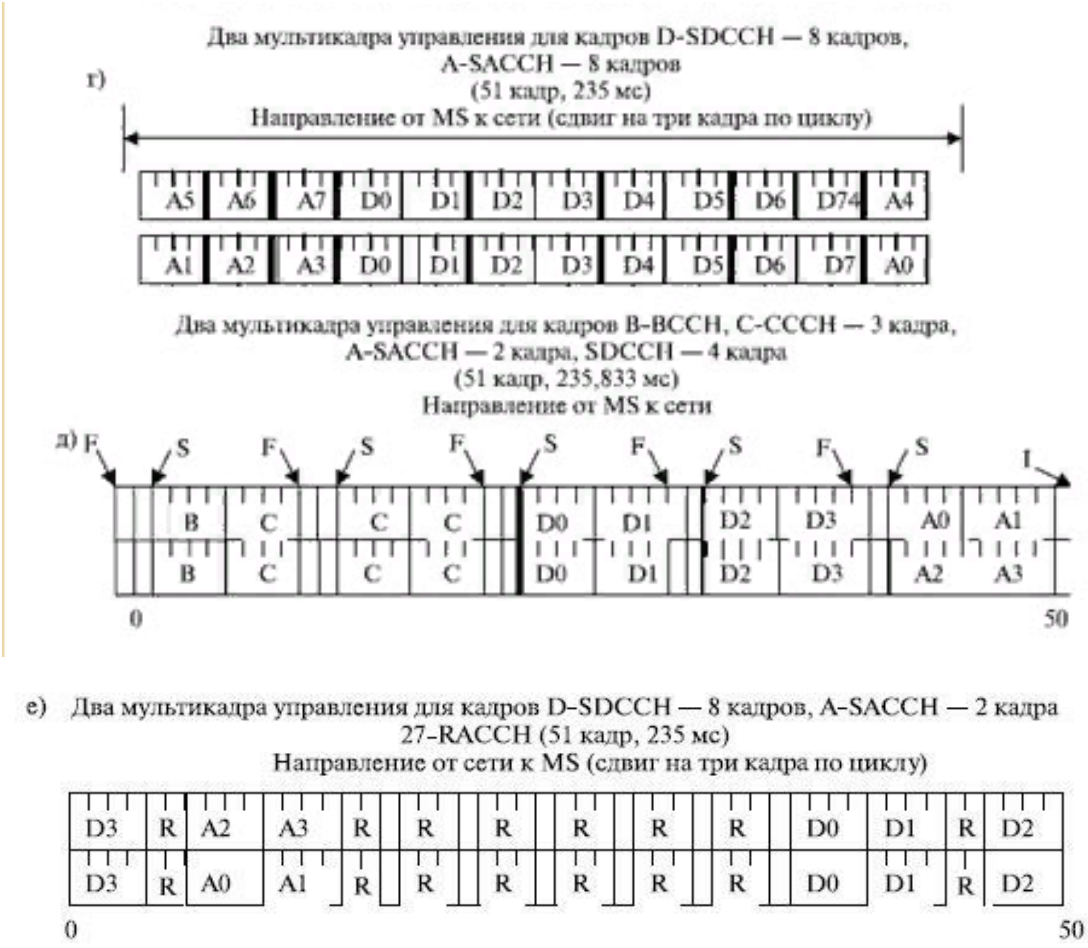


Рис. 3.17**.** Организация мультикадра управления

Каналы *BCCH*/CCCH могут использоваться всеми абонентами, находящимися в данной соте.

При передаче в направлении от сети к MS весь мультикадр разбивается на 5 групп по 10 кадров в каждой. Каждая группа начинается кадром канала FCCH, за которым следует SCH. Остальные 8 кадров разделяются на два блока по 4 кадра. Первая группа перового блока предназначена для передачи канала *BCCH*. Второй блок этой группы и остальные 8 блоков (всего 9 блоков), принадлежащие другим группам, предназначены для передачи кадров класса общего каналов управления — CCCH, а именно, входящих в него PCH и AGCH. Эти блоки называются блоками передачи каналов вызова. Таким образом, в рассматриваемом случае используются 4 кадра для передачи *BCCH*, 5 кадров для передачи FCCH, 5 кадров для SCH и 36 кадров (9 блоков вызова) для AGCH либо PCH.

Линия от MS к сети используется только для передачи кадров канала RACH.

В таблице 3.10 сведены итоговые сведения по организации логических каналов.

Таблица 3.10

Организация каналов управления

Канал управления CCH	Широковещательные каналы управления	FCCH	от сети к MS	Каналы настройки несущей частоты	Передается в речевом канале
		SCH	от сети к MS	Каналы временной синхронизации	
		BCCH	от сети к MS	Широкополосный канал управления	Передается в мултикадре канале
	Общие каналы управления CCOH	PCH	от сети к MS	Канал вызова	
		AGCH	от сети к MS	Канал представления доступа	
		RACH	от сети к MS	Канал с произвольным доступом	Передается в мультикадре управления
	Специализированные каналы управления DCCH	SDCCH/4	дуплекс	Автономный специализированный канал управления на 4 подканала	Передается в мультикадре управления
		SDCCH/4	дуплекс	Автономный специализированный канал управления на 4 подканалов	
		FACCH	дуплекс	Быстродействующий объединенный канал управления	
		SACCH	дуплекс	Низкоскоростной выделенный канал управления	

Примечание. Форматы, приведенные на рисунке 3.10д и рисунке 3.10е, применяются в случае небольшой загрузки каналов управления и не указаны в таблице 3.10.

Контрольные вопросы

1. Назначение SIM-карты и какая информация хранится в ней?
2. Дайте общее описание характеристик безопасности стандарта GSM.
3. Сколько классические алгоритмы используют ключей для шифрования-дешифрования?
4. Какие используются механизмы аутентификации в стандарте GSM?
5. Как обеспечивается секретность передачи данных в стандарте GSM?
6. Назначение числовой последовательности ключа шифрования.
7. Как устанавливается режим шифрования в стандарте GSM?
8. Как обеспечивается секретности в процедуре корректировки местоположения в стандарте GSM?
9. Какой общий состав секретной информации и как он распределяется в аппаратных средствах GSM.
10. Как обеспечивается секретность при обмене сообщениями между HLR, VLR и MSC.
11. Поясните общую структуру протоколов GSM.
12. Поясните, что входит в подсистему сигнальных протоколов GSM.
13. Перечислите основные сведения о подсистеме управления соединением канала сигнализации ОКС № 7 (SCCP-CSS№7).
14. Поясните состав подсистемы SCCP.
15. Какие параметры входят в «разрешенная подсистема (*SSA*)»?
16. Назначение прикладной части системы базовой станции BSSAP.
17. Как подразделяются пользовательские функции *BSS* (BSSAP)?
18. Назначение прикладной часть системы базовой станции (BSSMAP).
19. Какие процедуры используются при применении BSSMAP?
20. Какие поля включает BSSAP сообщения?
21. Приведите и поясните формат протокола BSSMAP.
22. Для каких целей применяется прикладная часть для прямой передачи DTAP.

23. Приведите и поясните формат передачи сообщений DTAP.
24. Приведите и поясните формат идентификатора транзакции.
25. Назначение сигнальных протоколов третьего уровня.
26. К какому уровню управления радиоресурсами (RRM) относится управления мобильностью (MM)?
27. Из каких сообщений состоят протоколы LAPD 3-его уровня?
28. Назначение протокола BTSM.
29. Поясните, как организуется частотный план в стандарте GSM?
30. Поясните структуру кадров трафика радио доступа системы GSM.
31. Поясните структуру кадров управления в стандарте GSM.
32. Поясните структуру и состав слотов управления.
33. Как объединяется информация управления и трафика в единый поток?
34. Как организуются физические каналы в стандарте GSM?
35. Как организуются каналы в мультикадре управления F-FCCH,B-BCCH, C-CCCH в направлении от MS к сети?
36. Как организуются каналы в мультикадре управления RACH в направлении от сети к MS?

ГЛАВА 4. ОБРАБОТКА РЕЧИ В СТАНДАРТЕ GSM

4.1. Процессы обработки речи в стандарте GSM

Процессы обработки речи в стандарте GSM направлены на обеспечение высокого качества передаваемых сообщений, реализацию дополнительных сервисных возможностей и повышение потребительских качеств абонентских терминалов [5,21].

Обработка речи осуществляется в рамках принятой системы прерывистой передачи речи (DTX), которая обеспечивает включение передатчика только тогда, когда пользователь начинает разговор и отключает его в паузах и в конце разговора. DTX управляется детектором активности речи (VAD), который обеспечивает обнаружение и выделение интервалов передачи речи с шумом и шума без речи даже в тех случаях, когда уровень шума соизмерим с уровнем речи. В состав системы прерывистой передачи речи входит также устройство формирования комфортного шума, который включается и прослушивается в паузах речи, когда передатчик отключен. Экспериментально показано, что отключение фонового шума на выходе приемника в паузах при отключении передатчика раздражает абонента и снижает разборчивость речи, поэтому применение комфортного шума в паузах считается необходимым. DTX процесс в приемнике включает также интерполяцию фрагментов речи, потерянных из-за ошибок в канале.

Качество воспроизведения, как показывает практика, существенно зависит от скорости кодирования речи (рис. 4.1).

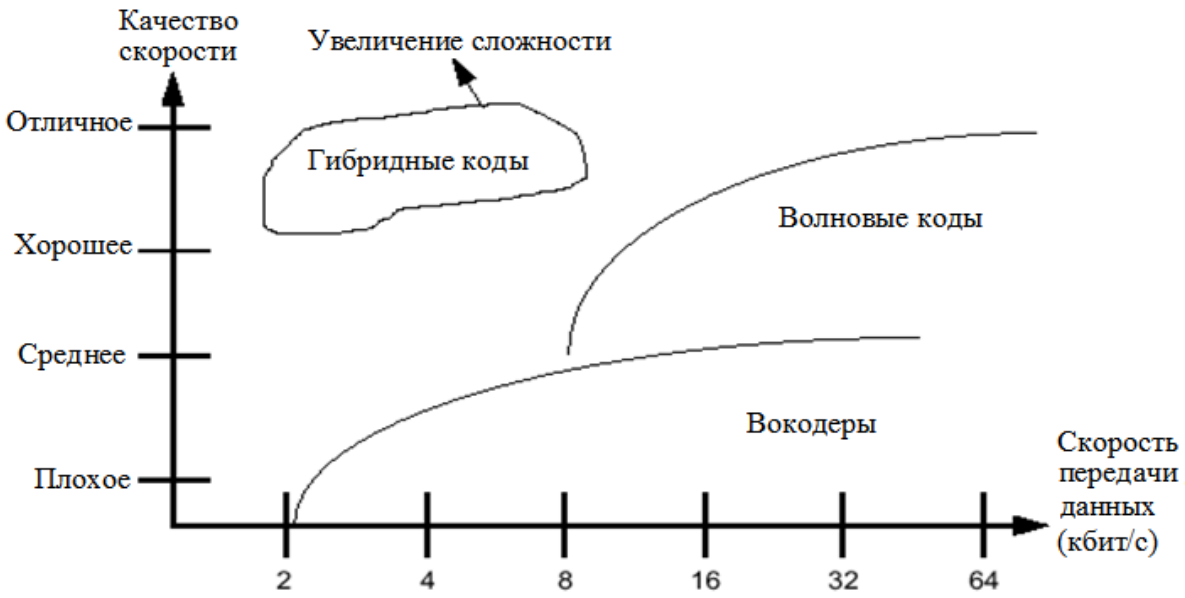


Рис. 4.1. Зависимость качества речи от скорости кодирования

Основным методом уменьшения скорости битового потока, представляющего собой закодированную речь, является передача информации о речи, а не самой речи, то есть в системе GSM непосредственно речевые сигналы не передаются. Вместо речи предаются параметры речи: тон (частота речевого сигнала), продолжительность конкретного тона, высота звука (уровень речевого сигнала). Параметры речи после их генерации передаются через сеть к другой MS, которая воспроизводит речь по полученным параметрам речи.

Процесс сегментации и речевого кодирования осуществляется в следующей последовательности. Воспроизведение человеческой речи начинается с вокального аккорда, производимого генерирующим тональные сигналы речевым органом. Такие речевые органы как рот, язык, зубы и т.д. работают как фильтр, изменяя природу данного тона. Цель речевого кодирования в системе GSM заключается в передачи только информации об оригинальном тоне и о фильтрах.

Поскольку речевые органы являются достаточно инерционными, параметры фильтра, представляющего речевые органы, остаются постоянными в течение минимум 20 мсек. В связи с этим при речевом

кодировании в системе GSM используется блочное кодирование с длительностью каждого блока в 20 мсек (рис.4.2).

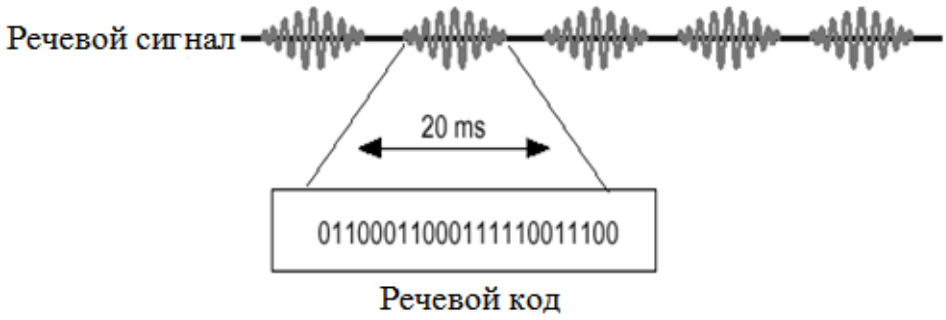


Рис. 4.2. Сегментация и речевое кодирование

Кодирование осуществляется одним набором битов. На самом деле данный процесс похож на оцифровку речи с частотой 50 раз в секунду вместо 8000, как это используется при стандартном аналого-цифровом преобразовании.

Речевое кодирование (Speech Coding). Вместо использования кодирования последовательностью из 13 битов, применяемого в аналого-цифровом преобразовании, в речевом кодировании используется кодирование последовательностью из 260 битов. Следовательно, общая скорость передачи информации о речи составляет 50*260 = 13 кбит/сек. Данное кодирование обеспечивает удовлетворительное качество речи, которое приемлемо в мобильной телефонии и сравнимо с качеством проводных линий сетей общего пользования PSTN.

В настоящее время существует множество различных речевых кодеров. Некоторые кодеры являются высококачественными с большей скоростью кодирования (waveform coders – кодирование формы сигнала). Некоторые кодеры обладают низким качеством, но обеспечивают меньшую скорость кодирования (vocoders). В системе GSM используются гибридные кодеры (Hybrid Coders), которые обеспечивают удовлетворительное качество речи при относительно малой скорости кодирования.

Речевой GSM кодер осуществляет кодирование со скоростью 13 кбит/сек для одного абонента. Следовательно, 8 абонентов при использовании одной несущей будут обслуживаться со скоростью 8*13 кбит/сек = 104 кбит/сек. Оптимальность такого метода кодирования особенно заметна при сравнении с кодированием при аналого-цифровом преобразовании со скоростью 832 кбит/сек.

Однако речевое кодирование не защищает передаваемую информацию от искажения и ошибок при её передаче через радиоэфир. Для защиты речи от этих негативных явлений используются другие методы:

- канальное кодирование;
- перемежение (интерливинг).

Канальное кодирование (Channel Coding). Канальное кодирование в системе GSM использует 260 бит, получаемых после речевого кодирования, как входную величину, и преобразует в последовательность, состоящую из 456 бит (рис.4.3) [19,21].

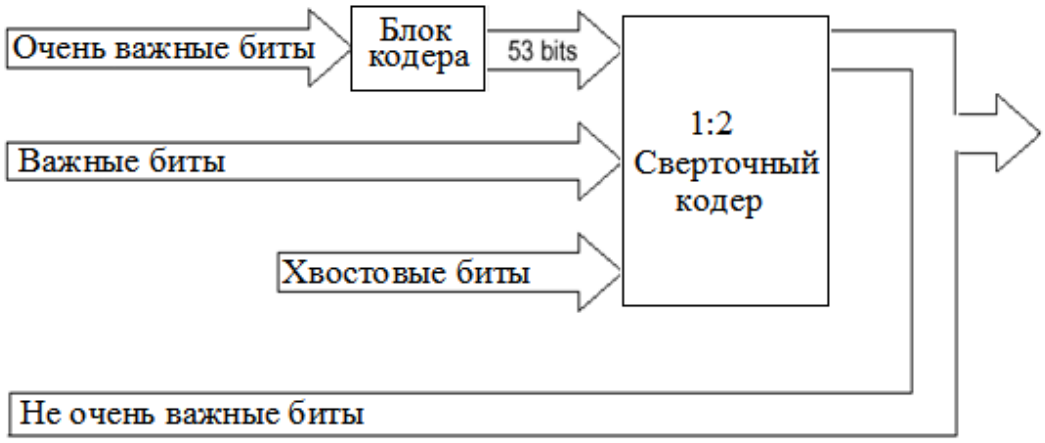


Рис. 4.3. Канальное кодирование

260 бит информации распределяются согласно их относительной важности:

- Блок 1: 50 бит – очень важные биты;
- Блок 2: 132 бит - важные биты;

- Блок 3: 78 бит – не очень важные биты.

Первый блок, состоящий из 50 бит, передаётся через кодер (устройство блочного кодирования), который добавляет ещё 3 бита для проверки четности, следовательно, получается последовательность из 53 битов. Эти 3 бита предназначаются для обнаружения ошибок в принимаемом сообщении.

После блочного кодирования 53 бита первого блока и 132 бита второго блока, плюс 4 хвостовых бита (в общем 189 бит) передаются в свёрточный кодер 1:2, на выходе которого получается 378 бит информации. Добавленные биты при свёрточном кодировании позволяют исправлять ошибки при приёме сообщений.

Остальные же биты третьего блока не защищены.

В результате на выходе кодера получаем следующие сигналы (рис.4.4).

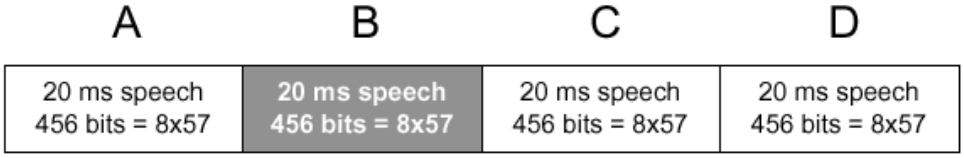


Рис. 4.4. Речевой кадр

Перемежение (Interleaving). *Первый уровень перемежения*[1,16]. Следует отметить, что канальный кодер осуществляет кодирование последовательностью из 456 битов для каждых 20 мсек. речи. После этого осуществляется интерливинг, в результате чего формируется 8 блоков по 57 бит каждый (рис. 4.5).

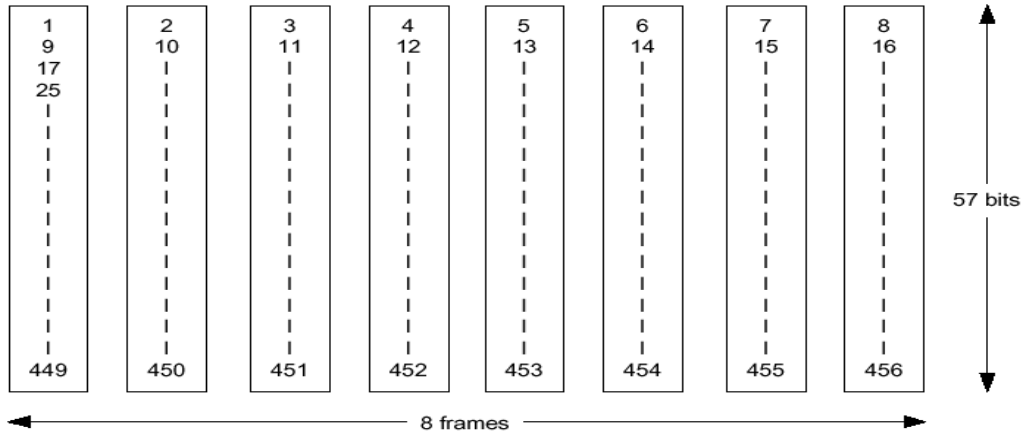


Рис. 4.5. Интерливинг кодированной речи в интервале 20 мсек

Как показано на рисунке 4.6 в обычном пакете (normal burst) есть пространство для двух таких речевых блоков (по 57 бит). Назначение остальных битов рассмотрим ниже. Таким образом, если один из этих блоков теряется, это будет соответствовать 25% BER внутри интервала речи продолжительностью 20 мсек. (2/8 = 25%).

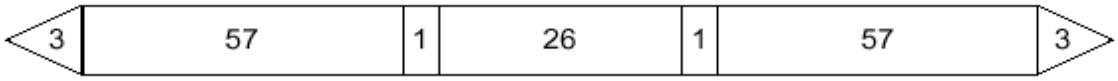


Рис. 4.6. Normal burst (обычный интервал)

*Второй уровень интерливинга***.** Как указывалось выше, при первом уровне интерливинга результирующие потери составляют 25%. Последнее слишком велико для осуществления корректировки в канальном кодере. Введение второго уровня интерливинга позволяет снизить BER до 12.5 % (рис. 4.7).

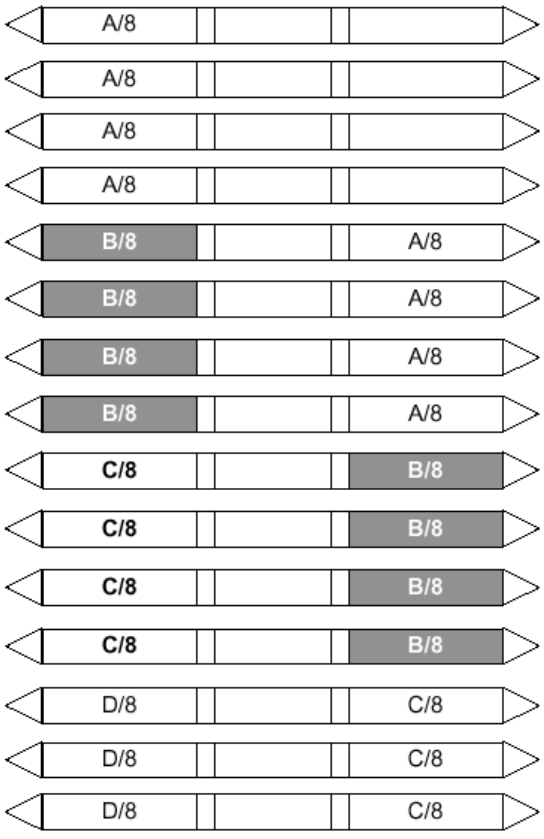


Рис. 4.7. Второй уровень интерливинга

Здесь, вместо передачи двух блоков по 57 бит речевого сообщения для интервала 20 мсек. внутри одного пакета, система передаёт один блок информации из одного 20 миллисекундного речевого сообщения и один блок информации из другого 20 миллисекундного речевого сообщения вместе. Такая одновременная передача организует в системе задержку в 20 мсек., вследствие чего MS должна ждать следующие 20 мсек. речи. Однако система при потере всего пакета (burst) теряет только 12.5% бит каждого временного кадра. Последнее хорошо исправляется канальным кодером.

Шифрование (Ciphering/Encryption). Цель шифрования заключается в зашифровке речевого пакета (burst) таким образом, чтобы никто другой не смог расшифровать данное сообщение при использовании различных внешних декодеров. Алгоритм шифрования в системе GSM называется алгоритмом A5 (рис. 4.8) [5,20].

При шифровании в передатчике информация из открытой (незашифрованной) преобразуется в закрытую (зашифрованную) по определенному алгоритму шифрования с применением секретного ключа, причем, чем больше размер секретного ключа в битах, тем труднее будет злоумышленнику взломать шифрованную посылку (расшифровать данные), перехваченную из канала передачи. Размер секретного ключа определяется алгоритмом шифрования, степенью защищенности и трудоемкостью процедуры шифрования. При условии, что на приеме известен алгоритм шифрования и секретный ключ, информация из закрытой преобразуется в открытую (дешифрируется).

В стандарте GSM 900 для реализации шифрования применяется схема шифрования A5, построенная на трех сдвиговых регистрах LFSR 1, LFSR 2 и LFSR 3 длиной по 19, 22 и 23 бита соответственно. Секретный ключ для схемы шифрования A5 составляет 64 бита.

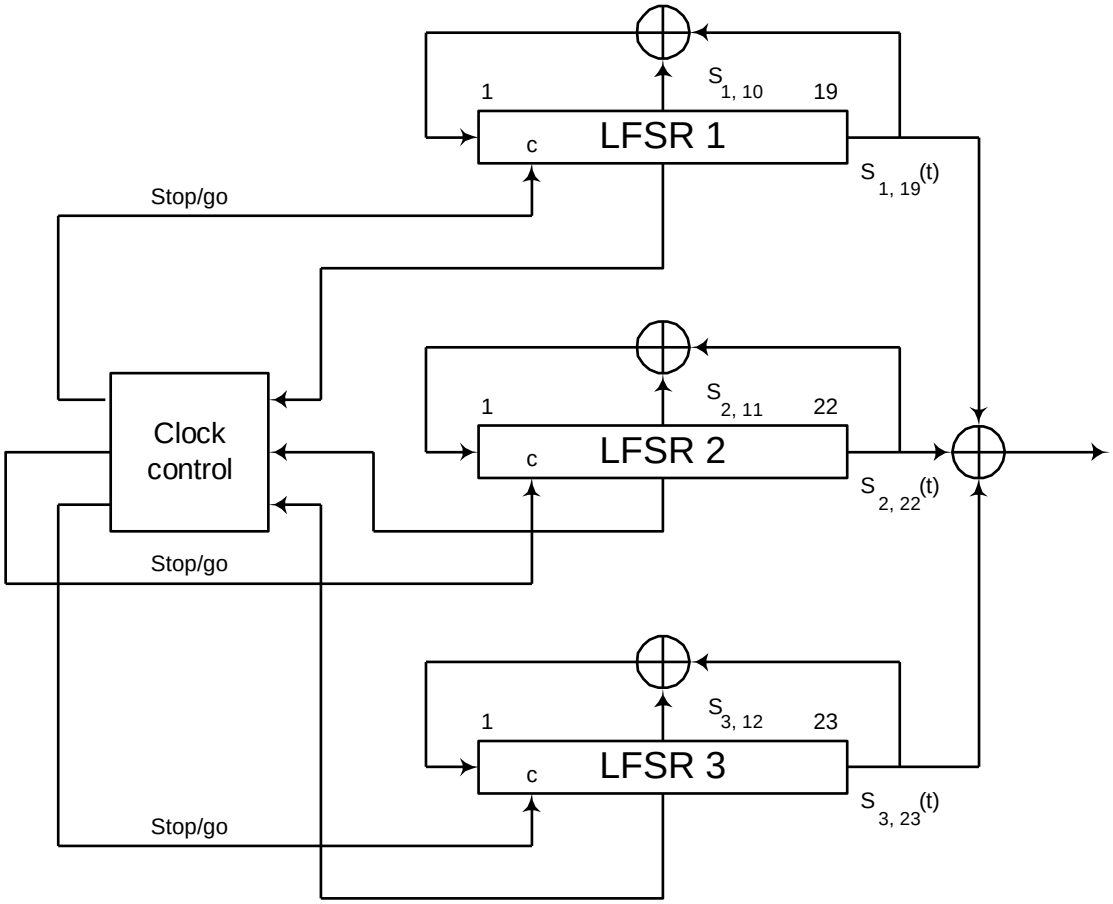


Рис. 4.8. Схема шифрования A5

Процесс шифрования происходит следующим образом:

1. Секретный ключ помещается в три сдвиговых регистра LFSR 1, LFSR 2 и LFSR 3 таким образом, что его старшие биты с 64 по 46 оказываются в регистре LFSR 1, биты с 45 по 24 - в регистре LFSR 2 и биты с 23 по 1- в регистре LFSR 3 соответственно.

2. По приходу синхроимпульса CLK от тактового генератора происходит следующее:

• Вычисляется выход логической схемы $Y(t) = (S_{1,19} + S_{2,22} + S_{3,23}) \bmod 2$ (сумма по модулю 2 битов 19, 22 и 23 сдвиговых регистра LFSR 1, LFSR 2 и LFSR 3 соответственно);

• из сдвиговых регистров считываются биты: $S_{1,10}$ -10-ый бит регистра LFSR1, $S_{2,11}$ - 11-ый бит регистра LFSR 2 и $S_{3,12}$ -12-ый бит регистра LFSR 3;

• если $S_{1,10} = S_{2,11} = S_{3,12}$, то производится сдвиг во всех трех регистрах, причем первым элементом регистра становится сумма по mod2 последнего битарегистра и считанного из середины бита.

• если из трех битов $S_{1,10}$, $S_{2,11}$ и $S_{3,12}$ равны только два ($S_j = S_i$), то сдвиг происходит только в этих двух регистрах LFSR j и LFSR i соответственно.

• возвращение к началу пункта 2 произойдет только после того, как все его действия не будут повторены 192 раза. Если все действия пункта 2 выполнены 192 раза- происходит переход к пункту 3.

1. Из полученных на выходе логической схемы 192 бит берутся 92 последних бита. Они дополняются 22 битами открытого ключа, в которые записывается двоичный номер кадра. Сумма 92 и 22 бит образует специфическую ключевую комбинацию.

2. Осуществляется перевод 144 битового кадра стандарта GSM 900 с открытой информацией в 144 битовый кадр с закрытой информацией.

С этой целью над 144 битами информации (одним кадром) и 144 битами специфической ключевой комбинации выполняется логическая операция XOR. Результатом применения булевой операции является зашифрованный (закрытый) информационный кадр.

Процесс дешифрации абсолютно аналогичен процессу шифрации с той лишь разницей, что логическая операция XOR выполняется над зашифрованным (закрытым) информационным кадром и полученной все тем же образом, но уже в приемнике, специфической кодовой комбинации, состоящей из 92 битов секретной кодовой комбинации и 22 битов открытого ключа с номером кадра.

Форматирование пакета (Burst Formatting). Как указывалось, выше, каждая передача информации от MS/BTS содержит излишнюю информацию (тестовую последовательность). Процесс форматирования пакета заключается в добавлении этих битов (среди которых имеются хвостовые биты) к основной передаваемой информации, увеличивая тем самым

скорость (bit rate) кодирования, но в то же самое время решая проблемы, возникающие при передаче информации через радиоэфир.

В системе GSM входной информацией для форматирования пакета является шифрованная информация объемом в 456 бит. Процедура форматирования пакета добавляет ещё 136 бит на блок из 20 мсек., в общем преобразуя исходное сообщение в результирующее сообщение объемом 592 бит.

Однако продолжительность каждого временного интервал кадра TDMA составляет 0.577 мсек. Следовательно, имеется возможность передать 156.25 бит информации (передача каждого бита занимает 3.7 мксек.), но пакет содержит только 148 бит. Свободное пространство в 8.25 бит является пустым и называется защитным периодом (Guard Period - GP). Данный период времени дает возможность MS/BTS осуществить процедуру “rampup” , “rampdown”. **Rampup** означает получение питание от батареи или от источника питания MS для передачи сигналов. Процедура **Rampdown** осуществляется после каждой передачи, и необходима для того, чтобы убедиться, что MS не использует энергию батареи в течение временного интервала, занятого другой MS.

После форматирования пакет состоит из 156.25 бит (для одного пакета) или 625 бит (в четырех пакетах) для речевого отсчета продолжительностью 20 мсек. Однако для того, чтобы настроить модулятор, с двух сторон пакета доступа используются несколько пустых битов. Это увеличивает объем сообщения до 676 бит для каждого речевого отсчета в 20 мсек. При использовании одной несущей в кадре TDMA кадре для организации связи одновременно для 8 абонентов общая скорость битов для системы GSM составляет 270.4 кбит/сек.

Детектор активности речи(VAD) играет решающую роль в снижении потребления энергии от аккумуляторной батареи в портативных абонентских терминалах. Он также снижает интерференционные помехи за счет переключения свободных каналов в пассивный режим. Реализация VAD

зависит от типа применяемого речевого кодека. Главная задача при проектировании VAD - обеспечить надежное отличие между условиями активного и пассивного каналов. Если канал на мгновение свободен, его можно заблокировать, поскольку средняя активность речи говорящего ниже 50%, то это может привести к существенной экономии энергии аккумуляторной батареи. К устройствам VAD предъявляются следующие основные требования [21,22]:

- минимизация вероятности ложной тревоги при воздействии только
- шума свысоким уровнем;
- высокая вероятность правильного обнаружения речи низкого уровня;
- высокое быстродействие распознавания речи, для исключения задержек включения;
- минимальное время задержки выключения.

В стандарте GSM принята схема VAD с обработкой в частотной области. Структурная схема VAD приведена на рис. 4.9.

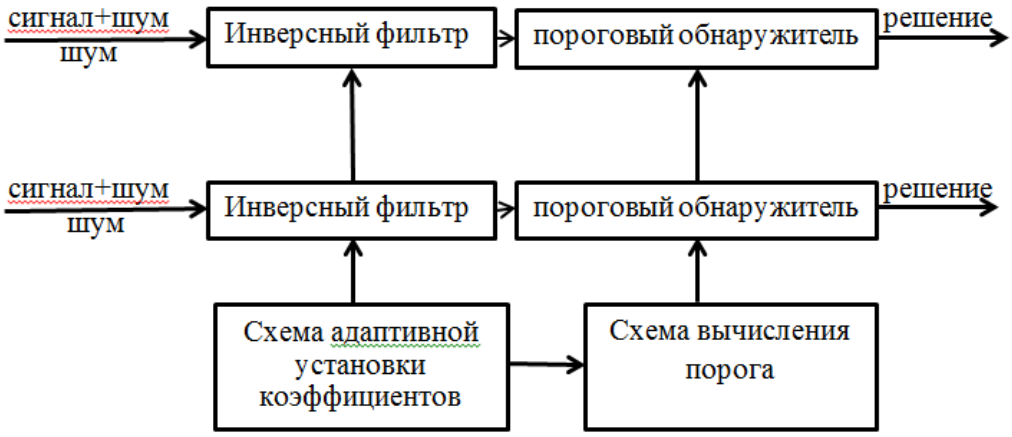


Рис. 4.9. Структурная схема VAD

Ее работа основана на различии спектральных характеристик речи и шума. Считается, что фоновый шум является стационарным в течение относительно большого периода времени, его спектр также медленно изменяется во времени. VAD определяет спектральные отклонения входного воздействия от спектра фонового шума. Эта операция осуществляется

инверсным фильтром, коэффициенты которого устанавливаются применительно к воздействию на входе только фонового шума. При наличии на входе речи и шума инверсный фильтр осуществляет подавление компонентов шума и, в целом, снижает его интенсивность. Энергия смеси сигнал + шум на выходе инверсного фильтра сравнивается с порогом, который устанавливается в период воздействия на входе только шума. Этот порог находится выше уровня энергии шумового сигнала. Превышение порогового уровня принимается за наличие на входе реализации (сигнал+шум). Коэффициенты инверсного фильтра и уровень порога изменяются во времени в зависимости от текущего значения уровня шума при воздействии на входе только шума. Поскольку эти параметры (коэффициенты и порог) используются детектором VAD для обнаружения речи, сам VAD не может на этой же основе принимать решение, когда их изменять. Это решение принимается вторичным VAD на основе сравнения огибающих спектров в последовательные моменты времени. Если они аналогичны для относительно длительного периода времени, предполагается, что имеет место шум, и коэффициенты фильтра и шумовой порог можно изменять, то есть адаптировать под текущий уровень и спектральные характеристики входного шума [21,22].

VAD с обработкой в спектральной области удачно сочетается с речевым RPE/LTP-LPC кодеком, так как в процессе LPC анализа уже определяется огибающая спектра входного воздействия, необходимая для работы вторичного VAD.

Экстраполяция потерянного речевого кадра. В условиях замираний сигналов в подвижной связи речевые фрагменты могут подвергаться значительным искажениям. При этом для исключения раздражающего эффекта при воспроизведении необходимо осуществлять экстраполяцию речевого кадра.

Было установлено, что потеря одного речевого кадра может быть значительно компенсирована путем повторения предыдущего фрагмента.

При значительных по продолжительности перерывах в связи предыдущий фрагмент больше не повторяется, и сигнал на выходе речевого декодера постепенно заглушается, чтобы указать пользователю на разрушение канала. То же самое происходит и с SID кадром. Если SID кадр потерян во время речевой паузы, то формируется комфортный шум с параметрами предыдущего SID кадра. Если потерян еще один SID кадр, то комфортный шум постепенно заглушается.

Применение экстраполяции речи при цифровой передаче, формирование плавных акустических переходов при замираниях сигнала в каналах в совокупности с полным DTX процессом значительно улучшает потребительские качества связи с GSM PLMN по сравнению с существующими аналоговыми сотовыми системами связи.

Формирование комфортного шума осуществляется в паузах активной речи и управляется речевым декодером. Когда детектор активности речи (VAD) в передатчике обнаружит, что говорящий прекращает разговор, передатчик остается еще включенным в течение следующих пяти речевых кадров. Во время первых четырех из них характеристики фонового шума оцениваются путем усреднения коэффициента усиления и коэффициентов фильтра LPC анализа. Эти усредненные значения передаются в следующем пятом кадре, в котором содержат информацию о комфортном шуме (SID кадр).

В речевом декодере комфортный шум генерируется на основе LPC анализа SID кадра. Чтобы исключить раздражающее влияние модуляции шума, комфортный шум должен соответствовать по амплитуде и спектру реальному фоновому шуму в месте передачи. В условиях подвижной связи фоновый шум может постоянно изменяться. Это значит, что характеристики шума должны передаваться с передающей стороны на приемную сторону не только в конце каждого речевого всплеска, но и в речевых паузах так, чтобы между комфортным и реальным шумом не было бы резких рассогласований в

следующих речевых кадрах. По этой причине SID кадры посылаются каждые 480 мс в течение речевых пауз.

Динамическое изменение характеристик комфортного шума обеспечивает натуральность воспроизведения речевого сообщения при использовании системы прерывистой передачи речи.

4.2. Модуляция

В стандарте GSM выбрана гауссовская частотная манипуляция с минимальным частотным сдвигом – GMSK и с индексом модуляции 0,3. Метод представляет собой частотную манипуляцию, при которой несущая частота принимает дискретные значения через интервалы времени, кратные периоду T битовой модулирующей последовательности. Используются две дискретные частоты несущей f_0:

$$f_н = f_0 - F/4 \text{ и } f_в = f_0 + F/4,$$

где F = 1/T - частота входной битовой последовательности.

Получаемый разнос частот $Df=f_в – f_н = F/2$ - это минимально возможный разнос, при котором обеспечивается ортогональность колебаний частот $f_в$ и $f_н$ на интервале T длительности одного бита. При этом за интервал T между колебаниями частот $f_в$ и $f_н$ набегает разность фаз, равнаяр. Таким образом, термин «минимальный сдвиг» в названии метода модуляции относится к минимально возможному сдвигу частоты несущей.

Модуляция несущей непосредственно прямоугольными импульсами битовой последовательности приводит к довольно широкому спектру частот, занимаемому в эфире радиосигналом. Более узкий спектр получается при модуляции «сглаженными» импульсами. Потому модулирующую битовую последовательность вначале пропускают через сглаживающий узкополосный гауссовский фильтр, чему и соответствует термин «гауссовская» в названии

метода модуляции. Именно эта дополнительная фильтрация отличает метод GMSK от метода MSK (Minimum Shift Keying - манипуляция с минимальным сдвигом).

Метод MSK иногда рассматривают как метод квадратурной фазовой манипуляции со смещением (OQPSK), но с заменой прямоугольных модулирующих импульсов длительности 2T полуволновыми отрезками синусоид или косинусоид. Рассмотрим сначала метод MSK, а затем отметим отличия, возникающие за счет дополнительной гауссовской фильтрации.

В методе MSK входная битовая последовательность разбивается на две последовательности, состоящие соответственно четным и нечетным импульсам. Модулированный выходной сигнал модулятора на протяжении очередного n-го бита определяется выражением, зависящим от состояния, текущего n-го и предшествующего (n-1)- го бита:

$$u(t) = \pm Cos(pt/2T)Cos\ w_0t \pm Sin(pt/2T)Sin\ w_0t = \pm Cos(w_0t \pm pt/2T),$$

$$(n-1)\ T \pounds t \pounds nT$$

Отсюда следует, что текущая фаза модулированного сигнала:

$$j(t) = w_0t \pm pt / 2T$$

За период следования входных битов T набег фазы составит:

$$Dj = \pm p/2,$$

а мгновенная частота, как производная от фазы

$$w(t) = d[j(t)]/dt = w_0 \pm p/2T = 2p\ (f_0 \pm F/4),$$

т.е. мгновенная частота принимает одно из двух значений $f_в$ или $f_н$. Эта частота постоянна на протяжении бита. Изменение знака перед синусами в выражении для модулированного сигнала означает переход с одной частоты на другую. Изменение общего знака перед выражением модулирующего сигнала, эквивалентное изменению начальной фазы, несущей на p, позволяет сохранить непрерывность фазы колебаний при изменении частоты.

Для наглядного пояснения метода MSK обратимся к рисунку 4.10.

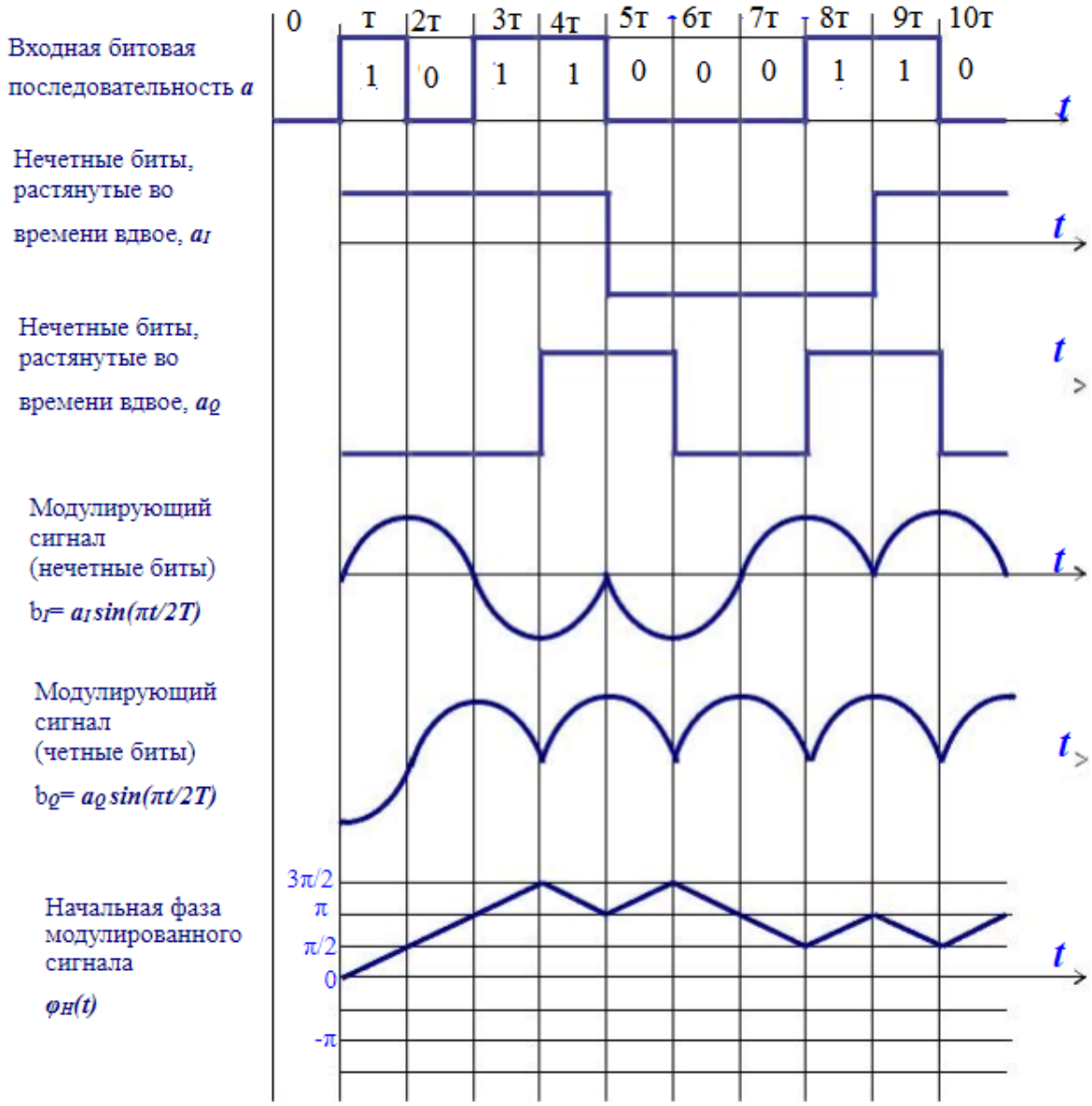


Рис. 4.10. Временные диаграммы сигналов GMSK

В первом графике представлен пример входной битовой (модулирующей) последовательности a. Второй и третий графики дают соответственно последовательности нечетных a_i и четных a_q бит входной последовательности, причем длительность каждого бита увеличена вдвое в сторону запаздывания, т.е. каждый бит «растянут» во времени до 2-х битового символа, и для удобства последующих рассуждений принято, что последовательности a_iи a_qпринимают значения + 1 и - 1 (значения - 1 соответствуют значению 0 исходной последовательности a). В результате для каждого битового интервала T расположенные одно над другим значения a_i и

a_qдают как раз ту пару четного и нечетного бит, которые являются аргументом закона модуляции.

Четвертый и пятый графики показывают форму модулирующих сигналов двух квадратурных каналов b_i и b_q, получаемых как произведение функций a_i и a_qсоответственно на квадратурные низкочастотные сигналы Sin (pt/2T) и Cos (pt/2T). Обратите внимание на скачкообразные изменения фазы этих сигналов на p в моменты изменения знаков a_i и a_q.

Окончательный модулированный сигнал, получается, как результат перемножения модулирующих сигналов квадратурных каналов с соответствующими несущими Sin(w_0t) и Cos(w_0t) и последующим суммированием полученных произведений. Принцип формирования GMSK-сигнала приведен на рисунке 4.11.

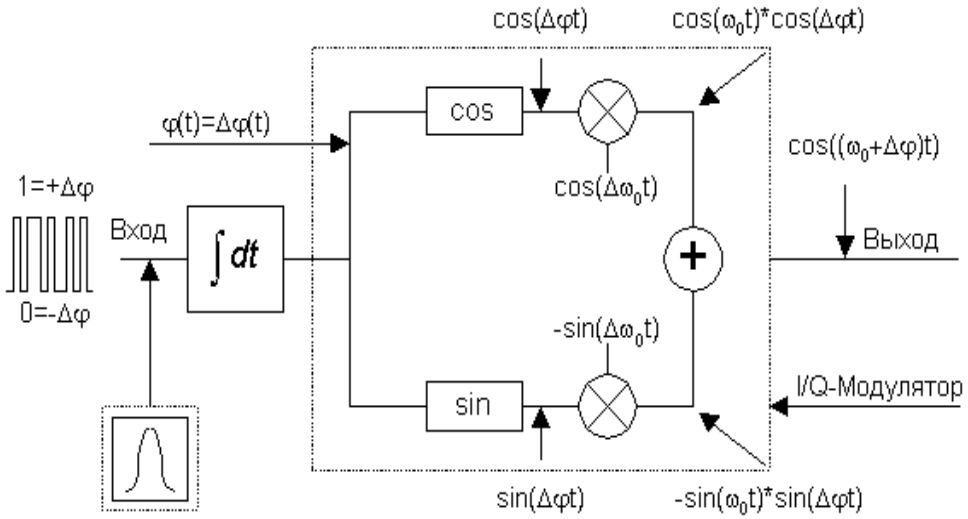


Рис. 4.11. Принцип формирования GMSK-сигнала

Модуляцию GMSK характеризуют следующие свойства:

- постоянная по уровню огибающая, позволяющая использовать передающие устройства с усилителями мощность класса С;
- узкий спектр на выходе усилителя мощности передающего устройства обеспечивающий низкий уровень внеполосного излучения;
- хорошая помехоустойчивость канала связи.

4.3. Проблемы, возникающие при передаче радиосигналов

Существует много проблем, возникающих при передаче радиосигналов. Рассмотрим некоторые наиболее известные их них [5,10,20,21].

Потери на пути распространения радиосигналов (Path loss) - это потери, возникающие тогда, когда принимаемый сигнал становится всё слабее и слабее из-за увеличения расстояния между MS и BTS. Проблема PL редко ведёт к разрыву соединения (dropped calls), потому что как только проблема становится экстремальной, соединение переключается на другую BTS и PL становится, соответственно, меньше.

*Затенения (Shadowing)*случаются тогда, когда на пути распространения радиосигнала между MS и BTS возникают физические препятствия, например, холмы, здания, деревья и т.д. Препятствия создают эффект затенения, который уменьшает уровень сигнала (signal strength). Уровень сигнала в процессе движения MS флуктуирует в зависимости от возникающих препятствий на пути между MS и BTS.

Действующие на сигнал *замирания* изменяют уровень сигнала. Снижение уровня сигнала называется глубиной замирания (fading dips). На рисунке 4.12 показаны препятствия, возникающие на пути распространения сигнала между MS и BTS.

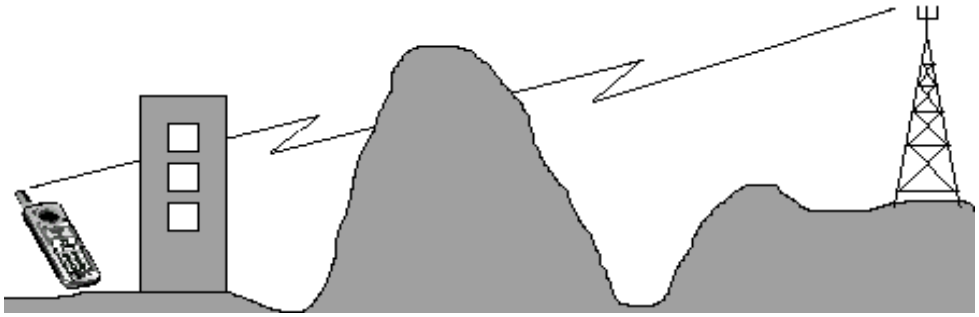


Рис. 4.12. Препятствия на пути передачи радиосигнала

Многолучёвые замирания (Multipath fading) возникают тогда, когда существует более чем один путь распространения радиоволны между MS и

BTS, и, в связи с этим, к приёмнику приходит более чем один сигнал. Последнее связано с многократным отражением радиосигнала от таких препятствий, как горы, здания, располагающиеся либо близко, либо далеко от приёмников.

Релеевские замирания сигналов (Rayleigh fading) возникают тогда, когда сигнал достигает приёмника по нескольким путям от базовой станции (рис. 4.13).

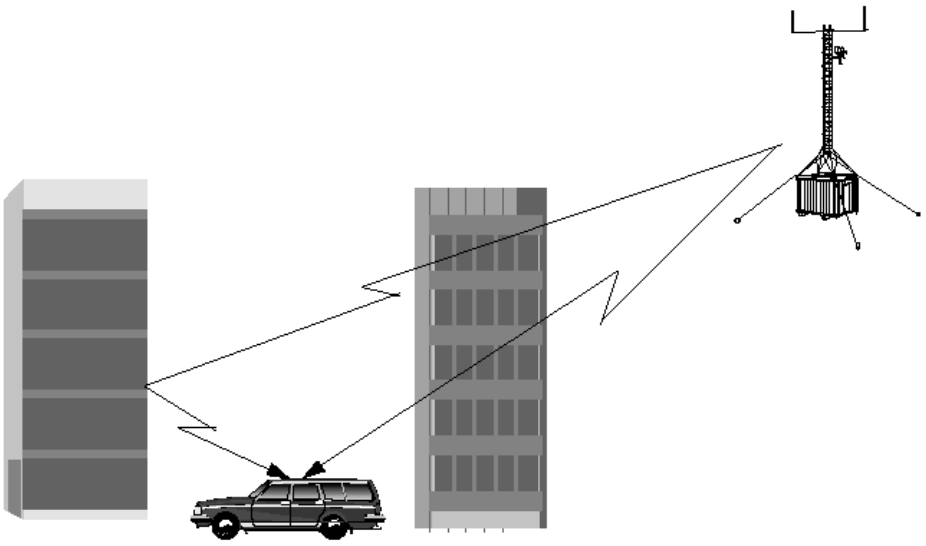


Рис. 4.13.Причина Релеевских замираний

В этом случае сигнал не принимается по линии прямой видимости прямо от передающей антенны, а приходит с разных направлений, отражаясь от зданий. Релеевские замирания сильно выражены тогда, когда препятствия располагаются близко к приёмной антенне. Результирующий принятый сигнал представляет собой сумму сигналов, пришедших с разной амплитудой и фазой. Глубина замираний и их периодичность зависят от скорости движения MS и рабочей частоты. Расстояние между замираниями приблизительно составляет половину длины волны колебания. Для систем GSM 900 расстояние между двумя замираниями составляет 17см.

Временная дисперсия (Time Dispersion) является дополнительной проблемой, связанной с многолучёвым характером распространения радиоволн между MS и BTS.

Однако в данном случае в сравнении с Релеевскими замираниями, отражённый сигнал приходит к приёмной антенне, отражаясь от достаточно удалённых объектов, таких как горы, холмы.

Временная интерференция вызывает межсимвольную интерференцию (Inter-Symbol Interference - ISI), где последовательные символы (биты) интерферируют друг с другом, что затрудняет приёмнику правильно определять символы.

Примером может служить рисунке 4.14, где представлена передача последовательности 1, 0 от BTS.

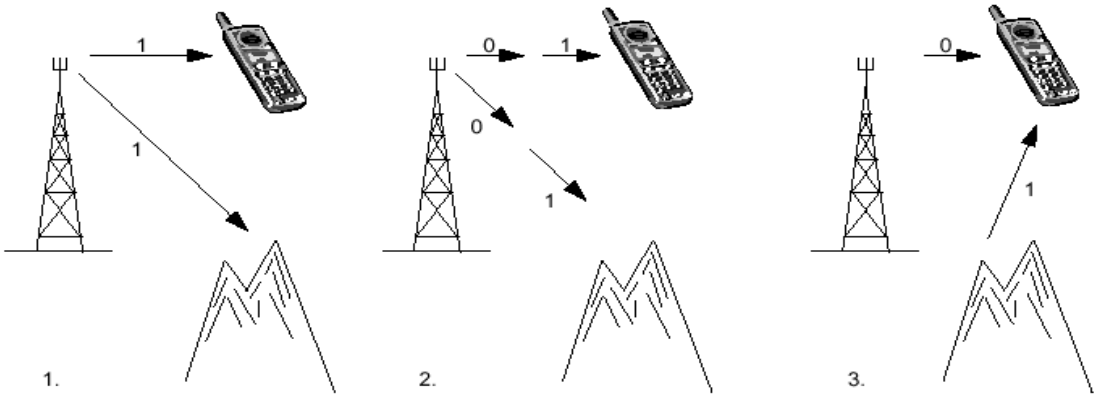


Рис. 4.14. Временная дисперсия

Если отраженный сигнал приходит после прохождения одного бита прямого сигнала, то приёмник обнаруживает «1» от отраженной волны и в то же самое время «0» от прямой радиоволны. Поэтому символ «1» интерферирует с символом «0» и MS не знает, какой из этих символов является правильным.

Временное наложение (Time Alignment). Каждая MS во время обслуживания вызова занимает один TS внутри кадра TDMA. Другими словами, мобильная станция занимает определённый временной интервал, в течение которого MS передаёт информацию на BTS.

Проблема временного наложения проявляется тогда, когда часть информации, переданная MS, не приходит в занимаемом TS. Вместо этого не пришедшая часть информации придёт в следующем TS, следовательно, может интерферировать с информацией, передаваемой другой MS, использующей другой TS (рис. 4.15).

Временное наложение возникает за счёт большого расстояния между MS и BTS. Сигнал же не может распространяться на большие расстояния внутри заданного значения временной задержки.

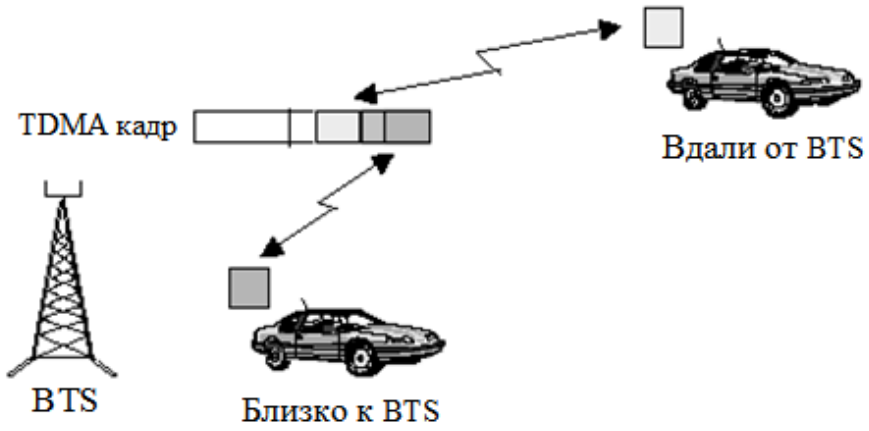


Рис. 4.15. Временная задержка

Комбинированные потери сигнала (Combined Signal Loss). Все проблемы, возникающие при распространении сигнала, в частности те, которые были описаны выше, возникают и существуют независимо друг от друга. Однако в процессе обслуживания некоторых вызовов эти проблемы могут возникать одновременно. Такое наложение сигналов можно представить зависимостью изменения сигнала на входе приёмника MS в процессе её движения.

На рисунке 4.16 представлена такая зависимость. На данном рисунке представлены суммарные потери в виде PL, затенений, Релеевских замираний (комбинированные потери сигнала). Уровень сигнала как глобальное среднее значение уменьшается с расстоянием (path loss), что приводит к разрыву соединения. Вокруг глобального среднего существуют

медленные вариации поля за счёт затенений и быстрые вариации за счёт Релеевских замираний.

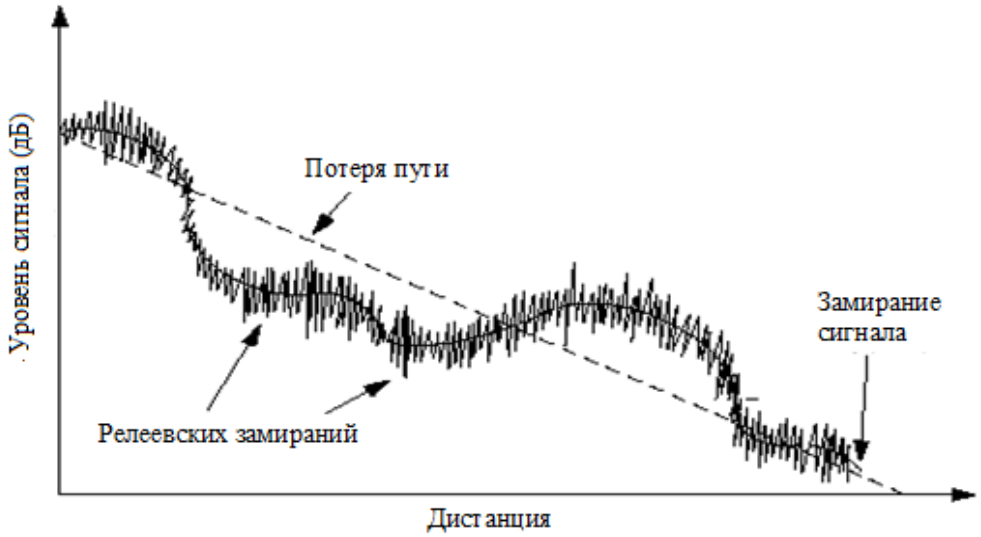


Рис. 4.16. Вариации сигнала с изменением расстояния

В любой другой точке флуктуации сигнала будут выглядеть так, как показано на рисунке 4.17.

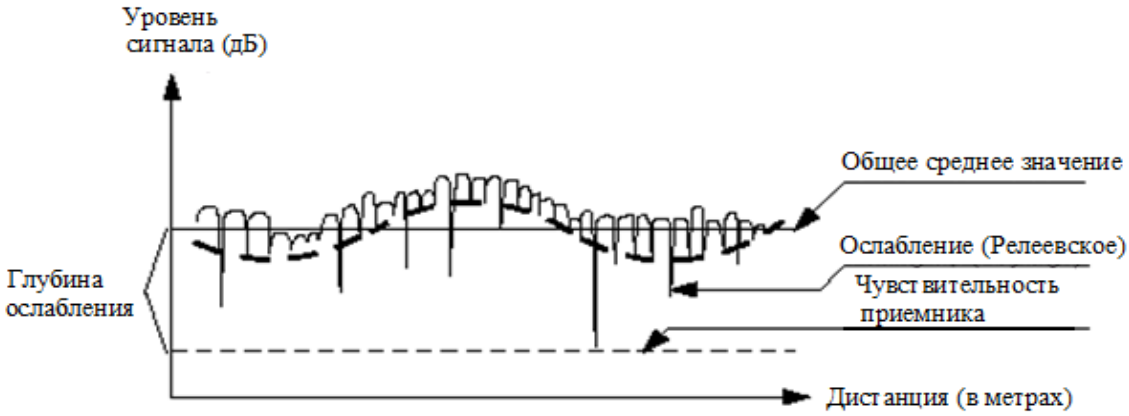


Рис. 4.17. Флуктуации сигнала на антенне приёмника

Из рисунка видно, что чувствительность телефона не должна быть меньше минимального значения сигнала (на рисунке 4.17 это показано глубиной затухания). Например, если необходимо принять сигнал с мощностью –100 dBm, то чувствительность телефона должна быть не меньше (-104 dBm), а даже больше, в противном случае информация будет

утеряна. Чтобы быть уверенным в том, что информация не будет потеряна, необходимо, чтобы глобальное среднее значение напряжённости поля было больше на такую величину dB, на какую в dB отклоняется самое большее замирание. Такой запас на замирание представляет собой разницу между чувствительностью и средним значением напряжённости поля.

Решение проблем, возникающих при передаче сигнала. При цифровой передаче данных качество переданного сигнала выражается в терминах «сколько некорректных битов информации было принято». Названием термина, характеризующего качество принятой информации, является частота ошибок по битам (BER – BitErrorRatio). BER определяет процентное отношение количества неправильно принятых битов к общему количеству переданных битов информации.

Переданные биты	1	1	0	1	0	0	0	1	1	0
Принятые биты	1	0	0	1	0	0	1	0	1	0
Ошибки		↑					↑	↑		3/10 = 30% BER

Данное отношение должно быть, как можно ниже. В общем случае, данное отношение невозможно свести к нулю, это связанно с тем, что путь распространения радиоволн постоянно меняется. Это особенно важно в течение передачи данных по сравнению с передачей речи, для которой приемлемо более высокое количество BER, чем для данных.

Канальное же кодирование используется для обнаружения и коррекции ошибок в принимаемом потоке битов. Данное кодирование добавляет биты к сообщению, осуществляя избыточность сообщения, позволяя не только обнаруживать неправильные биты, но и исправлять.

Перемежение (Interleaving). Чаще всего на практике битовые ошибки появляются последовательно друг за другом. Это связанно с тем, что долговременные глубокие замирания воздействуют сразу же на несколько последовательных битов информации. Канальное кодирование эффективно

используется в случаях появления одиночных ошибок и последовательностях короткой длины. В связи с этим, применение только канального кодирования не применимо в условиях появления длинных последовательностей ошибок.

Поэтому для избежание ошибочного приема битов вводится процесс Interleaving – интерливинга или перемежения (подробно рассматривался ранее). Этот процесс позволяет разбить последовательные биты сообщений так, чтобы эти биты не передавались последовательно друг за другом.

Рассмотрим в качестве примера блок сообщения, который может состоять из четырёх битов (1234). Если четыре таких последовательных блока передаются и один теряется, причём интерливинг отсутствует, то количество ошибок BER для всего сообщения составит 25%, а для потерянного сообщения 100%. И в этом случае восстановить его становится практически невозможным.

Если используется интерливинг, как показано на рисунке 4.18, то бит каждого блока может быть передан не последовательным способом. Если при передаче информации теряется один блок, то общее количество ошибок также составляет 25%. Однако такая потеря информации приводит к потере информации в каждом блоке, причём количество BER для каждого блока составляет 25%. Данная ситуация , как показано на рисунке 4.19, считается более приемлемой, чем ранее, так как вероятность определения и восстановления канальным кодером становится больше.

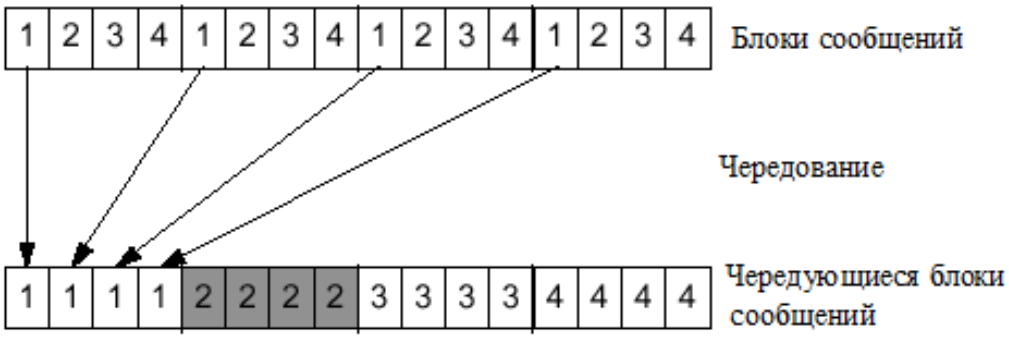


Рис. 4.18. Процесс интерливинга

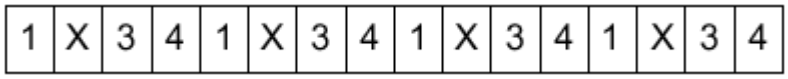


Рис. 4.19. Принятые блоки с учётом интерливинга

Разнесённый приём (AntennaDiversity). Использование разнесённого приёма позволяет получить больший уровень сигнала на выходе антенно-фидерного тракта посредством использования особенностей распространения радиоволн. Существует два типа разнесённого приёма:

• пространственное разнесение;

• поляризационное разнесение.

Пространственное разнесение. Для того, чтобы увеличить уровень принимаемого сигнала BTS прибегают к пространственному разнесению антенной системы. В данной конструкции используется 2 антенны вместо одной. Если при разнесении используется 2 антенны, то вероятность того, что в одно и тоже время на обе антенны придут две одинаковые волны, на которые повлияли глубокие замирания, очень мала. В диапазоне 900 МГц, используя пространственное разнесение, можно достичь усиления сигнала в 3 dB, при этом расстояние между антеннами должно быть 5 – 6 метров (12 – 18 λ) для горизонтального разнесения и 25*(12 – 18*λ) для вертикального разнесения. В диапазоне 1800 Мгц, расстояние должно быть уменьшено из-за меньшего значения длины волны.

Используя данный метод, и, выбирая сигнал с большим уровнем, можно в значительной степени уменьшить воздействие замираний сигнала.

Следует отметить, что пространственное разнесение даёт немного большее усиление сигнала (до 5 dBm), чем при использовании поляризационного приёма, но, в свою очередь, требует большего пространства для монтажа антенн.

На рисунке 4.20. представлено влияние использования пространственного приёма.

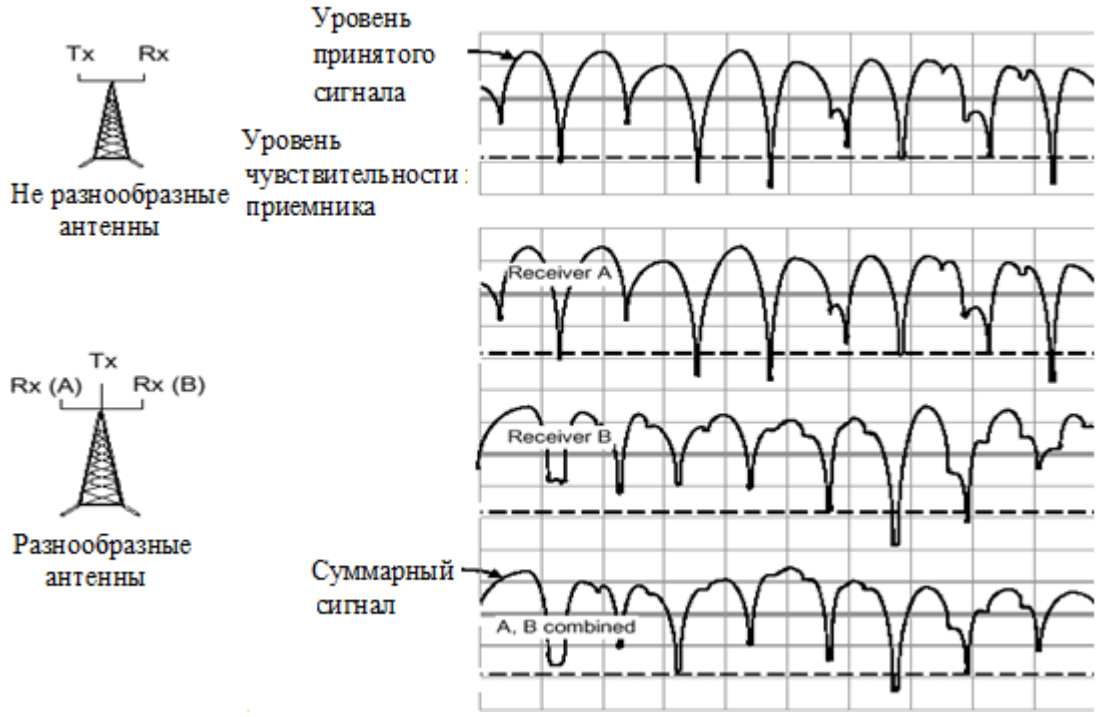


Рис. 4.20. Пространственное разнесение антенн

Поляризационное разнесение. При использовании поляризационного приёма антенны разнесённого приёма заменяются одной антенной с двойной поляризацией. Данная антенна имеет нормальный корпус, но имеет две различные поляризационные антенные решетки. Самые популярные антенны – это антенны с горизонтальной/вертикальной поляризацией и антенны, имеющие наклонную поляризацию в 45^{o}. Две антенные решётки соединяются **в** одну соединительную схему, называемую Rx в BTS. Две антенные решетки могут также быть использованы как совмещённые Tx/Rx антенны. На практике считается, что коэффициент усиления с использованием двух типов разнесённого приёма одинаков, но в случае поляризационного приёма экономится размер монтажной площадки антенно-фидерной системы.

Адаптивная коррекция (Adaptive Equalization)– метод, специально разработанный для решения проблем, связанных с временной дисперсией сигналов. Работа данного метода заключается в следующем**:**

1. За основу данного метода берется набор априорно известных битов информации, называемый тестовой последовательностью (training sequence). Данная последовательность известна как BTS, так и MS. BTS дает команду MS включить одну из этих последовательностей в передачу полезной информации по направлению к BTS.
2. MS включает в передаваемое сообщение по направлению к BTS тестовую последовательность (на рисунке 4.21, данная последовательность показывается буквой “S”). Однако, при передаче сообщения через радиоэфир, последнее может быть искажено (потеря нескольких бит информации).

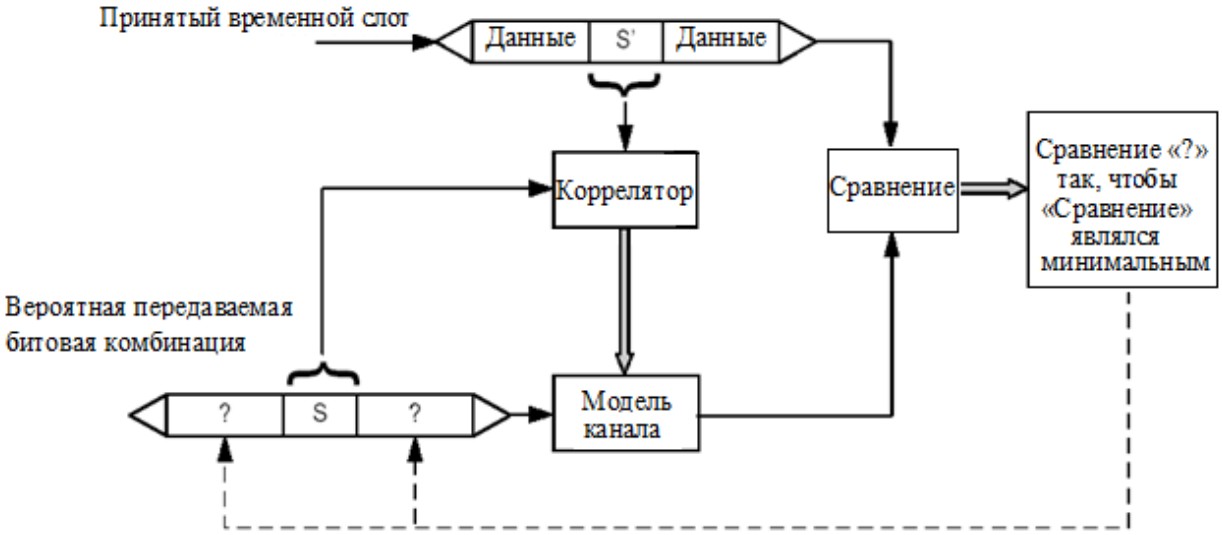


Рис. 4.21. Адаптивная коррекция

3. BTS принимает сообщение от MS и проверяет тестовую последовательность внутри передаваемого сообщения. После того, как сообщение принято, BTS сравнивает принятую тестовую последовательность с тестовой последовательностью, которую должна была использовать MS по указанию BTS. Если существует отличие междудвумя тестовыми последовательностями, это означает, что проблемы в радиоэфире воздействовали не только на тестовые последовательности, но также и на полезную информацию.

4. После установления различия в тестовых последовательностях, BTS начинает процесс восстановления потерянной полезной информации. Для этого она использует апостериорную информацию о повреждениях внутри тестовой последовательности. Поскольку BTS делает предположения о радиоэфире на основе тестовых последовательностей, то результат адаптивного восстановления потерянной информации не может быть 100% -но удачным.

Несмотря на это, применение такого метода дает достаточно хорошие результаты восстановления сигнала. К примеру, в качестве адаптивного эквалайзера в системе GSM используется эквалайзер Витерби (Viterbi equalizer).

Перескоки по частоте (Frequency Hopping). Как было указанно выше, Релеевские замирания частотно зависимы. Это означает, что глубина таких замираний различна в каждом из районов местности и на разных частотах. В связи с этим, в системе GSM предусмотрена опция Frequency Hopping - перескоки по частоте для MS и BTS в процессе установления соединения. Одновременный перескок по частоте MS и BTS обуславливается точной взаимной синхронизацией.

Согласно рекомендациям стандарта, GSM существует 64 последовательности перескока по частоте. Одна из этих последовательностей циклическая или последовательная, а 63 остальных – псевдослучайные, которые могут быть сконфигурированы самим оператором.

На рисунке 4.22, схематично представлен процесс перескока по частоте.

В течение кадра NTDMA используется несущая C1, в то время как в течение кадра N+1 используется несущая C2. Таким образом, на протяжении всего установленного соединения используется один и тот же временной интервал, но изменяются частоты согласно определённой последовательности перескока по частоте.

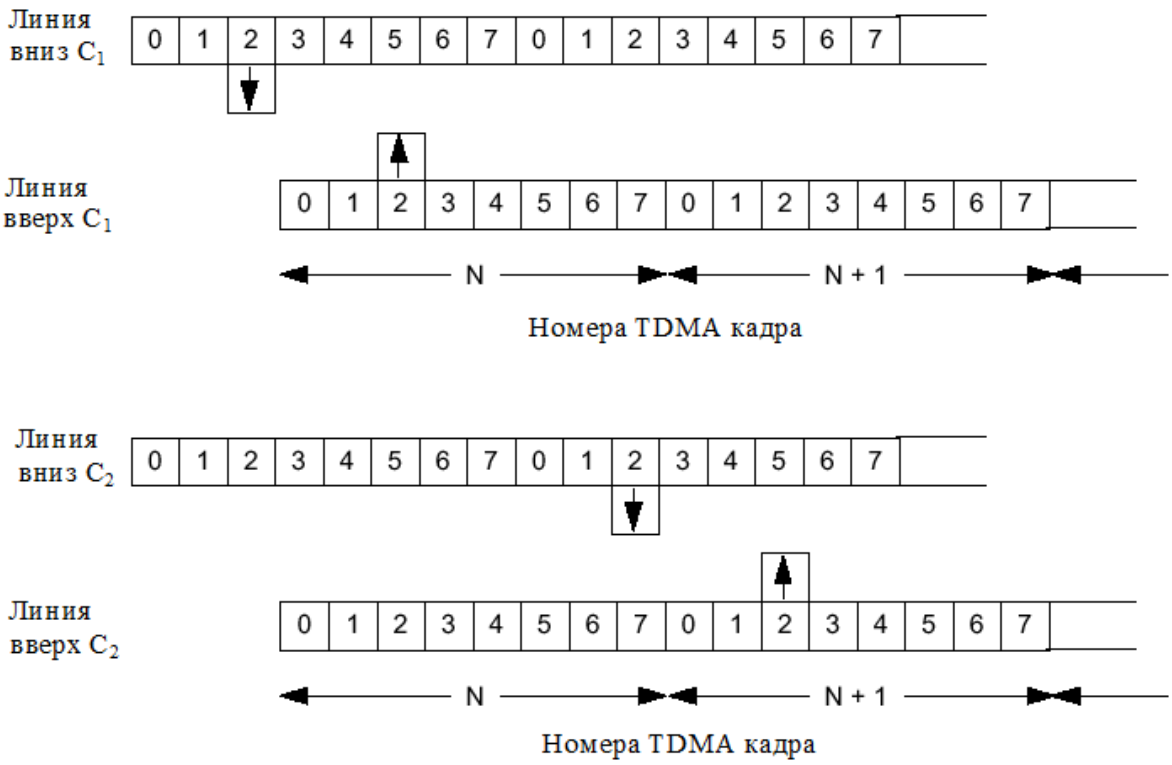


Рис. 4.22. Перескоки по частоте

Временная задержка (Timing Advance). Применение временной задержки связанно с тем, что иногда возникают проблемы с временным наложением. Данное опережение позволяет передавать свои кадры раньше, чем устанавливается соединение (рис. 4.23).

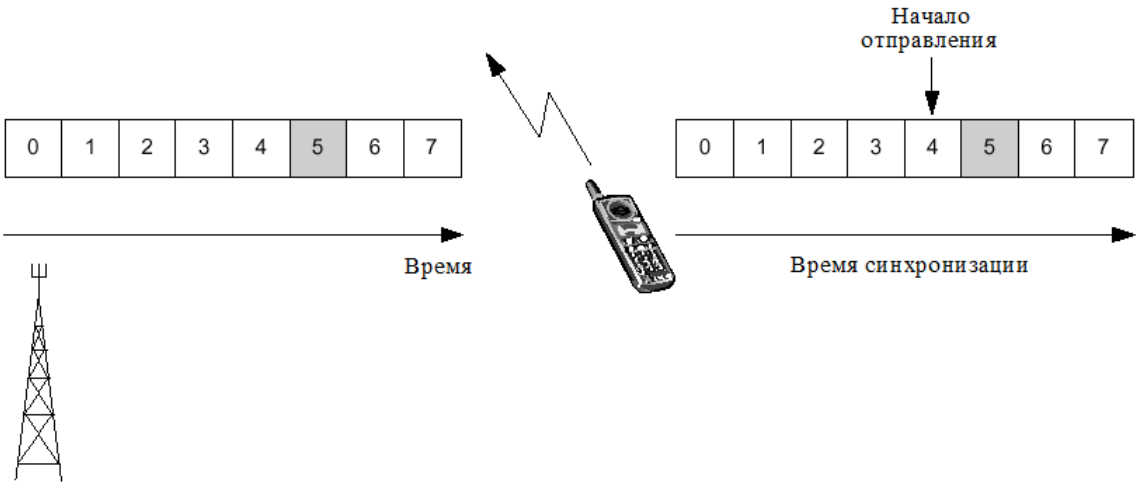


Рис. 4.23. Временное опережение

В системе GSM временная задержка интерпретируется в битах.

Известно, что первый этап установления соединения от MS к BTS осуществляется по направлению «Uplink» (направление от MS к BS). Данное соединение происходит в виде передачи пакета доступа (AB – access burst) по каналу параллельного доступа (RACH – random access channel).

Пакет доступа кроме первого этапа установления соединения используется при осуществлении хэндовера, при этом используется уже не канал RACH, а канал управления с быстрым доступом (FACCH – Fast Associated Common Control Channel).

Основной характеристикой пакета доступа является то, что кроме последовательности синхронизации (49 бит) и битов кодирования (39 бит) в нем передается информация о временной задержке распространения сигнала от MS к BTS. Информация о временной задержке предаётся в защитном интервале (GB – guard period), размер которого составляет 68.25 бит, а длительность - 252 мксек. Графическая интерпретация временных кадров представлена на рисунке 4.24.

Рис. 4.24. Графическая интерпретация интервала доступа

На рис. 4.24. TB (tail bits) означает так называемые хвостовые биты, они предназначенные для выравнивания во временном кадре.

При первом установлении соединения MS не знает, на каком расстоянии она находится от BTS, и, следовательно, не знает о величине временной задержки. Пакет доступа, который мобильная станция посылает со значением временной задержки «0» по отношению к ее внутренней временной базе,

является достаточно небольшим по своим размерам и умещается во временном интервале 252 мксек, включая двойную максимальную задержку распространения сигнала по радиоканалу.

Использование временной задержки даёт возможность определять расстояние между мобильным абонентом и базовой станцией.

Максимальный радиус соты в стандарте GSM составляет 35 км. Это расстояние и определяется максимальной задержкой на распространение сигнала (63 бит).

Используя данные о значениях временной задержки, можно определить действующее расстояние между базовой станцией и подвижной станцией, которое может быть записано в виде произведения TA и множителя расстояния, формула 4.1.

$$R = \frac{D_{RT}}{2} \cdot (TA) \quad , \qquad (4.1)$$

где TA – временная задержка для обычного радиуса сот; D_{RT} – расстояние от мобильной станции до базовой станции, которое определяется как

$$D_{RT} = v \cdot t \quad , \qquad (4.2)$$

где v – скорость света $3 \cdot 10^8 [м/с]$; $t = 1$ *бит* = 48/13 *[мксек]*.

Контрольные вопросы

1. Приведите общее описание процессов обработки речи стандарта GSM.
2. Поясните процесс речевого кодирования (Speech Coding).
3. Поясните процесс канального кодирования (Channel Coding).
4. Поясните, что понимается под процессом перемежения (Interleaving).
5. Поясните, что понимается под первым уровнем перемежения.
6. Поясните, что понимается под вторым уровнем интерливинга.

7. Назначение шифрования (Ciphering/Encryption) в стандарте GSM.
8. Как форматируется пакет (Burst Formatting) в стандарте GSM.
9. Назначение и работа детектора активности речи (VAD).
10. Зачем формируется комфортный шум в стандарте GSM.
11. Как осуществляется экстраполяция потерянного речевого кадра в стандарте GSM?
12. Какая модуляция радиосигнала используется в стандарте GSM, приведите структурную схему и поясните её.
13. Поясните, что понимается под потерями на пути распространения радиосигналов (Path loss).
14. Поясните процесс затенение сигнала.
15. Как происходит процесс многолучёвого замирания (Multipath fading)?
16. Когда происходят релеевские замирания сигналов (Rayleigh fading)?
17. Что понимается под временной дисперсией сигнала (Time Dispersion)?
18. Как происходит временное наложение (Time Alignment) сигнала?
19. Как происходят комбинированные потери сигнала (Combined Signal Loss)?
20. Как при цифровой передаче данных оценивается качество переданного сигнала?
21. Что понимается под перемежением (интерливингом)?
22. Какие существуют типы разнесённого приёма сигнала (Antenna Diversity)?
23. Поясните процесс пространственного разнесения сигналов.
24. Поясните процесс поляризационного разнесения сигналов.
25. Что понимается под адаптивной коррекцией сигнала (Adaptive Equalization)?
26. Поясните и как осуществляется перескоки по частоте (Frequency Hopping).
27. Поясните назначение и процесс применения временной задержки (Timing Advance) сигнала.

ГЛАВА 5. УПРАВЛЕНИЕ СЕТЯМИ СВЯЗИ В СТАНДАРТЕ GSM

5.1. Задачи системы сетевого управления

Задачи управления процессами связи в системе GSM решаются центром управления и обслуживания OMC (Operation and Maintenance Center) (рис. 5.1).

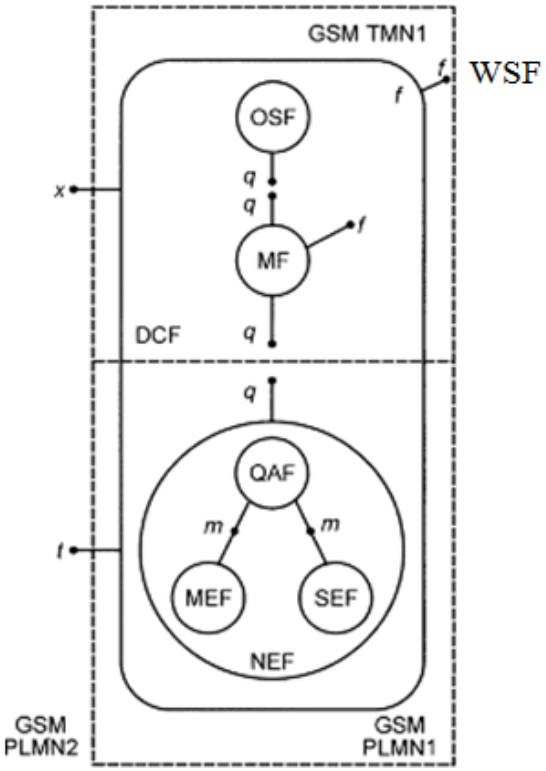


Рис. 5.1. Схема управления процессами связи в системе GSM

где: RP - контрольные точки (интерфейсы)

q - класс контрольных точек между OS, M и NE функциями;

f - класс контрольных точек рабочей станции (с абонентами сетей GSM);

д - класс контрольных точек от рабочей станции до пользователя (MMI);

x - класс рабочих точек для связи с другими сетями, включая другие TMN;

т - нестандартные внутренние контрольные точки;

t - контрольные точки для связи с другими сетями

FB - функциональные блоки

WSF - функциональный блок рабочей станции;

OSF - функциональный блок операционных систем;

MF - промежуточный функциональный блок;

DCF - функции системы связи GSM, связанные с передачей данных;

QAF - функции адаптера Q-интерфейса;

SEF - функции поддержки (обеспечения) абонента;

MEF - функции технического обслуживания абонентов;

NEF - функции элементов сети.

В основе построения OMC заложен принцип сетевого управления, в соответствии с которым для системы сетевого управления (GSM NM) были определены следующие задачи проектирования [5,10-11]:

1. Система GSM NM должна обеспечивать взаимодействие с существующими системами связи общего пользования и быть их естественным продолжением.
2. Система GSM NM должна быть достаточно гибкой, чтобы обеспечивать перспективное развитие наземных сетей связи общего пользования (PLMN), а также функций и служб сетевого управления.
3. Система GSM NM должна быть настолько прозрачной для технологий, используемых в существующих PLMN, насколько это возможно.
4. Система GSM NM должна иметь модульную структуру, чтобы независимо от размеров сети, где осуществляется управление, обеспечивать требуемые функции.
5. Система GSM NM не должна быть зависимой от изготовителя, то есть должна предусматривать взаимозаменяемость оборудования.

6. Структура и функции GSM NM не должны ограничивать деятельность и выбор операторов и изготовителей, а также возможность индивидуального использования, например, для организации частных локальных сетей связи.
7. Система GSM NM должна быть отказоустойчивой, то есть ни отказ оборудования, ни человеческий фактор не должны приводить систему или сеть связи в нерабочее состояние.

Перечисленные задачи решены путем принятия для сетей связи GSM модели открытых систем (OSI) Международной организации стандартов (ISO), выбором функциональной архитектуры системы сетевого управления, учитывающей различное физическое исполнение, четким определением сопряжения стандартов и протоколов передачи сообщений.

5.2. Принципы построения системы сетевого управления

В основу построения системы сетевого управления электросвязью (TMN) в стандарте GSM положена структурированная концепция CCITT [7,10], которая учитывает возможность развития и интеграции создаваемых и существующих сетей управления. В соответствии с выбранной концепцией GSM TMN должна обеспечить организованную сетевую структуру для достижения взаимосвязи различных операционных систем (для TMN) и устройств связи (для PLMN) на основе согласованной архитектуры со стандартными протоколами и устройствами сопряжения. Концептуально TMN представляет собой отдельную сеть, которая сопрягается с PLMN в нескольких различных точках с целью получения от нее информации и контроля ее работы. Для обеспечения управления TMN может использовать отдельные структурные части PLMN (например, систему сигнализации SS № 7, B-канал в структуре канала связи ISDN). Исходя из общей концепции, GSM TMN обеспечивает высокую степень гибкости, что отвечает различным технологическим условиям построения PLMN и требованиям различных операторов.

Функционально TMN обеспечивает средства для транспортировки и обработки информации, относящейся к управлению PLMN. Как показано на рисунке 14.1, обобщенная функциональная архитектура для GSM TMN и PLMN включает в себя функциональные блоки OSF операционных систем (OS), промежуточные функциональные блоки MF и функциональные блоки передачи данных DSF. Они включают в себя основные функции TMN, что позволяет ей решать свои прикладные задачи. TMN подключается к функциональным блокам элементов сети PLMN (NEF), а также непосредственно к функциональным блокам рабочей станции (WSF).

Рабочая станция может непосредственно подключаться к различным элементам сети через внешние для TMN соединения.

Контрольные точки, показанные на рис.5.1, определяют концептуальные точки информационного обмена между функциональными блоками. Контрольная точка становится интерфейсом, когда функциональные блоки включаются в отдельные части оборудования [7,10].

Такая функциональная концепция GSM TMN обеспечивает выполнение функций сетевого управления на оборудовании PLMN (в смысле использования одних и тех же ресурсов для обработки) над операционными системами и промежуточными устройствами, ориентированными на сетевое управление. Следует отметить, что в случае применения одного процессора для выполнения функций сетевого управления и функций связи, они всегда логически разделяются.

5.3. Распределение функций сетевого управления

Операционные системы. Физическая конфигурация TMN обеспечивает альтернативные решения как централизации, так и распределения общих функций операционных систем, что включает в себя:

- обслуживающие прикладные программы;
- функции базы данных;

- обеспечение абонентского терминала;
- анализирующие программы;
- форматирование данных и передачу сообщений.

В GSM TMN все эти функции используются для централизованной дистанционной обработки, то есть в центре управления и обслуживания OMC (в терминологии TMN нужно рассматривать как сетевую OS), тогда как специальные части этих функций (так называемые функции жизнеобеспечения) должны локально присутствовать в узловой базовой OS.

Процессы сопряжения. Составной частью функций сети управления связью являются процессы сопряжения — процессы, которые определяют направления соединений и/или воздействий на информацию, передаваемую между отдельными элементами сети (NE) и операционными системами по каналам передачи данных.

Процессы сопряжения классифицируются по пяти общим категориям:

1) управление связью;

2) сопряжение протоколов и обработка данных;

3) сопряжение (объединение) простых функций;

4) процессы принятия решений; 5) хранение данных.

Процессы сопряжения имеют место как в автономном оборудовании, так и в отдельных элементах сети.

Передача данных в GSM TMN. Функции передачи данных (DCF) для GSM TMN обеспечиваются сетью передачи данных (DCN) или локальными сетями связи (LCN).

DCN для GSM TMN соответствует эталонной модели OSI. Функции передачи данных включают в себя обеспечение соединения через соответствующие сопряжения различных элементов сети к операционным системам. Интерфейс, используемый в процессе соединений, определяется в Рекомендациях МККТТ М.2х как Q3 интерфейс. Этот интерфейс обеспечивает полный доступ ко всем частям TMN. Некоторые функции

определены тем, что система сигнализации МККТТ SS N7 должна относиться к интерфейсу Q3.

Для других функций оператор имеет возможность использовать закрепленные каналы с протоколом серии X.25 или коммутируемые сети пакетной передачи данных общего пользования (PC PDN).

В локальных сетях связи (LCN) при осуществлении соединений с PLMN для реализации функций передачи данных TMN могут использоваться интерфейс Q2 МККТТ и A-bis интерфейс.

Элементы сети. В системе связи GSM элементами сети (NE) являются узлы PLMN, например, MSC, HLR, BSS или любая часть связного оборудования. Элементы сети могут обеспечивать следующие группы функций сетевого управления:

- функции обслуживания объекта (MEF), сопряжены с процессами связи. Обслуживаемый объект (ME) может иметь одну иди более функций MEF;
- функции обеспечения объекта (SEF), непосредственно не включены в процесс связи. К ним относятся, например, локализация отказов, сбор данных. Объект обеспечения (SE) может иметь одну или более функций SEF.

Элементы сети могут иметь функции первой или второй группы, а также то и другое одновременно.

5.4. Стандартные интерфейсы в системе сетевого управления

Обеспечивают взаимодействие элементов сети, операционных систем и рабочих станций через сети передачи данных или локальные сети связи. Для гарантированной совместной работы соединяемых элементов сети необходимы четкие технические требования к интерфейсу, функционально независимые от типа устройства и поставщика. Это требует совместимых протоколов связи и совместимого метода представления данных для

передачи сообщений, включая совместимые описания групповых сообщений для функций сети управления.

Интерфейсы между TMN. Состав и функциональное назначение интерфейсов в GSM TMN показаны на рисунке 5.2.

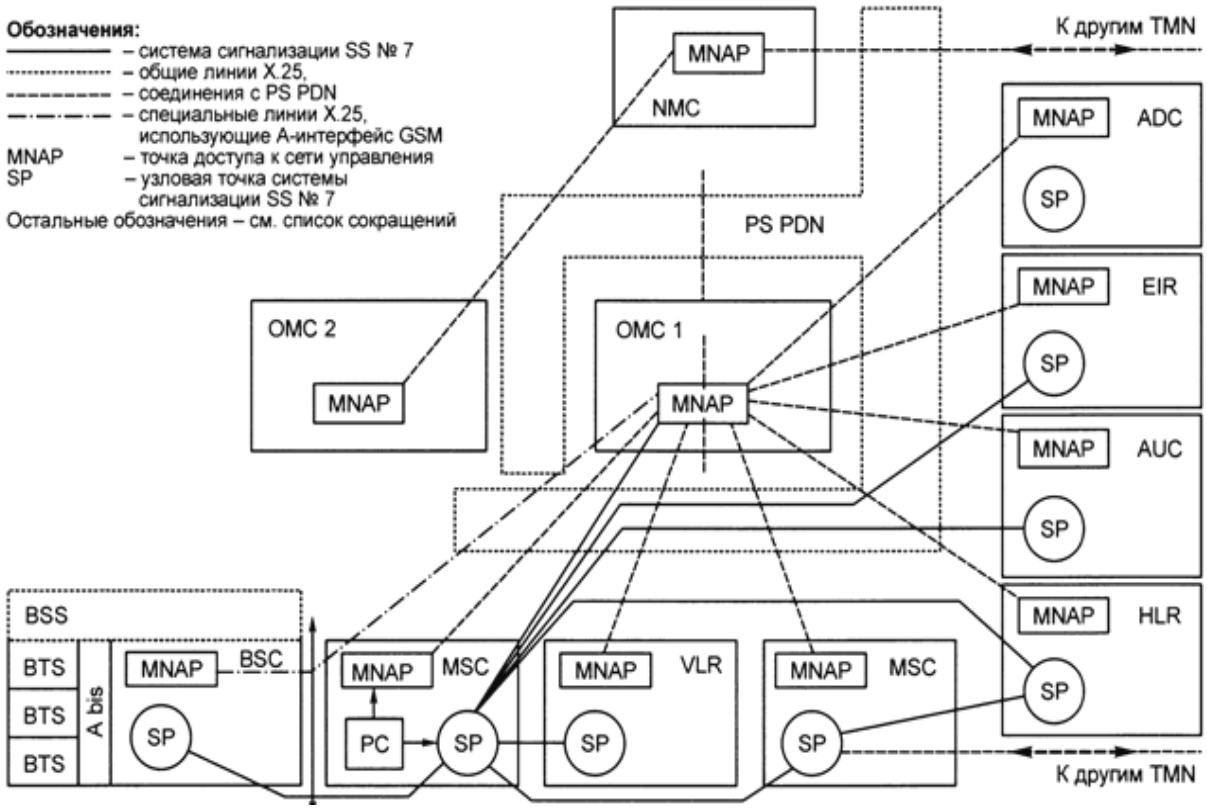


Рис. 5.2. Интерфейсы GSM TMN

Для передачи сообщений между сетями управления, используемыми, например, разными операторами применяется система сигнализации CCITT SS № 7 или X.25. При применении SS№7 используются протоколы CCITT (Голубая книга), рекомендация Q.795 [13-16]. При использовании сетей X.25 необходимы дополнительные соглашения между операторами по использованию протоколов более высокого уровня. Некоторые функции сетевого управления определены CEPT рабочей подгруппой SPS 6 в рекомендации GSM 09.02 [13-16], которая требует использования SS № 7 в следующих случаях:

- передачи информации между MSC и HLR другой PLMN;

- идентификации оборудования;
- обмена сообщениями между регистрами положения;
- при запросе на «эстафетную передачу».

Интерфейс TMN между PLMN и узлами TMN.В общем случае операторы сетей могут свободно использовать либо систему сигнализации SS № 7, предусмотренную в PLMN, либо специализированную сеть X.25 в соответствии с рекомендациями CCITT (Голубая книга) Q.513 [13-16]. При использовании сетей X.25 могут быть необходимы средства для преобразования протоколов обмена (X.25 — SS № 7).

Информационный обмен в процессе сетевого управления между BSS и MSC (A-интерфейс, рис. 5.3) обеспечивается SS № 7.

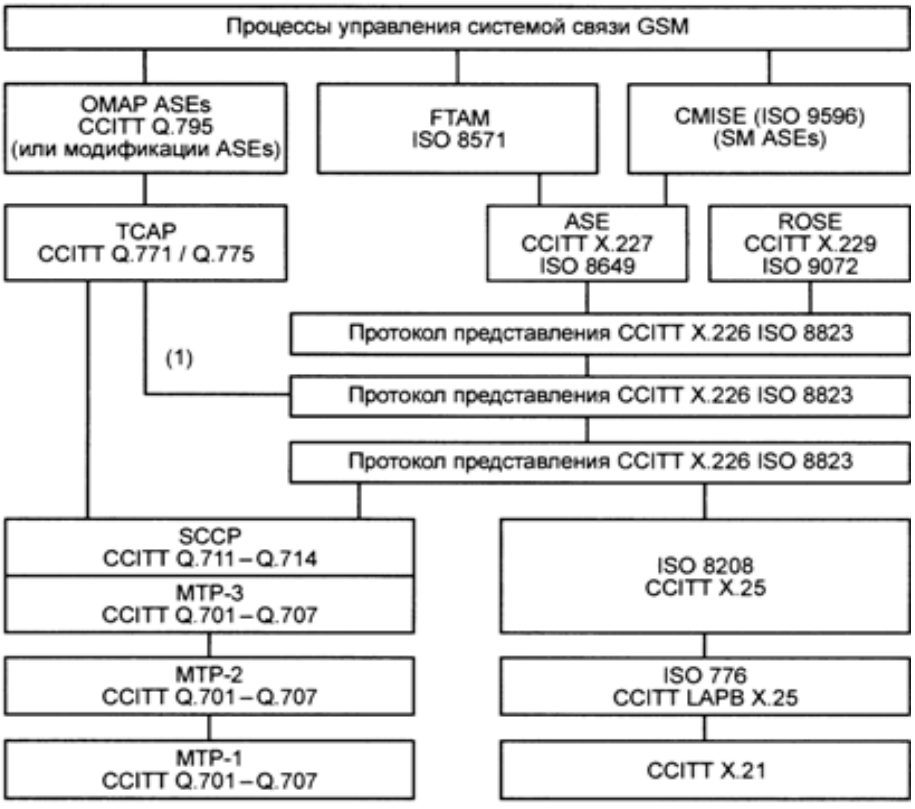


Рис. 5.3. Информационный обмен в процессе сетевого управления между BSS и MSC

Требования к средствам файлового обмена обеспечиваются использованием SCCP класса 2 и транспортного протокола X.224 класса 2, либо SCCP класса 3 и X.224 класса 0. Также предусмотрена специальная

версия GSM, касающаяся применения соединений X.25 на A-интерфейсе. Интерфейс между BTS и BSC (интерфейс GSM A-bis) основан на применении LAPD протоколов для информационного обмена при сетевом управлении. Все узлы PLMN, за исключением BTS, оснащены общим интерфейсом X.25. Это обеспечивает полный доступ к TMN на уровне 3 либо локально, либо дистанционно за счет использования отдельного подключения к PS PDN. При использовании в PLMN локальных сетей связи интерфейсы TMN определяются CEPT рекомендацией T/K 02-11 [11,13]. Полная структурная схема процессов управления системой связи GSM, состав и сопряжения протоколов связи показаны на рис.5.3.

Протоколы более высоких уровней, используемые в GSM TMN. Сопряжение на более высоких уровнях (выше уровня 3) может быть предусмотрено при использовании стандартных протоколов, основанных на рекомендациях (Голубая книга) CCITT Q.795 или на стандартах ISO для общих информационных служб управления (CMIS) и доступа и управления файловым обменом (FTAM), как это иллюстрируется на рис.5.3 [13-16]. Однако на первом этапе не рекомендуется использование OMAP в GSM TMN, так как это требует сетевого обслуживания без подключений, которое не может быть поддержано со стороны SS № 7 и X.25. Кроме того, способы файлового обмена, которые являются обязательными для эффективного управления PLMN, полностью не определены в OMAP.

Контрольные вопросы

1. Кем решаются задачи системы сетевого управления в стандарте GSM?
2. Какие определены задачи проектирования для системы сетевого управления (GSM NM)?
3. Что положено в основу построения системы сетевого управления в стандарте GSM?

4. Приведите и поясните обобщенную функциональную архитектуру для GSM TMN и PLMN.
5. Распределение функций сетевого управления в GSM. Операционные системы.
6. Распределение функций сетевого управления в GSM. Процессы сопряжения.
7. Распределение функций сетевого управления в GSM. Передача данных в GSM TMN.
8. Распределение функций сетевого управления в GSM. Элементы сети.
9. Стандартные интерфейсы в системе сетевого управления GSM.
10. Виды интерфейсов между TMN.
11. Стандартные интерфейсы в системе сетевого управления GSM.
12. TMN интерфейсы между PLMN и узлами TMN.
13. Стандартные интерфейсы в системе сетевого управления GSM.
14. Протоколы более высоких уровней, используемые в GSM TMN.

ГЛАВА 6. МОБИЛЬНОЕ ПРИЛОЖЕНИЕ В СТАНДАРТЕ GSM

6.1. Определение мобильного приложения

Мир современных технологий достаточно быстро развивается в последние годы. Домашний компьютер или же ноутбук — не очень удобные предметы, так как их перемещение весьма трудоёмкий процесс. Для того чтобы облегчить людям жизнь, создали так называемые «умные» телефоны — смартфоны, а также много других мобильных устройств.

На сегодняшний день каждый человек имеет, помимо обычного персонального компьютера, кучу различных гаджетов, таких как смартфон, планшет, mp3-плеер и т.д.Теперь каждый из нас имеет возможность в любой точке мира общаться с людьми, проверять почту, окунуться в мир игр и прочее.

В современном мире трудно представить себе мобильное устройство, на котором бы не стояло ни одного приложения. Они прочно вошли в нашу жизнь практически одновременно с планшетами и смартфонами. Поэтому данное направление так стремительно развивается и захватывает рынок. Все больше предпринимателей понимают необходимость разработки мобильного приложения.

Мобильное приложение представляет собой разработанную программу для планшетов и смартфонов, которая устанавливается на ту или иную платформу и имеет определенный функционал. Проще говоря, выполняет определенные действия и решает заданный круг вопросов.

Совсем недавно мобильные приложения представляли собой только игры. Однако очень быстро предприниматели поняли, что приложение может помочь вести бизнес, а также стать сильным маркетинговым инструментом, с помощью которого можно повысить узнаваемость и доверие к своему бренду, проводить рекламные кампании, упростить обратную связь с клиентами.

Преимущества мобильных приложений. Изначально мобильные дополнения были предназначены для быстрого доступа к электронной почте. Такое приложение имело очень высокий спрос, потому эта сфера стала стремительно развиваться. Такому расширению способствовало быстрое развитие, как сотовой связи, так и беспроводных технологий. На данный момент все большее количество людей входят в Интернете с мобильных устройств, что позволяет при наличии мобильного дополнения иметь быстрый доступ к нужной информации.

Мобильные приложения имеют такие преимущества:

- удобный доступ к сервису электронной почты;
- возможность входа в любую социальную сеть;
- наличие различных игр;
- полезные программы для жизни.

Имея мобильное дополнение можно быстро и легко проверить почту, отправить неограниченное число сообщений, независимо от их вместительности. Каждый из нас зарегистрирован в большом количестве социальных сетей, в таком случае мобильное приложение значительно облегчает доступ к ним на смартфоне и прочем мобильном устройстве [24,25].

Большой ассортимент игр в мире приложений помогает развлечь человека в свободное время в дороге, на работе и дома. Кроме забавных игр, существуют полезные приложения, такие как программы для прочтения книг, рецепты на все случаи жизни, программы тренировок, дневники похудения и так далее.

Кроме того, мобильные приложения — это отличный маркетинговый инструмент для любого бизнеса. Такие дополнения помогают быстро распространять необходимую информацию для определенного человека, эффективно взаимодействовать с клиентами, укреплять имидж компании, оптимизировать бизнес-процессы, а также получать доход от продажи приложений.

Мобильные приложения делятся на основные три вида[24]:

- Веб-приложение или мобильный сайт;
- Гибридное приложение;
- Нативное приложение.

Веб-приложение или мобильный сайт представляет собой обычный сайт с расширенным функционалом. Главной особенностью является то, что работа приложения целиком зависит от интернет-соединения и осуществляется при помощи браузера. При плохом интернет-соединении качество связи оставляет желать лучшего.

Мобильным сайтом считается специальный сайт, адаптированный для просмотра и функционирования на мобильном устройстве. А мобильное приложение, в свою очередь, является специально разработанное приложение под конкретную мобильную платформу (iOS, Android, Windows Phone).

Сравнительная характеристика мобильного сайта и мобильного приложения приведена в таблице 6.1.

Таблица 6.1.

Сравнительная характеристика мобильного сайта и мобильного приложения

Совместимость	Мобильный сайт	Мобильное приложение
Охват аудитории	Отображается одинаково в браузере смартфона на любой платформе, вне зависимости от модели телефона	Требуется разработка нескольких приложений для разных платформ
Затраты при выходе на рынок	Любые мобильные устройства, имеющие выход в интернет	Только смартфоны и планшеты
Открытость	Затраты на размещение сайта на хостинге	Оплата разработчикам лицензий AppStore, Android Market

Простота использования	Доступен для всех пользователей	Доступен после установки
Доступность функционала	Не требует дополнительных действий	Необходимо скачивание и установка
Использование без интернета	Ограничена	Практически полная
Поддержка	Не на всех устройствах	На всех устройствах
Поддержка графики	Легко изменять и справлять проблемы	Возможно после обновления
Взаимодействие с пользователями	С «тяжелыми изображениями» возникают трудности при загрузке	Поддерживает
Удобство при регулярном использовании	Средний уровень	Высокий уровень
Персонализация	Средний уровень	Высокий уровень
	Нацелен больше на сервис, чем на пользователя	Приложение больше нацелено на индивидуального пользователя, чем мобильный сайт

Гибридное приложение по сути является чем-то средним между веб-приложениями и нативными. Такие приложения скачиваются в официальных магазинах и имеют ограниченный доступ к аппаратной части мобильных устройств. Например, можно настроить push-уведомления. Но контент остается кроссплатформенным и размещенным на сервере.

По стоимости есть дешевые и дорогие гибридные приложения. Цена зависит от того, насколько такое приложение будет приближенно к нативному.

Основными недостатками гибридного приложения являются:

• внешний вид, который не будет изменяться в зависимости от мобильной платформы;

• ограниченность объема хранения информации, дополнительную информацию приложение будет докачивать из интернета;

• сложный процесс оптимизации под разные размеры экранов;

• разработка некоторых компонентов (дополнительные строки, выезжающее меню и т.д.) каждый раз с нуля.

Нативное приложение самое трудоемкое, но большинство из них подходит для каждой операционной мобильной системе**.** Разработка осуществляется для каждой платформы (Windows Phone, IOS, Android) отдельно. Это достаточно сложно и сроки будут более растянутыми, по сравнению с другими видами приложений. Соответственно цена будет самой дорогой. Это и есть главные два минуса нативного приложения.В остальном плюсы очевидные:

- приложение будет работать в любом месте независимо от интернет-соединения;
- быстрая скорость и корректность работы;
- доступ к аппаратной части мобильного устройства (камера, геолокация, микрофон, адресная книга и т.д.);
- экономия батареи и памяти мобильного устройства.

Выбор из рассмотренных видов мобильных приложений зависит от того, на какие результаты нацелен потребитель, какую территории должны использовать приложения и какое качества интернет-соединения.

6.2. Выбор видов приложений при технической реализации проектов

Выбор видов приложений при технической реализации производится по следующим основным параметрам.

Интерфейс. Одним из первых аргументов, которые приводят сторонники приложений – наиболее близкий к ОС и привычный для пользователей интерфейс. Действительно мобильное приложение наиболее тесно интегрировано с платформой и дает реализовать привычный отзывчивый интерфейс. С другой стороны web-сайт с помощью хорошего форматирования и использования JavaScript может дать вполне понятный метод взаимодействия. На текущий момент отзывы о web-сайте значительно уступает приложению, но мощность мобильных устройств продолжает расти и сами браузеры существенно меняются в лучшую сторону. Кроме того, различные версии мобильных ОС могут диктовать свои стандарты, которых приходится придерживаться. При этом некоторые нововведения могут оказаться не совсем понятны обычным пользователям. Существенным в данном случае является то, что наиболее активными пользователями (теми, кто выставляет рейтинг и делает комментарии в магазинах приложений) являются те, кто «фанатеет» от последних новшеств мобильной ОС. На это стоит обратить внимание при продвижении проекта – их можно использовать как союзников, помогающих распространению.

Быстродействие. Web-сайт, а особенно интерактивный, существенно уступает приложению с точки зрения быстродействия. Браузеры мобильных устройств пока не могут порадовать высокой производительностью, кроме того, web-разработчики используют не самые оптимизированные версии библиотек (плохая реализация этих библиотек никак не сказывается на «больших» браузерах, поэтому с этим там можно смириться). Однако и приложение не всегда может радовать хорошим быстродействием – излишняя анимация, сложный интерфейс значительно снижают «отклик». Кроме того, для сложной графики и анимации приходится использовать языки более низкого уровня, разрабатывать или покупать отдельные специализированные библиотеки.

Интеграция с платформой. В этой области приложения далеко опережают сайт. В приложении существенно больше возможностей для

доступа к устройству. Однако выше упоминался уже третий вариант, когда компонент браузера внедряется в приложение и в этом случае такая разница нивелируется. Кроме того, постоянно растет уровень предоставления доступа к возможностям устройства из браузера через расширяющийся набор API.

Наличие Интернета. Web-сайт запускается из браузера, поэтому требует постоянного соединения с сетью. Это не имеет значения, если проект реализуется исключительно как онлайновый. Однако даже в этом случае из-за особенностей мобильного доступа в Интернет переход между частями приложения (навигация) связана с неприятными для пользователя задержками. Возможно, использование API для хранения локальных данных решат эту проблему, но пока примеров такого применения найти не удалось. Мобильные приложения могут осуществлять работу без подключения, выполняя кеширование и обновление данных, если требуется, при появлении соединения. Но все же и приложению нужно подключение в подавляющем большинстве бизнес-решений.

Фрагментация. Для реализации проекта на всех или каких-то определенных платформах требуется разработать приложение для каждой из платформ отдельно, причем на каждой свои среда и язык разработки, свои стандарты интерфейса. В случае мобильного сайта одна версия должна покрывать потребности всех платформ. Так выглядит в теории. Но на практике оказывается, что браузеры на различных платформах функционируют по-разному. Приходится поддерживать либо несколько версий одного сайта, либо в коде подстраивать выдаваемый контент под текущий запрос. Существенные отличия в размерах экрана также сказываются и на верстке сайта.

Ресурсы. Существует такой аргумент, как наличие специалистов. Считается, что специалиста для разработки мобильных приложений очень трудно найти и требуется очень высокая оплата. Учитываем еще то, что под каждую платформу, скорее всего, потребуется отдельный разработчик. В то время как web разработчиков очень много и их услуги сравнительно меньше

стоят. Видимо все зависит от конкретной ситуации и конкретного места. Если в наличие есть web-разработчик, то наиболее выгодным будет разработать именно web-сайт, если есть мобильные разработчики, то вполне может оказаться не слишком затратным разработка приложения. Но опять же, зависит от проекта – если потребуется серверная часть (а она скорее всего потребуется), то опять же нужен будет web-разработчик, хотя возможно не такой высокой квалификации и трудоемкость его части будет существенно ниже.

Публикация. Приложения некоторых платформ «завязаны» на определенный магазин (AppStore, Windows Store). Даже если такой жесткой привязки нет, то пользователи все равно привыкли находить приложения в магазинах (Google Play). Такие магазины накладывают существенные ограничения на функции приложений (в первую очередь в области платных услуг), к тому же требуется значительно время на утверждение каждой новой версии. Со своей стороны, web-сайт доступен сразу, достаточно только открыть браузер и ввести адрес (хотя если присмотреться, то это довольно трудоемкое действие может оказаться). Новая версия web-сайта доступна сразу на момент публикации. Возможность предоставления платных услуг никак не ограничивается. Опять же аргумент весьма своеобразный – с одной стороны ограничение и медленная публикация в магазине, с другой – в магазине уже есть огромное число пользователей и уже готовые системы для оказания платных услуг. Тогда как на сайт пользователей надо привести, и оплата через сайт на мобильном устройстве остается очень трудоемкой процедурой.

HTML5. Большое внимание в последнее время уделяется аббревиатуре HTML5. Это понятие существенно отличается, если смотреть на него с маркетинговой или технической точки зрения.

Технологически HTML5 это дальнейшее развитие языка разметки HTML. Однако сделан существенный шаг в сторону большей структуризации представления, нежели формата отображения. В язык добавлены большие

мультимедийные возможности для проигрывания аудио и видео. Добавлена возможность работать с графикой. Существенно расширен язык форматирования CSS. В язык Java Script добавлено несколько API для работы с графикой, локальными данными, мультимедийным контентом. Сам язык существенно переработан в сторону увеличения быстродействия. Стандарт HTML5 все еще находится в разработке и продолжает дополняться.

С маркетинговой точки зрения HTML5 это гораздо более широкое понятие. Под ним понимают еще много дополнительных API в той или иной степени поддерживаемых различными браузерами, многие интересные расширения CSS (в первую очередь в области интерактивного отображения). Основой понятия является высокая интерактивность сайта, которая позволяет пользователям принимать его за нативные приложения.

С точки зрения мобильной разработки существенно разделять обычный web-сайт и сайт с использованием HTML5 не имеет смысла. Фактически стандартом любого сайта становится интерактивность в той или иной мере, реализованная с помощью Java Script и новых API. Не целесообразно выделять отдельно разработчиков web сайта и разработчиков HTML5 – web разработчик должен свободно владеть технологиями HTML5 и использовать их в случае, если проект удобно реализовать с помощью последних разработок.

Выводы. Как оказывается, ни один из приведенных аргументов не склоняет чашу весов в ту или иную сторону. В каждом аргументе есть как преимущества, так и недостатки обоих вариантов решения. Третий, комбинированный (гибридный), вариант тоже может решить часть проблем, но при этом порождает новые. Поэтому в каждом конкретном случае надо принимать решение исходя из текущей ситуации.

С точки зрения экономии ресурсов самым предпочтительным вариантом выглядит web разработка. Главное – не погрязнуть в тонкостях реализации, предоставить наиболее полезные функции пользователям. Помнить, что

главное – контент, а «красивости» (анимация, графика) отходят на второй план.

Если планируется онлайн работа проекта как основной вариант взаимодействия с пользователем – безусловно, надо начинать с сайта, который может охватывать не только мобильных клиентов, но и пользователей стационарных компьютеров. В случае успеха можно далее реализовать отдельно мобильные приложения на выбранные платформы. Для большинства бизнес-приложений такой вариант наиболее подходит.

Если проект предусматривает больше оффлайн работу и нацелен на мобильных пользователей, то тут стоит отдать предпочтение приложениям. Однако, как упоминалось выше, возможно web разработчик все равно потребуется.

Для реализации игр и других приложений, требующих высокой производительности интерфейса вероятно дальновиднее реализовать через приложения. Существуют кросс платформенные библиотеки для разработки игр, которые позволяют на одном коде (или с минимальными изменениями) реализовать нативные приложения для различных платформ.

6.3. Примеры использования GSM приложений

В основе применения GSM приложений чаще всего используется GSM-модуль, позволяющий управлять дистанционно любой автоматикой, принимая сигнал с телефона, работающего в диапазоне GSM, и осуществляя включение/выключение подсоединенной аппаратуры. Применяется он для открытия распашных и откатных ворот, шлагбаума на паркингах, автостоянках, в дачных и гаражных кооперативах, частных домах, удаленного управления инженерными системами полива, освещения, отопления, перезагрузки серверов и роутеров и т. д [25].

Наиболее широкое распространение GSM-модуль получил как надежный и бюджетный контроллер для управления групповым доступом на

объект, совместимый с популярной автоматикой ворот и шлагбаумов Doorhan и Came.

Как работает модуль. По сути GSM-модуль — это радиоприемник с установленной SIM-картой любого оператора сотовой связи и контроллер для обработки поступающей и исходящей информации. В базу данных модуля заносятся телефонные номера всех пользователей, имеющих право доступа на закрытую территорию. Современные модели поддерживают запись и хранение до 2000 номеров, более дорогие модификации способны обрабатывать до 10000 номеров.

Принцип работы устройства показан на рисунке 6.1.

Рис. 6.1. Принцип работы устройства открывание ворот

Принципиальная схема работы устройства. При осуществлении звонка контроллер производит сверку входящего номера с записанными данными, и при его наличии в памяти подается команда на осуществление открытия и приведение в действие привода шлагбаума и откатных ворот. Если номера в списке нет, то устройство просто сбрасывает звонок, не производя больше

никаких действий. Подобным же образом контроллер открывает распашные ворота, оборудованные электрозамком и приводом Doorhan или Came.

Соединения со звонящим абонентом не происходит, либо оно обрывается через несколько секунд, благодаря чему расходы на оплату услуг сотовой связи равны нулю. Если данные не совпадают, то пропуск через ограждающее устройство не предоставляется. В некоторых моделях существует возможность отключения идентификации, и пропуск осуществляется при любом входящем звонке на контроллер. Настройка блока управления GSM-модулем выполняется с помощью смс-команд, веб-интерфейса, программы на компьютере, подключенному через USB-порт, android-приложения для смартфонов.

Следующим примером является автоматическая дистанционная GSM-система управления отоплением. Дистанционное автоматическое управление системой отопления загородного дома может быть частью общей автоматизации инженерных систем, охраны, противопожарной безопасности, известной под названием «Умный дом», или работать самостоятельно, обеспечивая заданный уровень комфорта к приезду хозяев. Использование GSM-модулей позволяет запускать и контролировать автоматические процессы с помощью установленного на сотовый телефон мобильного приложения.

Принцип действия GSM-системы. Если пользоваться домом от случая к случаю, то отопление может работать в следующих режимах:

- ручное управление — приехал, включил, дождался прогрева дома, выключил, уехал — низкий уровень комфорта, риск замерзания трубопроводов;
- автоматическое поддержание «холостого» или «рабочего» температурного режима — высокие затраты на отопление, риск возникновения пожара;
- включение и поддержание температурного режима с удалённого источника — в случае приезда или в аварийной ситуации (возгорание,

промерзание трубопроводов) — высокий уровень комфорта и безопасности, низкие затраты на энергоносители.

Последний вариант представляется самым оптимальным, хотя и требует предварительной адаптации системы отопления (в том числе и котла) и приобретения, собственно, самого модуля.

Принцип действия системы состоит из внешнего воздействия на GSM-устройство, которое подает команды на включение системы отопления в заданном режиме. Принципиальная схема GSM-управления приведена на рисунке 6.2.

Рис. 6.2. Принципиальная схема GSM-управления

Включается котёл, запускается работа климатических и системных датчиков, передающих информацию на контроллеры, которые её анализируют и выдают команды исполнительным механизмам:

- открытие, закрытие, регулирование трубопроводной арматуры;
- увеличение, снижение мощности или отключение котла;
- блокировка вышедших из строя элементов.

В свою очередь, система передает данные GSM-модулю, который посылает сообщения в виде SMS на командное устройство (мобильный телефон, планшет и т.д.): информацию о температуре в помещении, о температуре теплоносителя, о нештатных ситуациях. Причем получение сообщений зависит от возможностей и заданных настроек.

Рассмотрим также GSM сигнализацию, её функциональные возможности и преимущества. Охрана домов, дач, квартир и гаражей является достаточно сложной задачей, для эффективного решения которой возникает потребность в применении различных защитных систем. Наиболее эффективным охранным комплексом, отличающимся широкими функциональными возможностями и высоким уровнем безопасности, является GSM сигнализация (рис. 6.3).

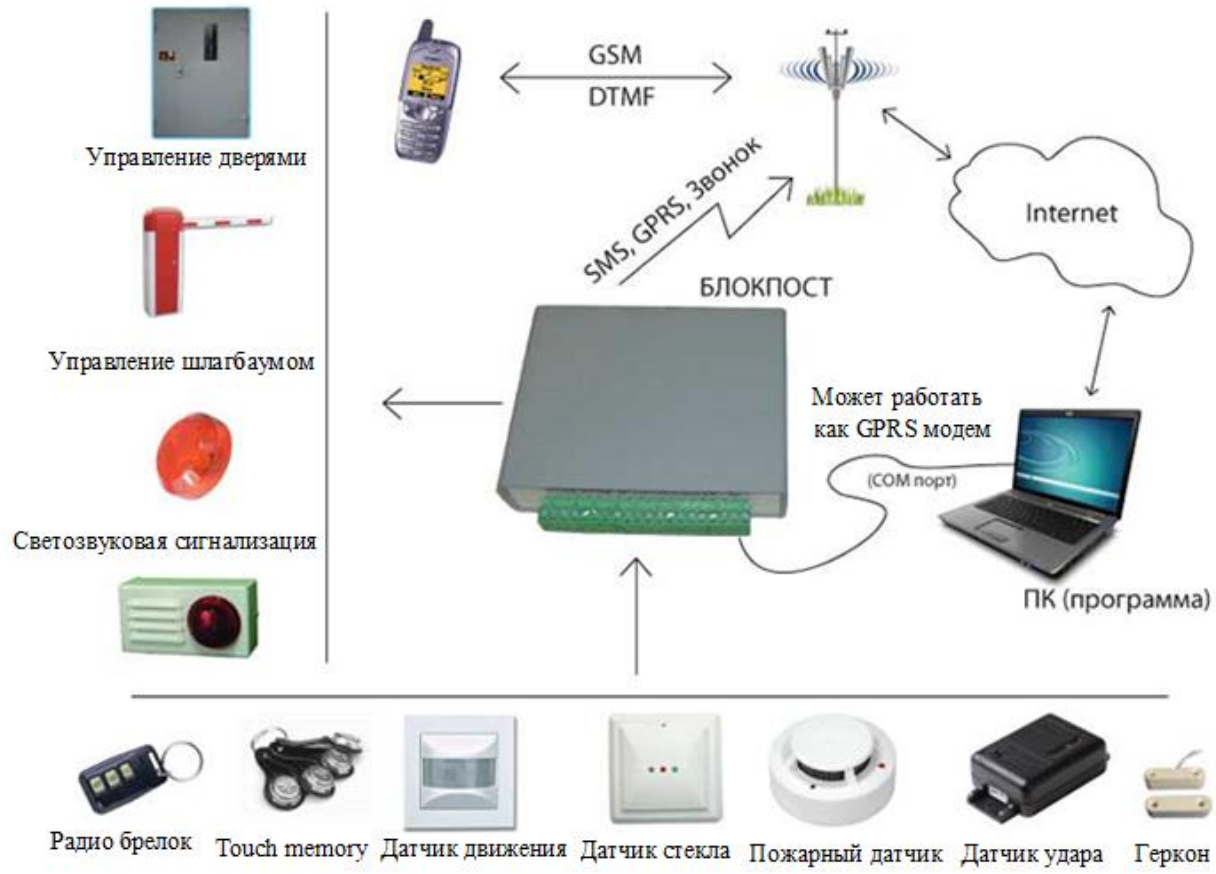


Рис. 6.3. Охранный комплекс с GSM сигнализацией

Эта инновационная разработка обеспечивает одновременный контроль объекта и мгновенную подачу предупредительных сигналов владельцу и соответствующим службам при возникновении ситуаций проникновения и взлома. Отличительной чертой таких систем является то, что кроме защиты от воров и злоумышленников, такого рода охранные комплексы позволяют следить за безопасностью на объекте в целом, предохраняя его от возможного пожара, затопления водой или от утечки газа.

Важным является также и то, что для передачи сигналов об опасности используются высокочастотные каналы сотовой связи, а не проводные магистрали, которые могут легко повредить злоумышленники.

ДЖСМ сигнализация представляет собой электронную систему, которая включает в свой состав несколько функциональных модулей. Они обеспечивают непрерывный контроль ситуации на объекте (движение, взлом, повышение температуры, задымленность, утечка газа/воды), срабатывают при возникновении одной или нескольких внештатных ситуаций и передают соответствующий сигнал тревоги на мобильные устройства владельца либо совершают дозвон на запрограммированные стационарные номера.

В качестве устройств, с помощью которых контролируется состояние объекта, используются специальные датчики и чувствительные сенсоры. Они могут быть проводными или беспроводными в зависимости от чего их связь с центральным электронным блоком поддерживается за счет радиоканала или проводной магистрали.

Центральный электронный модуль представляет собой микропроцессорное устройство, с помощью которого настраивается охранная сигнализация GSM, обрабатываются сигналы от датчиков и приводятся в действие исполнительные системы в виде светозвуковой сигнализации.

В состав центрального электронного блока входит ключевой элемент такого рода сигнализаций – GSM адаптер. Он представляет собой модуль сотовой связи, который поддерживает установку одной или двух SIM-карт и

программирование мобильных и стационарных номеров, на которые можно будет вести рассылку предупредительных сигналов и совершать дозвон в случае возникновения взлома или внештатной ситуации.

Еще одним немаловажным элементом, благодаря которому охранная система GSM функционирует непрерывно, является система питания. Преимущественное большинство сигнализаций владеют двумя системами – стационарной и автономной. Первая из них обеспечивает питание от сети 220 В, а вторая работает от встроенного аккумулятора.

Применение резервной автономной системы позволяет поддерживать работоспособность охраны даже в случае аварийного отключения основной сети или ее преднамеренного повреждения злоумышленниками.

Отличительной чертой, которой владеют охранные электронные комплексы, является поддержка широкого спектра различных датчиков. ЖСМ сигнализация может работать со следующими устройствами:

- датчики движения;
- миниатюрные видеокамеры;
- акустические датчики;
- термочувствительные сенсоры;
- датчики изменения объема и массы;
- пожарные датчики;
- мультифункциональные сенсоры, реагирующие на утечку воды, газа,
- появление дыма.

Если на объекте планируется GSM охрана**,** GSM сигнализация с различными функциональными датчиками будет оптимальным вариантом.

Наличие перечисленных устройств позволит реализовать многофункциональную систему охраны дома или квартиры от непрошенных гостей и от различных аварийных ситуаций.

Охранные системы GSM сигнализация в процессе своей работы поддерживает:

- оперативное оповещение владельцев с помощью SMS или MMS сообщений;
- дозвон на внесенные в память мобильные/стационарные телефонные номера;
- связь с владельцем охраняемого объекта, диспетчером или полицией/охранной компанией;
- ведение видеонаблюдения или звуковой записи по периметру объекта;
- функционирования факторов психологического сдерживания злоумышленника в виде звуковой сирены и световой сигнализации;
- работу исполнительных систем и механизмов, которые обеспечивают пожаротушение, удаление дыма из помещений, перекрытие подачи газа/воды или электричества;
- возможность постановки и снятия с охраны с помощью звонка, SMS-сообщения или DTMF-команды;
- использование системы, препятствующей блокированию злоумышленниками
- передачи сигнала тревоги через радиоканал.

Преимущества сотовых сигнализаций. GSM охрана по сравнению с иными системами безопасности владеет целым рядом преимуществ, среди которых:

- поддержка отправки сигнала тревоги сразу на несколько запрограммированных номеров;
- возможность совершения дозвона как на мобильные номера, так и на стационарные телефоны;
- оповещение о тревоге различными способами – звонок, SMS/MMS сообщение, звуковое/видеовещание с объекта, звуковая/световая сигнализация;
- высокий уровень защищенности от взлома и блокирования работы такого рода сигнализаций;
- возможность работы от автономных источников питания;

- автоматический контроль степени зарядки батареи и наличия денег на SIM-карте;
- возможность использования нескольких SIM-карт разных операторов мобильной связи;
- одна система GSM имеет возможность параллельного контроля нескольких объектов;
- поддержка обратной связи с мобильными устройствами владельца (пульт, мобильный телефон, планшет, смартфон и пр.).

К *недостаткам* сотовых сигнализаций GSM относятся:

- зависимость от качества сотовой связи;
- для максимальной эффективности работы сигнализации потребуются услуги диспетчера;
- достаточно высокая стоимость.

Система охранной GSM сигнализации выбирается по следующим критериям:

1. Подбираются датчики по типу подключения и функциональности. По способу подключения датчики могут быть беспроводными или проводными. Второй вариант стоит дешевле, но предусматривает дополнительные работы по прокладке коммутационных проводников от датчика к центральному электронному блоку.
2. Важно, чтобы GSM сигнализация поддерживала работу с несколькими операторами связи. Это исключит ее простой при отсутствии сигнала связи у одного из операторов.
3. Если требуется мультифункциональная система безопасности объекта важно выбирать комплексы охраны, которые поддерживают широкий спектр различных датчиков.
4. Чтобы исключить блокирование передачи сигнал тревоги с помощью специальных электронных приспособлений, важно чтобы системы GSM сигнализации поддерживали технологию защиты сигналов от глушения извне.

5. При выборе охранных систем нужно обратить внимание на наличие автономной системы питания и продолжительности работы устройств от нее. Независимый источник питания позволит исключить ситуации, когда охранные системы GSM сигнализации пребывают в неработоспособном состоянии.

В заключении рассмотрим, как построить «*Умный Дом»* своими руками. *Умный Дом* - это доступно, это просто, это нужно, без этого уже нельзя жить. Современная квартира, а тем более дом, коттедж, дача, офис - это сложный набор различных систем и коммуникаций - источников возможной опасности пожара, взрыва, затопления. Кроме того, это многочисленные окна и двери - места возможного нежелательного проникновения в Ваши владения и научить свой дом *уму-разуму,* можно своими руками без посторонней помощи.

Прежде всего, стоит осознать, что интеллектуальный дом - это централизованная система контроля и управления отдельными элементами, установленными по всему дому. В целом данные элементы можно разделить на несколько групп:

1. Элементы охраны.
2. Элементы пожарной безопасности.
3. Устройства для контроля водоснабжения и газа.
4. Элементы домашней автоматики.

Для того, чтобы самому собрать "*Умный дом*" нужно пройти несколько этапов:

1 этап. Постановка проблемы.

Прежде всего, необходимо определиться "Что должна уметь система?". Если устанавливается "*Умный дом*" ради престижа, то тогда не стоит тратить время на изучение всех тонкостей. Лучше сразу обратиться к профессионалам премиум-класса за баснословную сумму. Однако если решаетесь на самостоятельную сборку системы, следует четко сформулировать проблему. Например, *"Желательно получать SMS-*

сообщения о несанкционированном проникновении в мой дом", что позволяет сузить круг оборудования, отпадают всевозможные датчики утечки дыма/газа, *модуль* домашней автоматики и т.д.

2 этап. Получение консультации технического специалиста.

Прежде чем начать *поиск* соответствующих элементов, необходимо связаться с техническим специалистом. Технический специалист, найти которого можно через *Интернет-сайт* компании, предоставляющей подобные услуги, расскажет, какие именно элементы необходимо для выполнения тех или иных функций. Таким образом, сложится *представление* о примерной стоимости решения запланированной проблемы, а также о необходимых элементах, и круг оборудования станет еще уже.

3 этап. Выбор производителя.

Выбор производителя - одно из самых сложных и кропотливых занятий, которое у неподготовленного человека займет уйму времени.

Системы различных производителей имеют свои отличительные черты, особенности и нюансы. Например, если один производитель предлагает встроенный *GSM-модуль* (*Модуль* для управления системой с мобильного телефона), то другой предлагает его отдельно и так далее. Поэтому для дальнейшего сбора "Умного дома" нужно определиться с производителем. Для самостоятельной сборки "Умного дома" необходимо выбрать одного производителя (!). Нельзя взять датчик Jablotron, контрольную панель *Electronics Line*, пульт управления *Siemens*. Теоретически совмещать оборудование различных производителей можно, но мы не рекомендуем делать это без практической помощи технического специалиста. Таким образом, цель при поиске - выбрать одного производителя. В Интернете можно найти сайты производителей и подробно изучить системы и элементы каждого. Позвонив производителю можно узнать нюансы и особенности каждой системы.

4 этап. *Поиск* необходимых элементов и оформление заказа.

В результате трех пройденных этапов, должны иметь четкое *представление* о том, как должна выглядеть система и из каких элементов она будет состоять. Рекомендуется расписать состав системы на листке бумаги, так будет проще сориентироваться в море выплывающих нюансов. Необходимо также указать количество устройств исходя из количества комнат в жилище. Теперь главное - собрать эти элементы в одну корзину. Для примера возьмем стандартный вариант против проникновения:

Решение против проникновения с оповещением по SMS для одной комнаты.

Состав системы:

Контрольная панель с *GSM*-модулем и встроенной клавиатурой ("Мозг" всей системы, по радиоканалу принимает информацию от датчиков и других устройств, находящихся в доме, и команды, поступающие непосредственно от владельца системы) - 1 шт.

Магнитоконтакт (устройство, фиксирующее открытие/закрытие входной двери.

Датчик движения - 1 шт. (Инфракрасный детектор)

Брелок - 2 шт. (два пользователя системой)

Следует обратить внимание на то, что один и тот же производитель может предлагать различные варианты одного и того же датчика. Самым распространенным вариантом является датчик движения (бывают датчик-шторка, датчик, не реагирующий на животных, и т.д.). Уточните состав системы, найдите *Интернет*-магазин, предлагающий данные элементы и оформите заказ.

5 этап. Выбор тарифа и мобильного оператора.

После приобретения всех необходимых элементов рекомендуется изучать все инструкции, и подробно ознакомиться с существующими на момент покупки тарифами мобильных операторов. При этом особое внимание следует обратить на:

- *Стоимость* исходящего *SMS*-сообщения;
- *Стоимость* исходящего звонка;
- *Стоимость* междугороднего/международного звонка.

Рекомендуем установить sim-карту выбранного оператора.

В Интернете есть сайты, предлагающие сводные таблицы с тарифами, подходящими для использования в подобных системах.

6 этап. *Программирование*, установка и тестирование системы.

Три больших шага - *программирование*, установка и тестирование системы объединяем в один, так как все эти действия сводятся к изучению инструкции по инсталляции системы. Внимательно прочитайте инструкцию и в случае возникших проблем обратитесь за помощью к техническому специалисту.

Как видно, *Умный дом* можно собрать самостоятельно, но следует помнить, что подробное изучение работы системы займет не один день и много нервов. К сожалению, в Интернете не так много специалистов готовых и способных подробно расписать особенности каждой системы человеку со стороны. Да и с наличием необходимых элементов у многих проблемы. Поэтому, будет не лишним подумать о "запасном" варианте и начать *поиск* грамотных специалистов.

Контрольные вопросы

1. Дайте определение мобильного приложения.
2. Приведите преимущества мобильных приложений.
3. Как могут быть технически реализованы проекты приложений для мобильных устройств?
4. На основе каких основных параметров сравниваются направления технической реализации проектов приложений для мобильных устройств?
5. Поясните назначение GSM-модуля и его работу.

6. Поясните принцип работы устройства открывание ворот на основе GSM-Модуля.
7. Поясните принцип действия системы отопления по принципиальной схеме GSM-управления.
8. Поясните охранный комплекс с GSM сигнализацией.
9. Перечислите преимущества GSM охранных сотовых систем сигнализации.
10. Перечислите недостатки GSM охранных сотовых систем сигнализации.
11. По каким критериям выбирается система охранной GSM сигнализации?

ЗАКЛЮЧЕНИЕ

В современной подвижной радиосвязи связи одной из доминирующих, являются системы сотовой связи, которые явились новым шагом к эффективному использованию спектра частот и увеличению емкости сетей в условиях увеличения дефицита частотного ресурса. В настоящее время уже развернуты системы второго, третьего, четвертого и тестируются сети пятого поколения.

Вместе с тем, сети стандарта GSM, которые относятся к сетям второго поколения, не потеряли своей актуальности и широко используются во многих странах и континентах. Популярность стандарта настолько велика, что аббревиатура GSM уже понимается как «глобальная система подвижной радиосвязи».

Стандарт GSM по отношению к другим цифровым стандартам второго поколения отличается лучшими энергетическими и качественными показателями, обладают самыми высокими характеристиками безопасности и конфиденциальности связи. В стандарте используется ВРК с восемью временными окнами на несущую. Речь преобразуется кодеком RPE-LTP со скоростью 13 кбит/с. Качество, принимаемых речевых сообщений, обеспечивается при отношении сигнал/шум на входе приемника равной 9 дб, а в стандарте D-AMPSэто показатель равен 16дб.

В GSM предусмотрены ряд услуг, которых нет в других стандартах сотовой связи, а именно:

- использование интеллектуальных SIM-карт для доступа в сеть и слугам связи;
- закодированный радиоинтерфейс;
- шифрование передаваемых сообщений;
- использование криптографических алгоритмов для аутентификации абонента и идентификации абонентского оборудования;
- передача коротких сообщений по каналам сигнализации;

- межнациональный и национальный автоматический роуминг абонентов различных сетей;
- межсетевой роуминг абонента GSM с абонентами сетей DCS 1800, PCS 1900, DECT, а также со спутниковыми сетями наземной подвижной связи (Globalstar, Iridium, Inmarsat-P).

Используемые в GSM современные мобильные приложения строятся на основе GSM-модулей, позволяющие управлять дистанционно автоматикой, принимая сигнал с телефона, работающего в диапазоне GSM, и осуществляя включение/выключение подсоединенной аппаратуры. Применяется он для открытия распашных и откатных ворот, шлагбаума на паркингах, автостоянках, в дачных и гаражных кооперативах, частных домах, удаленного управления инженерными системами полива, освещения, отопления, перезагрузки серверов и роутеров, является основой построения «умного дома» и т.д. [25].

ГЛОССАРИЙ

2,5G (2,5 Generation) - технологии переходного периода, основанные на использовании усовершенствованных средств 2-го поколения, но способные обеспечивать услуги 3-го поколения.

3G (3 Generation) - 3-е поколение. Новое поколение систем мобильной связи, разрабатываемое в рамках программы IMT-2000. Сети радиодоступа этого поколения будут обеспечивать обмен информацией со скоростью до 144 кбит/с для абонентов с высокой мобильностью (скорость движения до 120 км/ч), 384 кбит/с для абонентов с низкой мобильностью (скорость до 3 км/ч) и 2,048 Мбит/с.

3GPP (3 Generation Partnership Project, проект партнерства 3-го поколения) - организация, созданная 4 декабря 1998 г. с целью проведения практических работ по стандартизации систем 3-го поколения в рамках программы IMT-2000. Основные учредители - ARIB (Япония), ETSI (Европа), T1P1 (США), TTA (Корея) и TTC (Япония).

3GPP2 (3-rd Generation Partnership Project 2, второй проект партнерства 3-го поколения) - организация, занимающаяся разработкой технических спецификаций 3G-стандартов, построенных на основе действующих в Северной Америке магистральных базовых сетей ANSI-41.

8-PSK (8-Phase Shift Keying) 8-ми позиционная Фазовая Манипуляция, при которой один символ передаётся тремя битами.

ADSL (Asymmetric data rate Digital Subscriber Line) — асимметричная высокоскоростная абонентская линия. Благодаря заложенной в ней асимметричности (до 8 Мбит/с в сторону абонента — так называемый поток downstream и до 1 Мбит/с в сторону сети — поток upstream) эта технология идеально подходит для подключения к Internet и применения в других системах типа клиент-сервер. Она способна обеспечить связь на расстоянии до 5,5 км, что точно совпадает с типичной длиной абонентских линий городских телефонных станций.

AMPS (Advanced Mobile Phone System) - Усовершенствованная Система Мобильной Связи. Аналоговая система, основанная на FDMA и работающая в частоте 800 МГц. Ширина канала 30 кГц.

ANSI (American National Standards Institute) - Американский Национальный Институт Стандартизации.

ANSI-136 Североамериканский цифровой стандарт мобильной связи, известный ранее как Interim Standard 18-136 (IS-136), используемый в системах TDMA (известных ранее под названием D-AMPS).

ARIB (Association of Radio Industries and Businesses) - Ассоциация Радиопромышленности и Бизнеса, которая была учреждена Министерством Почты и Связи (МРТ) Японии 15 мая 1995 г. Осуществляет функции, выполнявшиеся ранее научно-исследовательским центром по радиосистемам RCR и ассоциацией технологий радиовещания BTA. Аналогично ETSI в Европе организация ARIB осуществляет национальную стандартизацию в Японии.

Bluetooth - Международная инициатива компаний Ericsson, IBM, Intel, Nokia и Toshiba, направленная на установление стандарта беспроводного соединения между телефонами мобильной связи, ПК, ручными компьютерами и другими периферийными устройствами. Предусматривается использование мало дистанционных (до 10 м) каналов в свободной полосе 2,45 ГГц, используемой научно-медицинскими приборами.

BREW™ (Binary Runtime Environment for Wireless™) - технология, позволяющая разрабатывать свои программные приложения для телефонов.

BS (Base Station) - базовая станция.

BSC (Base Station Controller) - контроллер базовой станции, аппаратура управления базовыми станциями.

BTS (Base Transciever Station) - приемопередатчик базовой станции, приемная и передающая аппаратура.

CAP (Carrierless Amplitude-Phase) - амплитудно-фазовая модуляция без несущей. Существуют две ее разновидности — CAP64 и CAP128. В первом

варианте каждое модуляционное изменение несет информацию о 6 бит информации, во втором – о 7 бит. В отличие от 2B1Q этот вид модуляции не чувствителен к высокочастотным помехам и его спектр не занимает полосу разговорного канала (от 0 до 4 кГц). К сожалению, данная технология пока не стандартизована.

CATT (China Academy of Telecommunications Technology) – Китайская Академия Телекоммуникационных Технологий

CDG (CDMA Development Group) - Ассоциация по развитию технологии CDMA, включающая около 90 компаний, которые расположены в основном в США. Ассоциация содействует внедрению сетей cdmaOne и развитию систем 3-го поколения на базе cdma2000.

CDMA (Code Division Multiple Access) - множественный доступ с кодовым разделением.

CDMA2000 1xEV-DO (CDMA2000 1xData Only) - CDMA2000 1-я эволюция, только данные.

CDMA2000 1xEV-DV (CDMA2000 1xEvolution Data and Voice) - 1-я эволюция, данные и голос. Максимальная скорость до 3-5 Мбит/с, а нормальная пропускная способность в канале 1,25 МГц составляет 1 Мбит/с.

CDMA One - полностью цифровой стандарт, использующий диапазон частот 824-849 МГц для приема и 874-899 МГц для передачи.

CDPD (Cellular Digital Packet Data) - цифровая сотовая пакетная передача данных. Торговая марка первой в США коммерческой сотовой сети пакетной передачи данных. Сеть CDPD может взаимодействовать с существующими сетями сотовой телефонной связи, например, TDMA/D-AMPS. Обеспечивает передачу данных со скоростью до 9,2 кбит/с, выход в Internet и межсетевой роуминг.

Cell - Сота, ячейка

Cell site - Совокупность базовых станции, установленных в одном месте.

Cellular – Сотовый.

CEPT (Conference of European Post and Telecommunications) - Европейская Конференция Почты и Связи, которая учреждена 19 европейскими странами в 1959 г. По состоянию на июнь 1999 г. членами CEPT являются представители 43 стран. Штаб-квартира CEPT находится в Норвегии. CEPT имеет три комитета: один по почтовой связи (CERP) и два по телекоммуникациям (ERC и ECTRA).

CO (central office) - центральныйофис.

CTIA Cellular Telecommunication Industry Association - Ассоциация производителей сотовой связи, созданная в США в мае 1984 г. В настоящее время в нее входит более 90% компаний США.

CWTS (China Wireless Telecommunication Standards Group) – Группа Стандартов Беспроводной Связи Китая.

D-AMPS Digital AMPS - См. TDMA (ANSI-136)

DCCH (digital control channel) – цифровой контрольный канал **DCS 1800 см.GSM 1800DECT (Didital Enhanced Cordless Telecommunications)** – цифровая микросотовая система беспроводной связи.Он обеспечивает своим пользователям устойчивую высококачественную связь, защищенную от несанкционированного доступа. Стандарт DECT поддерживает речевую и факсимильную связь, а также передачу данных.

DECT EP (Digital Enhanced Cordless Telecommunications ETSI project) - расширенный стандарт системы с микросотовой структурой, подготовленный ETSI.

DIG (Digitalisation Interest Group) - группа по цифровизации сотовых сетей стандарта NMT.

DMT (Discrete MultiTone) - дискретная многотональная модуляция. В DMT формируется сразу 256 несущих с шагом в 4 кГц.

DSC (Digital Cellular System) - цифровая сотовая система. Достаточно общий термин, часто ассоциируется с DSC-1800.

DS-CDMA (Direct Sequence CDMA) - многостанционный доступ с кодовым разделением каналов и прямым расширением спектра. Метод

широкополосной передачи сигналов в CDMA-системах, основанный на использовании двухступенчатой модуляции кодированного потока данных. На первом шаге модуляции кодированный поток данных модулирует несущую (обычно методом BPSK или QPSK), а на втором осуществляется модуляция с расширением спектра с использованием прямой последовательности.

DSSS (Direct Sequence Spread Sequence) - расширение спектра методом прямой последовательности. Метод формирования широкополосного сигнала, при котором исходный двоичный сигнал преобразуется в псевдослучайную последовательность для манипуляции несущей. В эфир передается шумоподобный сигнал, обладающий всеми свойствами аддитивного белого шума. Расширение спектра сигнала в n раз с использованием DSSS позволяет уменьшить спектральную плотность мощности сигнала во столько же раз.

ECSD (Enhanced Circuit-Switched Data) - усовершенствованные системы с канальной коммутацией.

EDGE (Enhanced Data rates for Global Evolution), он же UWC-136 (практическая скорость - 384 кбит/сек, теоретически достижимая - 473,6 кбит/сек). Это не самостоятельный стандарт, а метод увеличения пропускной способности в GSM, GPRS сетях. Метод основан на применении более оптимальных методов модуляции и канального кодирования.

E-GPRS (Enhanced GPRS) - усовершенствованная служба GPRS. Один из терминов для обозначения технологии EDGE.

EIA (Electronic Industies Allience) - Альянс представителей электронной промышленности, который объединяет семь крупных организаций США.

ETCI (European Telecommunications Standards Institute) - Европейский Институт Телекоммуникационных Стандартов. Организация ETSI учреждена собранием директоров CEPT 14 января 1988 г. Основу ее деятельности составляет разработка телекоммуникационных стандартов.

ETMDA (Extended Time Division Multiple Access) - расширенный доступ с временным разделением.

FAC (Frequency Advisory Committee) - Консультативный комитет по частотам. Подчинен Федеральной комиссии связи (США); его основная сфера деятельности - обеспечение частотной координации.

FCC (Federal Communication Commission) - Федеральнаякомиссиясвязи (ФКС). Правительственный орган США, созданный в 1934 г. и ответственный за распределение частотного ресурса. Штаб-квартира FCC расположена в Вашингтоне.

FDD (Frequency Division Duplex) Двухсторонняя связь с Частотным Разделением.

FDMA (Frequency Division Multiple Access) - множественный доступ с разделением по частоте.

FPLMTS (Future Public Land Mobile Telecommunications System) - будущая публичная наземная мобильная телекоммуникационная система. Эта концепция была отвергнута в 1997 году после того, как стала очевидной невозможность создания единого глобального стандарта. После появилось семейство стандартов IMT-2000.

GAA (GPRS Applications Alliance) – Альянс по применению GPRS. Межотраслевое промышленное объединение, созданное в 1999 г. с целью содействия развитию GPRS и обеспечения координации работ по внедрению этой новой технологии в GSM и TDMA.

GERAN (GSM/EDGE Radio Access Network) - GSM/EDGE сеть с радиодоступом.

GMSK (Gaussian Minimum Shift Keying) - Минимальная Гаусовская Манипуляция, при которой один символ передаётся одним битом.

GPRS (General Packed Radio Services) - Радио-системы передачи с Пакетной коммутацией. GPRS часто упоминается как GSM-IP (GSM Internet Protocol). Расчётная скорость - 64 кбит/сек, практически достижимая скорость - 48 кбит/сек, теоретически достижимая - 115 кбит/сек.

GPS (Global Positioning System) - Система глобального позиционирования. Система использует навигационные спутники. При проектировании системы планировалось вывести 24 спутника на квазистационарные орбиты. Такие системы обеспечивают круглосуточную информацию о трехмерном положении, скорости и времени для пользователей, обладающих соответствующим оборудованием и находящихся на или вблизи земной поверхности (а иногда и вне её). Первой системой GPS, широко доступной гражданским пользователям, стала NAVSTAR, обслуживаемая Министерством обороны США.

GSM (Global System for Mobile communications) - Глобальная Система Мобильной связи, цифровой стандарт мобильной связи. Стандарт сотовой связи, использующий частоты 900, 1800 и 1900 МГц. Ответственный за стандартизацию технологии GSM Европейский Институт Стандартизации Электросвязи (ETSI). GSM использует TDMA технологию.

GSM 1800 цифровой стандарт GSM на частоте 1800 МГц, известен также как DCS 1800 или PCN, используется в Европе, в Тихоокеанских странах Азии, Австралии, России.

GSM 1900 цифровой стандарт GSM на частоте 1900 МГц, известен также как PCS, используется в США, Канаде, отдельных странах Латинской Америки и Африки.

GSM 900 цифровой стандарт GSM на частоте 900 МГц, распространен в более 100 странах Европы и Азии.

HCS (hierarchical cell structure) - иерархическая сотовая структура

HDSL (High data rate Digital Subscriber Line) — высокоскоростная цифровая абонентская линия. HDSL обеспечивает одинаковую скорость в обоих направлениях, которая обычно не превышает 2 Мбит/с. Чаще всего для организации линии HSDL используются две пары медных жил. Дальность связи составляет 5 – 7 км.

HPSK (Hybrid Phase-Shift Keying) - гибридная фазовая манипуляция, известная также как OCQPSK.

HSCSD (High-Speed Circuit Switched Data) - Высокоскоростные Системы передачи с Канальной Комутацией. Технология базируется на использовании существующих каналов GSM, в которых канальные интервалы объединены в группы (до четырех каналов), образуя общий групповой канал со скоростью 38,4 кбит/с (четыре канала по 9,6 кбит/с) или, теоретически, 57,6 кбит/с (четыре канала по 14,4 кбит/с). Реальная скорость 28,8 - 43,2 кбит/сек

HSWD (High Speed Wireless Data) - Высокоскоростная Беспроводная Передача Данных.

IFS (IMT-2000 Family of Systems) - Семейство систем IMT-2000

IH (intracell handover) - внутрисотовый хэндовер. Процедура смены рабочих параметров абонентской станции, обычно частоты или номера канального интервала, при связи с той же абонентской станцией.

i-mode - технология, обеспечивающая постоянное соединение с пропускной способностью 9,6 Кбит/с. Это позволило DoCoMo начать разработку мобильных приложений на базе IP-телефонии, опередив GPRS. Данная технология конкурирует и с WAP, так как использует компактную версию HTML (cHTML), в то время как WAP работает со специальным языком маркеров WML (Wireless Markup Language).

IMT-2000 (International Mobile Telecommunications - 2000) - международные мобильные средства телекоммуникаций 2000. Согласно данной инициативе IMT разрабатывает стандарт службы обеспечения радио доступа к глобальной телекоммуникационной инфраструктуре через спутниковые и наземные системы, которые призваны обслуживать пользователей фиксированных и мобильных систем в частных сетях и сетях общего пользования. Иными словами, это службы связи третьего поколения.

IMT-DS IMT-2000 Direct Spread - построен на базе проектов WCDMA (UTRA FDD) с прямым расширением спектра (DS-CDMA) и частотным дуплексным разносом (FDD), ориентированным на использование в парных полосах частот.

IMT-FT (IMT-2000 Frequency Time) - название проекта DECT EP, который поступил от ETSI. Новый стандарт на микросотовую систему DECT предполагает применение комбинированного частотно-временного дуплексного разноса и предназначен для работы как в парных, так и в непарных полосах частот. В IMT-FT определены три значения скоростей передачи: 1,152; 2,304 и 3,456 Мбит/с, реализовать которые можно за счет введения новых методов модуляции p/2-DPSK, p/4-DQPSK и p/8-D8PSK соответственно.

IMT-MC (IMT-2000 Multi Carrier) - по сути представляет собой модификацию многочастотной системы cdma2000, в которой обеспечивается обратная совместимость с оборудованием стандарта cdmaOne (IS-95). Увеличение пропускной способности реализуется за счет одновременной передачи сигналов на нескольких несущих с частотным дуплексным разносом, предполагается работа в непарных полосах частот.

IMT-SC (IMT-2000 Single Carrier) базируется на спецификациях проекта стандарта UWC-136; в нем определено поэтапное расширение возможностей существующей системы TDMA при условии работы системы в парных полосах частот.

IMT-TC (IMT-2000 Time-Code) - стандарт, представленный в МСЭ, основан на кодово-временном разделении каналов TDMA/CDMA с временным дуплексным разносом (TDD) и предназначен для организации связи в непарных полосах частот. IMT-TC фактически представляет собой чисто формальное объединение двух различных технических решений - европейского предложения UTRA TDD и китайского TD-SCDMA.

IPUI (International Portable User Identity) - международный код опознания абонента.

IRC (Idle Receiver Contriol) - управление свободным приемником. Протокол управления приемником в соте, когда соединение с абонентом еще не установлено.

IS-136 см. **TDMA (ANSI-136).**

ISDN (Integrated Services Digital Network) - цифровая сеть с интеграцией функций, позволяет осуществлять высокоскоростные передачи голосовых данных, информации или видео посредством существующих линий инфраструктуры.

ITU (International Telecommunication Union) - Международный Союз Электросвязи. Данная организация координирует использование правительственными и частными организациями глобальных телекоммуникационных сетей и интерфейсов. В 1932 году, в Мадриде, на базе International Telegraph Convention (Международная Телеграфная Конвенция) от 1865 года и International Radiotelegraph Convention (Международная Радиотелеграфная Конвенция) от 1906 года была разработана International Telecommunication Convention и был создан International Telecommunication Union (Международный Союз Электросвязи). Сейчас штабквартира организации находится в Женеве (Швейцария).

ITU-R (InternationalTelecommunicationUnion - Radiocommunication) - Сектор радиосвязи Международного союза электросвязи. Был образован в 1993 г. и является правопреемником Международного консультативного комитета по радиосвязи (МККР).

ITU-T (International Telecommunication Union - Telecom Standartization) - Сектор стандартизации в области телекоммуникаций Международного союза электросвязи. Был образован в 1993 г. и является правопреемником Международного консультативного комитета по телеграфии и телефонии (МККТТ).

IWU (Internetworking Unit) - устройство межсетевого обмена. Устройство, осуществляющее конвертирование протоколов связи при сопряжении сетей.

JDC (Japanese digital cellular) - японская цифровая сотовая

KSS (Key Stream Segments) - сегментированная шифрующая последовательность, вычисляемая на основе общего ключа в соответствии с заданным стандартным алгоритмом.

LCE (Link Control Entity) messages - сообщения логического модуля управления каналом.

LLME (Lower Layer Management Entity) – среда управления нижними уровнями. В этой среде передачи реализуются процедуры генерации соединения и разъединения физических каналов, отбора пригодных для связи каналов, а также оценивается качество принимаемых сигналов.

MAC (Media Access Control) - управление доступом к среде. Канальный подуровень, который отвечает за процедуры, сообщения и протоколы, обеспечивающие управление радиоресурсами, т.е. за установление, поддержание и разрыв соединений, динамический выбор каналов и др.

MAHO (Mobile Assisted Handover) - полуавтоматический хэндовер. Метод автоматического переключения, при котором абонентская станция выполняет измерение уровня сигнала и высылает отчет о результатах измерения на базовую станцию.

MBC (Multi-Bearer Conrol) - многоканальное управление. Протокол, поддерживающий соединение между двумя MAC-уровнями.

MCHO (Mobile-Controlled Handover) - управляемый абонентской станцией хэндовер. Метод децентрализованного управления переключением каналов, при котором мобильная станция измеряет уровень принимаемого от базовой станции сигнала и решает, где и какой хэндовер необходим.

MCS (Modulation Coding Scheme) - Кодовая Схема Модуляции.

MC-TDMA (Multi-Carrier TDMA) - многочастотная TDMA. Гибридная технология многостанционного доступа с временным разделением, при котором каждый канал характеризуется частотой и номером временного интервала в кадре.

misuse - неправомочное использование. Создание станции-двойника или использование чужой абонентской станции, (например, в результате хищения) с целью избежать оплаты услуг телефонной сети.

MM (Mobility Management) - управление мобильностью. Служба сетевого уровня, которая обеспечивает все функции, связанные с мобильностью.

MOS (Mean opinion score) - средняя экспертная оценка разборчивости речи. Метод субъективного тестирования качества речи, часто используемый для сравнения характеристик речевых кодеков, при котором слушатели выставляют оценки по пятибалльной системе. Результирующая оценка MOS вычисляется как среднее арифметическое для большого числа оценок.

MSDSL (Multirate SDSL) - является развитием SDSL. В данной технологии используется одна пара и поддерживается подстройка скорости в диапазоне от 64 до 1152 кбит/с.

NAMPS (Narrowband Advanced Mobile Phone System) - Узкополосная Усовершенствованная Система Мобильной Связи. Аналоговая система, основанная на FDMA и работающая в частоте 800 МГц. Ширина канала 10 кГц.

NIST (National Institute of Standard of Technology) - Национальный институт по стандартам и технологиям (прежнее название NBS). Правительственная организация США, отвечающая за разработку стандартов; ею, в частности, разработаны стандарты шифрования данных.

NMT (Nordic Mobile Telephone) - аналоговые мобильные системы скандинавских стран. Стандарт был разработан в Скандинавских странах, работает в частотном диапазоне 450 МГц.

NTIA (National Telecommunications Information Administration) - Национальная администрация по информатике и телекоммуникациям (США).

NWL (Network Layer) - сетевой уровень. Третий уровень сетевой модели OSI, на котором реализуются функции адресации и маршрутизации при межсетевом обмене, т.е. функции, связанные с распознаванием протокола, идентификацией, управлением условиями предоставления услуг, приемом и передачей широковещательной информации, а также управлением мобильностью.

ODMA (Opportunity Driven Multiple Access) - многостаронний доступ с управляемыми возможностями. Технология, базирующаяся на CDMA/TDMA

(бывшая концепция), предложенная ETSI в 1997 г. Протокол ретрансляции данных ODMA обеспечивает возможность прямой ретрансляции сигналов между мобильными станциями.

OQPSK (Offset Quadrature Phase-Shift Keying) - квадратурная фазовая манипуляция со сдвигом. Метод квадратурной манипуляции с временным сдвигом на T/2 (T - длительность передачи символа) между сигналами синфазного и квадратурного каналов, вследствие чего фаза манипулированного сигнала изменяется с шагом 6p/2. Применение OQPSK позволяет снизить требования к линейности усилителя мощности передатчика и сгладить провалы огибающей радиосигнала.

OVSF (Orthogonal Variable Spreading Factor codes) - ортогональные коды с переменным коэффициентом расширения. Ансамбль кодов с переменной длиной, определяемой коэффициентом расширения спектра SF. Такие коды формируются на основе кодового дерева, каждый последующий уровень которого удваивает число возможных кодовых комбинаций.

p/4 DQPSK - фазовая манипуляция, использующая коды из четырех символов {-p/4; p/4; -3p/4; 3p/4}, каждому из которых ставится в соответствие два бита данных {00, 01, 10, 11}. Модуляция (p/4 DQPSK применяется в ряде систем сотовой и транкинговой связи (IS-136, TETRA и др.).

PAP (Public Access Profile) – профиль общего доступа. Дополнение стандарта DECT (1994 г.), связанное с уточнением процедур аутентификации абонентских станций и интеграции их с сетями ТФОП, ISDN, X.25, IEEE 802.x, GSM.

PARK (Portable Access Right Key) – категории прав доступа. В стандарте DECT определены четыре категории прав, которые зависят от размеров сети: с малым числом сот (A), офисные со сложной коммутацией и связью с локальными сетями (B), сопряженные с сетями общего пользования (C), сопряженные с сетями GSM (D).

PCN (Personal Communications Network) - сеть персональной связи, известна также как DCS 1800 или GSM 1800.

PCS (Personal Communications Service) - система персональной связи, обобщающее название для сотовых сетей США стандарта GSM 1900.

PCSS (Personal Communications Satellite Services) - услуги (службы) спутниковойперсональнойсвязи.

PDC (Personal Digital Cellular) - персональная цифровая сотовая связь.Подобно GSM, стандарт основан на технологии TDMA. Используется исключительно в Японии.

PHS (Personal Handyphone System) - система персонального ручного телефона.

POTS (Plain Old Telephone Service) - обычная телефонная служба. Традиционная телефонная сеть, построенная на принципах коммутации каналов и предоставляющая услуги междугородной и международной связи.

PP (Portable Part) - терминальный абонентский радиоблок. Портативный терминал, в котором реализован GAP-профиль услуг.

PT (Portable Radio Termination) - сетевое окончание портативного радиоблока.

PTP (peer-to-peer) - Пиринговые сети - от английского \"peer-to-peer\" - это сети непосредственной (без центрального сервера) связи между двумя или несколькими компьютерами.

QOQAM (Quaternary Offset Quadrature Amplitude Modulation) - квадратурная амплитудная модуляция со смещением на четверть. Метод модуляции с повышенной спектральной эффективностью и меньшим диапазоном изменения, огибающей по сравнению с обычной квадратурной амплитудной модуляцией QAM. Он предъявляет менее жесткие требования к линейности усилителей мощности передатчиков.

RADSL (Rate Adaptive Digital Subscriber Line) — является разновидностью ADSL и обеспечивает скорость от 1 до 6 Мбит/с.

RAP (RLL Access Profile of DECT) — профиль абонентского радиодоступа.

RF (Radio Frequency) – радиочастота.

RFP (Radio Fixed Part) — базовый радиоблок. Фиксированный терминал, оснащенный двухпроводной линией связи, которая подключается к АТС (аналог базовой станции).

RLL (Radio Local Loop) — абонентская радиолиния. Технология беспроводного доступа, преимущественно предназначенная для решения проблемы «последней мили» и организации связи с удаленными пользователями. См. также: WLL.

ROBO (Regional Office/Branch Office) — региональный офис/филиал. Технология подключения к центральной системе сетей средних размеров (например, сетей региональных отделений предприятия). См. также: SOHO.

RSSI (Radio Signal Strengh Indicator) — индикатор уровня радиосигнала. Этот уровень является основным показателем, определяющим пригодность радиоканала для связи. Диапазон изменения RSSI в стандарте DECT определен от – 93 до -33 дБм (шаг 6 дБ).

RSSI handover - Хэндовер на основе измерения уровня RSSI. Процедура переключения абонентской станции, основанная на измерении уровня сигнала от двух и более базовых станций. Для того чтобы, предотвратить колебательный процесс (частое переключение), переключение осуществляется не сразу, а с определенным гистерезисом, т.е. при уверенном превышении одного сигнала над другим.

SB (simplex bearer) — симплексный канал. Тип физического канала передачи данных.

SC (sliding collision) — скользящий конфликт. Конфликт, который возникает в системах с временным доступом (TDMA) из-за перекрытия по длительности сигналов двух станций, работающих в соседних временных интервалах одного кадра. Чтобы исключить потери информации, в конце кадра обычно вводят защитный интервал, т.е. несколько пустых позиций, на которых сигнал не передается.

SCK (static cipher key) — статический шифровальный ключ. Открытый ключ с низкой криптостойкостью, который хранится в ЗУ абонентской

станции. Такой ключ обычно используется для защиты каналов сигнализации, а также в системах, которые функционируют без явной аутентификации.

SDSL (Single line Digital Subscriber Line) — высокоскоростная цифровая линия по одной физической паре. Иногда под буквой S подразумевают термин «симметричная». В SDSL скорость 2 Мбит/с обеспечивается по одной медной паре.

SH (seamless handover) — гладкийх эндовер. Хэндовер без разрыва соединения, процедура которого подразумевает, что мобильная станция не разрывает уже установленное соединение до тех пор, пока не будет установлено новое. За счет плавного переключения с одной базовой станции на другую не происходит ухудшения качества связи в момент переключения.

SMS short message service - услуга передачи коротких сообщений

SOHO (Small Office/Home Offce) — малый офис/домашний офис. Профиль удаленного доступа для сетей небольших офисов и домашних сетей.

TACS (Total Access Communications System) – Система связи полного доступа. Аналоговый стандарт с шириной канала 25кГц.

TBC (Traffic Bearer Control) - управление каналом трафика (функция MAC-уровня).

TDD (Time Division Duplex) - Двухсторонняя связь с Временным Разделением. Метод обмена информацией по одной линии связи с уплотнением каналов приема и передачи в разных временных интервалах одного кадра. Режим TDD предназначен для применения в пико- и микросотах, когда абоненты передвигаются с невысокой скоростью в ограниченном пространстве.

TDMA (Time Division Multiple Access) – Доступ с Временным Разделением.

TD-SCDMA (Time Division Synchronous Code Division Multiple Access) – Доступ с Синхронным Временно-Кодовым Разделением.

TETRA (Terrestrial Trunked Radio) – Транкинговая радиосвязь. Этот стандарт был создан под эгидой Европейского института

телекоммуникационных стандартов (ETSI) с целью заменить со временем все существующие разнородные аналоговые стандарты транкинговой связи. Сегодня он является единым стандартом цифровой транкинговой радиосвязи в странах ЕС. Уровень надежности и безопасности стандарта TETRA многократно превышает существующие аналоговые системы.

TIA (Telecommunications Industry Association) – Ассоциация Индустрии Связи США.

TRAU (Transcoding Rate Adaptation Unit) - блок перекодирования и адаптации по скорости передачи. Цифровое устройство, которое обеспечивает сопряжение речевых каналов, использующих разные скорости передачи и методы модуляции, без индивидуального декодирования (путем цифрового преобразования). Такое устройство является автономным, хотя и может входить в состав мобильного центра коммутации.

TTA (Telecommunication Technology Association) - Ассоциация Телекоммуникационных Технологий Южной Кореи.

TTC (Telecommunication Technology Committee) - Комитет телекоммуникационных технологий Японии.

UAK (User Authentication Key) - абонентский аутентификационный ключ. Зашифрованная последовательность длиной 128 бит, которая обычно хранится вместе с регистрационными данными пользователя в ПЗУ абонентской станции.

UMTS (Universal Mobile Telecommunication System) - Универсальная Мобильная Телекоммуникационная Система передача данных до 384 кбит/сек при передвижении со скоростью до 120км/час и до 2мбит/сек при передвижении со скоростью до 10км/час. Данный стандарт сотовой связи третьего поколения для Европы, разработан ETSI.

UPI (User Personal Identity) - персональный идентификатор пользователя. Идентификатор, который обычно не хранится в памяти абонентской станции, а вводится вручную, аналогично PIN-номеру. Далее с его помощью вычисляется аутентификационный номер.

UPT (Universal Personal Telecommunications) – универсальная персональная связь. Технология, основанная на обеспечении единого номера абонента вне зависимости от его местонахождения и используемой сетевой инфраструктуры.

UTRA (UMTS Terrestrial Radio Access) - проект стандарта радиоинтерфейса, обеспечивающего наземный радиодоступ в систему UMTS, который разработан рабочей группой SMG2 ETSI. Термин института для интерфейса WCDMA.

UTRAN (UMTS Terrestrial Radio Access Network) - наземная сеть радиодоступа, построенная на базе радиоинтерфейса UTRA.

UWC-136 (Universal Wireless Communications\'-136 - универсальные мобильные коммуникации) - Координацией разработки занимался UWCC. Стандарт, он же EDGE, разработан в основном для упрощенной миграции операторов, предлагающих свои услуги в стандарте DAMPS/TDMA IS-136. По IMT-2000 этот стандарт называется IMT-SC.

UWCC (Universal Wireless Communications Consortium) - объединение разработчиков и операторов стандарта сотовой связи TDMA IS-136 и UWC-136. (Универсальный Консорциум Беспроводных Коммуникаций. 26.01.2001 Консорциум объявил о прекращении своей деятельности в связи с тем, что все цели, поставленные перед организацией, были выполнены.)

VDB (Visitor Data Base) - визитная база данных. В ней хранится та часть информации о местоположении абонентов, которая позволяет отслеживать их перемещение.

VDSL (Very high data rate Digital Subscriber Line) – сверхвысокоскоростная цифровая линия. Она поддерживает передачу к абоненту на скорости до 52 Мбит/с, а в обратном направлении — до 2 Мбит/с. Правда, в отличие от других xDSL-технологий, VDSL способна работать лишь на малых дистанциях, до 500 м.

WAP (Wireless Application Protocol) - бесплатный не лицензированный протокол беспроводной связи, позволяющий создавать расширенные

системы мобильной телефонии и получать доступ к страницам Интернета с мобильных телефонов.

WARC (World Administrative Radio Conference) - Всемирная административная конференция по радиочастотам.

WBS (Wireless base station) - базовая беспроводная станция. БС, используемая в сетях микросотовой связи.

WCDMA (Wideband code division multiple access) - 1. Широкополосный многостанционный доступ с кодовым разделением каналов. Общее название технологии многостанционного доступа, основанной на использовании сигналов с расширенным спектром и высокой скоростью передачи данных. 2. Название проекта системы 3-го поколения, предложенного ARIB (Япония).

WIMS (Wireless Multimedia and Messaging Services) - 1. Беспроводная служба передачи сообщений и мультимедиа. 2. Проект стандарта системы 3-го поколения WCDMA, подготовленный подкомитетом TR-46.1 (США).

WLL (Wireless Local Loop) - беспроводные абонентские линии. Наиболее часто используемое обозначение технологии абонентского доступа.

WPBAX (Wireless PABX) - беспроводная УАТС. Учрежденческая АТС, интегрированная с сетью базовых станций, которая обеспечивает услуги беспроводной связи в пределах территории предприятия. Абоненты пользуются либо носимыми абонентскими станциями, либо портативными абонентскими радиоблоками, к которым подключено стандартное абонентское оборудование — телефон, факс, модем и т.д.

WRS (Wireless Relay Station) - беспроводная ретрансляционная станция. Станция, предназначенная для ретрансляции данных в сетях абонентского радиодоступа.

Z-field Z-поле - Защитный интервал в кадре. См. также: SC (sliding collision).

ЛИТЕРАТУРА

1. «О стратегии действий по дальнейшему развитию Республики Узбекистан». Указ президента Республики Узбекистан №УП-4947 от 07.02.2017 г.
2. «О мерах по дальнейшему совершенствованию технологий и коммуникаций». Указ президента Республики Узбекистан №УП-5349 от 19.02.2018 г.
3. Постановление Президента Республики Узбекистан «О мерах по дальнейшему внедрению и развитию современных информационно-коммуникационных технологий в реальном секторе экономики» №ПП-2158 от 3 апреля 2014 года.
4. Постановление Президента Республики Узбекистан №ПП-2834 от 15марта 2017 года. «О мерах по дальнейшему совершенствованию деятельности Ташкентского университета информационных технологий».
5. Ибраимов Р.Р. Мобильные системы связи. Учеб. пос., ТУИТ, 2004.
6. Бабков В.Ю. Вознюк М.А. Михайлов П.А. Сети мобильной связи. М.: Горячая линия-Телеком, 2006.
7. Веселовский Кшиштоф. Системы подвижной радиосвязи. – М.: Горячая линия – Телеком, 2006, 536с.
8. Андреев, В.А. Направляющие системы электросвязи. В 2 тт. Т. 2.
9. Проектирование, строительство и техническая эксплуатация / В.А. Андреев, Э.Л. Портнов и др. М.: ГЛТ, 2010. 424 с.
10. Андреев В.А. Обзор системы GSM. Харьковский национальный университет радиоэлектроники. https://studfiles.net/preview/
11. Чекалин А.А. и др. Защита информации в системах мобильной связи. Учебное пособие, -2-е издание. М.: Горячая линия, 2005, 171с.

12. ETSI-GSM Technical Specification. GSM 04.08.-DCS Version 3.1.0 European digital cellular telecommunication system (Phase 1). Mobile Radio Interface — Layer 3. Specification 1996–1998
13. ETSI — GTS 08.08-EXT GSM 08.08 European digital cellular telecommunications system (Phase 1) BSS-MSC — Layer 3 specification 1996–1998
14. ETSI ETS 300 590 GSM 08.08 Digital cellular telecommunications system (Phase 2) (GSM). Mobile-services Switching Center — Base Station System (MSC - BSS) interface; Layer 3 specification 1996–1998
15. ETSI TS 100 590 GSM 08.08 Digital cellular telecommunications system (Phase 2+) (GSM). Mobile-services Switching Center-Base Station System (MSC-BSS) interface; Layer 3 specification 1997–2001
16. Аджемов А.С., Кучерявый А.Е. Система сигнализации ОКС № 7М.: Радио и связь, 2002.
17. Кожанов Ю.Ф. Протоколы и интерфейсы в цифровой сети с коммутацией каналов. Siemens. 2002
18. ITU-T Recommendation I.450 User — Network Interface Layer 3 — General Aspects. Март 1998 (Rec.Q.930)
19. Громаков Ю.А. Организация физических и логических каналов в стандарте GSM.Электросвязь. № 10. 1993. С. 9–12
20. C. Sonthcott. Speech Proceeding in the Pan-European Cellular Mobile Telephone System. IEE Colloquium: "Digitized Speech Communication via Mobile Radio". London. 19 December, 1988. p.p. 5/1-5/5.
21. D. Freeman, C. Sonthcott, 1. Boyd. A Voice Activity Detector for the Pan-European Digital Cellular Mobile Telephone Service. IEE Colloquium
22. "Digitized Speech Communication via Mobile Radio". London. 19 December,1988. p.p. 6/1-6/5
23. Что такое мобильное приложение. https://www.kakprosto.ru/
24. Чем отличается мобильный сайт от приложения? https://appcraft.pro/blog/

25. GSM сигнализация: функциональные возможности, преимущества. https://bezopasnostin.ru/

Учебник по курсу

GSM и управление мобильностью

для специальности 5А350901 –Мобильные системы связи

Рассмотрен на заседании кафедры ТМС
«__» ____ 2019 года (протокол №___)

Рассмотрен и рекомендован к печати научно-методическим Советом ФТТ ТУИТ «__» ____ 2020 года (протокол № ___)

Рассмотрен и рекомендован к печати научно-методическим советом ТУИТ
«__» ____ 2020 года (протокол № ___)

Авторы:	Ибраимов Р.Р.
	Пулатов Ш.У.
	Хатамов А.П.
	Мадаминов Х.Х.
Ответственный редактор	Раджабов Т.Д.
Технический редактор	Пулатов Ш.У.
Корректор	Юлдашев А.У.